SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

Rapporti patrimoniali e nuove tecnologie

Quaderno 31

MODUS

Volume a cura di Lorenza Calcagno, Antonella Ciriello e Marisaria Maugeri, *componenti del Comitato direttivo* e di Giusella Finocchiaro, *Professoressa ordinaria di diritto privato e di diritto di Internet presso l'Università* Alma Mater Studiorum *di Bologna*

Contributo redazionale: Antonella Licheri, *funzionario giudiziario della Scuola superiore della magistratura* e Giuliano Graniti, *nell'ambito del tirocinio curriculare presso la Scuola superiore della magistratura, a seguito della convenzione sottoscritta con la Libera Università Internazionale degli Studi Sociali Guido Carli*

POLIGRAFICO
E ZECCA
DELLO STATO
ITALIANO

Coordinamento editoriale e cura del progetto grafico:
Camilla Pergoli Campanelli

ISBN 9791280600400

SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

Rapporti patrimoniali e nuove tecnologie

Quaderno 31

MODUS

La Scuola e la collana dei Quaderni

La Magna carta dei giudici, adottata dal Consiglio consultivo dei giudici europei, facendo proprio un principio condiviso nell'ambito dei diversi ordinamenti europei, riconosce nella formazione "un importante elemento di garanzia dell'indipendenza dei giudici, nonché della qualità e dell'efficacia del sistema giudiziario" (pt. 8).

In questa prospettiva la Scuola superiore della magistratura raccoglie l'esperienza maturata dal Csm nell'attività di preparazione e aggiornamento professionale dei giudici e dei pubblici ministeri, che è proseguita fino all'entrata in funzione della Scuola, cui la riforma dell'ordinamento giudiziario ha affidato la competenza esclusiva in tema di formazione dei magistrati (d.lgs. n. 26 del 2006).

Il primo Comitato direttivo si è insediato il 24 novembre 2011. Il 15 ottobre 2012 è stato inaugurato il primo corso di formazione della Scuola dedicato ai magistrati ordinari in tirocinio e nel gennaio 2013 è stato avviato il primo programma di formazione permanente.

Oggi la Scuola è impegnata in tutti i settori della formazione dei magistrati: iniziale, permanente, decentrata, dirigenti, onorari, tirocinanti, internazionale.

Accanto all'organizzazione e alla realizzazione delle sessioni di aggiornamento professionale, la documentazione giuridica rappresenta un tema centrale nelle attività di formazione.

La Scuola mette già a disposizione di tutti i magistrati italiani una ricca biblioteca telematica all'interno della sezione del sito dedicata alle banche dati. Altrettanto fondamentale è il materiale didattico elaborato nel contesto delle sessioni formative e disponibile sul sito istituzionale, nell'ambito di ciascun corso.

La collana dei Quaderni, resa possibile grazie alla collaborazione con il Poligrafico e Zecca dello Stato italiano, nasce con l'intento di consentire la più ampia fruizione dei contributi più significativi di questo materiale di studio e dei risultati dell'attività di ricerca svolta dall'istituzione.

La collana si collega idealmente a quella inaugurata negli anni '80 del secolo scorso dal Csm e dedicata agli incontri di studio per i magistrati organizzati nell'ambito della formazione iniziale e continua, all'epoca di competenza consiliare.

I singoli volumi sono disponibili liberamente sul sito della Scuola e nell'ambito della biblioteca virtuale che contiene le pubblicazioni ufficiali dello Stato.

INDICE

Gli autori

Niccolò Abriani
Professore ordinario di Diritto commerciale, Università degli Studi di Firenze

Ugo Bechini
Notaio in Genova

Michele Colajanni
Professore ordinario di Ingegneria informatica,
Università di Bologna "Alma Mater Studiorum"

Valentina Di Gregorio
Professoressa associata di Diritto privato, Università degli Studi di Genova

Mario Libertini
Professore emerito di Diritto commerciale,
Università degli Studi di Roma "Sapienza"

Lorenzo Lentini
Giudice del Tribunale delle Imprese di Brescia

Marisaria Maugeri
Professoressa Ordinaria di Diritto privato,
Università degli Studi di Catania

Erica Palmerini
Professoressa associata di Diritto privato,
Scuola Superiore Sant'Anna di Pisa

Giorgio Resta
Professore ordinario di Diritto privato comparato,
Università degli Studi "Roma Tre"

Maria Tecla Rodi
Avvocato, consigliere della divisione Mercati della Consob

Guido Romano
Magistrato, Ufficio del Massimario e del Ruolo della Corte di cassazione

Riccardo Rovatti
Professore Ordinario di Elaborazione statistica dei segnali,
Università di Bologna "Alma Mater Studiorum"

Pasquale Serrao d'Aquino
Magistrato addetto all'Ufficio studi CSM

Presentazione

L'interconnessione fra rapporti giuridici patrimoniali e nuove tecnologie non costituisce un fenomeno nuovo. Da essa origina la stessa disciplina del diritto dell'informatica, nelle sue diverse e successive espressioni e denominazioni, che si può datare in Italia alla fine degli anni '60.

All'epoca risale il dibattito sulla tutela del *softwar*e, la richiesta di disposizioni per la protezione della *privacy* e più tardi la genesi delle norme sul documento informatico e sul commercio elettronico.

Ciò che rende oggi il tema di maggiore interesse, sì da travalicare l'ambito strettamente specialistico, è la ormai pervasiva digitalizzazione della società, cosicché si può affermare che non siano più tracciabili dei confini netti fra *online* e *offline*, ma che invece la nostra vita si svolga ormai in quello che è stato efficacemente denominato "onlife", secondo la nota definizione di Floridi. Gli strumenti digitali per svolgere le relazioni, prima sociali e poi giuridiche, pervadono la nostra quotidianità e sono ampiamente diffusi.

Naturalmente la tecnologia incessantemente avanza e si sviluppa, creando nuove possibilità. Oggi si sente parlare quotidianamente di criptovalute, *smart contract*, *blockchain*, intelligenza artificiale e dunque di nuovi fenomeni che devono innanzitutto essere compresi per poi essere qualificati sotto il profilo giuridico e poter approdare all'individuazione di possibili soluzioni, interpretative o *de iure condendo*.

Oltre che in sede dottrinale, il dibattito si svolge anche nelle sedi di elaborazione della regolazione, in particolare a livello europeo e nelle organizzazioni internazionali e la giurisprudenza, in Italia e all'estero, in molti casi, ha già avuto modo di esprimersi.

In particolare, il tema dell'intelligenza artificiale pervade ormai il dibattito generale e anche in campo giuridico, ormai da qualche tempo, si riflette sulle diverse questioni sollevate dalle applicazioni di IA.

Le riflessioni investono tutti i settori del diritto: i contratti conclusi da applicazioni di intelligenza artificiale, il trattamento dei dati personali da parte di appositi programmi, l'elaborazione di decisioni giurisprudenziali tramite algoritmi, il supporto agli organi societari, l'attribuzione dell'autorialità al software e molti altri, dal momento che le applicazioni di intelligenza artificiale sono potenzialmente rinvenibili in ogni ambito giuridico.

Il ragionamento giuridico muove dalla definizione di intelligenza artificiale e dalla distinzione fra le diverse tipologie di applicazioni, a seconda che siano più o meno autonome nella elaborazione.

Già la definizione di intelligenza artificiale non è univoca. E la formulazione della definizione di intelligenza artificiale reca tacitamente con sé la questione della soggettività giuridica delle applicazioni di intelligenza artificiale e quindi, implicitamente, traccia le linee entro le quali poi si sviluppano le considerazioni sulla responsabilità.

L'altra questione che riguarda l'intelligenza artificiale così come, in generale, le altre applicazioni di tecnologie nuove, attiene all'approccio metodologico.

La domanda che sorge è se sia opportuno per il legislatore adottare un approccio volto a disciplinare l'intelligenza artificiale nel suo complesso o invece regolare le applicazioni dell'intelligenza artificiale in specifici settori o singole materie: se sia preferibile un approccio normativo orizzontale, come quello adottato dal legislatore europeo o piuttosto, verticale, circoscritto a determinati ambiti, come ad esempio quello contrattuale, secondo quanto auspicato da alcune organizzazioni internazionali, quali Uncitral e Unidroit.

Ci si interroga anche circa il livello di regolazione: se debba essere almeno quello europeo, nell'epoca della post globalizzazione, e quale debba essere il grado di specializzazione tecnica già nelle norme primarie.

Si costruiscono sistemi multilivello, in cui la disciplina è dettata dal legislatore europeo, da quello italiano e poi dalle norme tecniche e specialistiche. Nel frattempo, si è comunque chiamati a dirimere i conflitti che sorgono, applicando i principi generali e le norme vigenti, come già è accaduto in molti casi affrontati dalla giurisprudenza.

Diritto e tecnica continuano il dialogo che intreccia una pluralità di temi, con diverse prospettive: da quella della teoria del diritto, a quella di politica – o meglio, oggi, geopolitica – del diritto, a quella più strettamente tecnico-giuridica.

Riprendendo il confronto fra Irti e Severino nelle pagine di "Contratto e impresa" del 2006, vedremo se alla fine si affermerà la prevalenza della tecnica sul diritto o se invece la tecnica potrà essere "domata" dal diritto o, ancora, se fasi diverse nella storia sono destinate ad alternarsi.

Giusella Finocchiaro

Marisaria Maugeri

Le tutele di consumatori e utenti di token di pagamento: dal codice del consumo alla MiCAR

Sommario: 1. Introduzione. – 2. Sulla non applicabilità al mercato finanziario della Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011, sui diritti dei consumatori. – 3. Sull'applicabilità agli strumenti finanziari tokenizzati della Direttiva 2002/65/CE, del 23 settembre 2002, sulla commercializzazione a distanza di servizi finanziari. – 4. Le deroghe alla Direttiva 2002/65/CE introdotte dalla Direttiva 2015/2366/UE del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno. – 5. Il coordinamento delle discipline consumeristiche con il nuovo Regolamento UE 2023/1114 del 31 maggio 2023, relativo ai mercati delle cripto-attività.

1. Introduzione

La tutela di consumatori e utenti di token di pagamento è oggetto di una pluralità di discipline europee.

In questa sede, io prenderò in considerazione esclusivamente quanto previsto: (i) dalla Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011, sui diritti dei consumatori; (ii) dalla Direttiva 2002/65/CE, del 23 settembre 2002, sulla commercializzazione a distanza di servizi finanziari, che rimarrà in vigore fino al 18 giugno 2026; (iii) dalla Direttiva 2015/2366/UE del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno e (iv) dal Regolamento UE 2023/1114 del 31 maggio 2023, relativo ai mercati delle cripto-attività (Regolamento MiCA).

Farò cenno anche alla recentissima direttiva del Parlamento europeo e del Consiglio 2023/2673 del 22 novembre 2023, che modifica la direttiva 2011/83/UE per quanto riguarda i contratti di servizi finanziari conclusi a distanza e abroga la direttiva 2002/65/CE.

Le prime tre direttive sono poste espressamente a tutela (quanto meno anche) del "consumatore", mentre MiCAR è volta a proteggere (anche) il "detentore al dettaglio" (oltre al detentore o possessore[1] *tout court* e al cliente).

[1] Nella versione italiana del Regolamento si usa a volte l'espressione detentore, a volte quella di possessore, laddove nella versione inglese si utilizza l'espressione "holder".

Il "detentore al dettaglio", però, viene definito come: "qualsiasi persona fisica che agisce per scopi estranei alla propria attività commerciale, imprenditoriale, artigianale o professionale". Viene definito, cioè, nello stesso modo in cui all'interno dell'Unione si definisce il consumatore nelle discipline poste a sua tutela.

Di qui l'esigenza di comprendere se e come tali discipline si possano coordinare fra loro.

2. Sulla non applicabilità al mercato finanziario della Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011, sui diritti dei consumatori

Nonostante la Direttiva 2011/83/UE espressamente non si applichi ai servizi finanziari (art. 3, comma 3, lett. d), definiti come "qualsiasi servizio di natura bancaria, creditizia, assicurativa, servizi pensionistici individuali, di investimento o di pagamento" (art. 2, punto 12), alcuni autori hanno ritenuto che la disciplina in questa contenuta potesse trovare applicazione nel settore delle cripto-attività, interno al mercato finanziario.

Sostegno a tale tesi sembrava potersi ricavare dalla prima versione della proposta MiCAR. Questa, infatti, nel considerando 16, faceva salva l'applicabilità della Direttiva 2011/83/UE, così implicitamente accettando l'idea che all'interno del mercato finanziario quest'ultima potesse trovare applicazione.

Nel testo approvato, però, tale riferimento non si trova più.

Il legislatore europeo sembrerebbe, pertanto, aver voluto prendere posizione a favore della inapplicabilità della stessa nel settore considerato.

Ciò, però, potrebbe non esser dirimente. Prima di chiudere il discorso conviene, dunque, prestare la dovuta attenzione alla principale questione che ha condotto parte della dottrina a propendere per l'applicabilità della direttiva sui diritti dei consumatori. Mi riferisco alla questione relativa alla possibilità o meno di ricondurre alla categoria dei "servizi finanziari" anche la vendita (o cessione) da parte dell'emittente di azioni, di obbligazioni o fondi, pure tokenizzati.

Il problema è stato di recente approfondito da Philipp Maume. Secondo l'autore l'unica disciplina applicabile in caso di acquisizione di token (cioè, di acquisizione di un'azione, di un'obbligazione o di un fondo) sarebbe quella contenuta nella Direttiva 2011/83/UE[2].

[2] In particolare, l'autore, nell'occuparsi del diritto di recesso per il consumatore, sostiene quanto

L'autore, cioè, distingue il contratto di "acquisizione di prodotti finanziari" dal "contratto di servizi finanziari", ritenendo che la Direttiva 2011/83/UE si applichi al primo, mentre la Direttiva 2002/65/CE al secondo.

La soluzione interpretativa non convince. In vero l'elenco, contenuto nella Direttiva 97/7/CE, riguardante la protezione dei consumatori in materia di contratti a distanza, abrogata e sostituita dalla Direttiva 2011/83/UE, cui l'autore fa espresso riferimento per circoscrivere l'ambito di applicazione di quest'ultima (che, come si è detto dalla 97/7/CE discende), è testualmente definito "non esauriente" nell'art. 3 della stessa direttiva del 1997. A ciò si aggiunga che la Direttiva 2002/65/CE, che disciplina la "commercializzazione a distanza dei servizi finanziari ai consumatori" (art. 1), definisce il contratto a distanza come "qualunque contratto avente per oggetto servizi finanziari, concluso tra un fornitore e un consumatore nell'ambito di un sistema di vendita[3] o di prestazione di servizi a distanza organizzato dal fornitore che, per tale contratto, impieghi esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto, compresa la conclusione del contratto stesso". Tale dato rende evidente che la disciplina non escluda affatto il contratto di vendita (o acquisizione) dal suo ambito di applicazione. In altre parole, la stessa è riferita al settore e non al tipo di contratto[4].

Ed è plausibilmente aderendo all'interpretazione in questa sede proposta che il legislatore europeo ha espunto il riferimento alla Direttiva 2011/83/UE, che – come ho detto – era contenuto nel considerando 16, dal testo finale di MiCAR.

---

segue: "*Not relevant… is Directive 2002/65/Ec on financial services and direct marketing (Financial Services Directive, FSF). It applies to the provision of financial services online. The Directive mentions typical financial services as examples: bank accounts, credit cards, portfolio management, etc… The non-crypto equivalent of a token acquisition (which would be the acquisition of a share, bond, or fund) is not mentioned. That is straightforward because selling something to someone is not the same thing as providing a service for someone. Token sales are more comparable to the sale of goods, which generally falls within the scope of Directive 97/7/EC on distance contracts (Rec. 10 FSD) and its successor, the CRD. Thus, issuing tokens is not a financial service within the scope of FSD*" P. Maume, *Consumer Protection*, in P. Maume – L. Maute – M. Fromberger *The Law of Crypto Assets. A Handbook*, C.H.BECK/Nomos Verlagsgesellschaft/Baden-Baden/Hart Publishing, 2022, 110.

[3] Enfasi mia.

[4] La Direttiva 2011/83/UE fa espresso riferimento al contratto del "settore" finanziario nel definire il suo ambito di applicazione (cfr. considerando 32). Per maggiori approfondimenti sul punto, sia consentito rinviare a M. Maugeri, *Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*, in G. Gitti – M. Maugeri, *La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*, numero speciale di *ODCC*, Il Mulino, 2023, 236 ss.

Nei lavori preparatori, dell'aprile del 2021, infatti, si legge quanto segue: "Directive 2011/83/EU does not apply to financial services; referring it would be contradictory with the purpose of restricting the scope to financial like products/services". Il riferimento ai prodotti, oltreché ai servizi, rende palese l'adesione all'idea secondo la quale la Direttiva 2002/65/CE sia applicabile al settore finanziario in generale.

3. Sull'applicabilità agli strumenti finanziari tokenizzati della Direttiva 2002/65/CE, del 23 settembre 2002, sulla commercializzazione a distanza di servizi finanziari

La disciplina che si applica, dunque, nella contrattazione a distanza all'interno del settore finanziario, nei rapporti BtoC, è quella contenuta nella Direttiva 2002/65/CE, recepita nell'ordinamento italiano negli artt. 67-bis e ss. del Codice del consumo.

Non vi è ragione alcuna per ritenere che la "commercializzazione" delle cripto-attività possa sfuggire all'ambito di applicazione di tale disciplina[5].

Tale direttiva definisce i servizi finanziari, al pari della Direttiva 2011/83/UE, come "qualsiasi servizio di natura bancaria, creditizia, assicurativa, servizi pensionistici individuali, di investimento o di pagamento" (art. 2, lett. b). La stessa impone obblighi di informazione nei confronti del consumatore prima della conclusione del contratto a distanza (art. 3), obblighi di forma nelle comunicazioni delle condizioni contrattuali e delle informazioni preliminari (art. 5) e il diritto di recesso per il consumatore (art. 6).

Le informazioni da dare al consumatore riguardano: (i) il fornitore (ad es., identità, attività principale, indirizzo geografico, registro di commercio al quale è iscritto, estremi dell'autorizzazione); (ii) il servizio finanziario (fra l'altro, le principali caratteristiche del prodotto, il prezzo totale, l'eventuale rapporto fra il servizio finanziario e strumenti che presentano particolari rischi o il cui prezzo dipenda dalla fluttuazione dei mercati, l'esistenza di eventuali imposte o costi non versati tramite il fornitore, modalità di pagamento ed eventuali costi aggiuntivi); (iii) il contratto a distanza (ad es., l'esistenza o la mancanza del diritto di recesso, la durata e la modalità di esercizio di quest'ultimo, la legislazione applicabile); e (iv) il ricorso (procedure extra giudiziali di reclamo, esistenza di fondi di garanzia etc…).

---

[5] Tribunale Verona, 24 Gennaio 2017 (in https://www.ilcaso.it/giurisprudenza/archivio/16726.pdf, consultato il 14 febbraio 2023) ha ritenuto applicabile la disciplina contenuta negli articoli del codice del consumo che recepiscono la Direttiva 2002/65/CE in un'operazione di cambio di valuta tradizionale contro bitcoin.

Le comunicazioni devono avvenire attraverso supporto cartaceo o altro supporto durevole. La Direttiva 2002/65/CE, però, prevede anche che "In qualsiasi momento del rapporto contrattuale il consumatore, se lo richiede, abbia il diritto di ricevere le condizioni contrattuali su supporto cartaceo" (previsione in Italia contenuta nell'art. 67 undecies, comma 3 del cod. cons.). La previsione appare in generale "datata" e, rispetto al mercato delle cripto-attività, decisamente distonica.

Non è un caso, dunque, che la stessa non compaia più nella citata recentissima direttiva del Parlamento europeo e del Consiglio 2023/2673 del 22 novembre 2023, che modifica la direttiva 2011/83/UE per quanto riguarda i contratti di servizi finanziari conclusi a distanza e abroga la direttiva 2002/65/CE.

Il diritto di recesso non si applica ai servizi finanziari il cui prezzo dipende da fluttuazioni del mercato finanziario che il fornitore non è in grado di controllare (art. 6, comma 2).

4. Le deroghe alla Direttiva 2002/65/CE introdotte dalla Direttiva 2015/2366/UE del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno

Ma se quella descritta è la disciplina applicabile in generale a tutela dei consumatori in presenza di cripto attività nel mercato finanziario, occorre adesso prestare attenzione in particolare al contesto dei servizi di pagamento.

In vero, la Direttiva 2015/2366/UE, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, c.d. PSD2, con riferimento ai servizi di pagamento, opera deroghe alla Direttiva 2002/65/CE.

In particolare, l'articolo 39 della PSD2 dispone che le disposizioni ivi contenute lascino impregiudicata qualsiasi disposizione del diritto dell'Unione contenente requisiti supplementari in materia di informazione preliminare. Tuttavia, ove sia anche applicabile la direttiva 2002/65/CE, i requisiti informativi di cui all'articolo 3, paragrafo 1, di detta direttiva, fatti salvi il punto 2, lettere da c) a g), il punto 3, lettere a), d) ed e), e il punto 4, lettera b), di tale paragrafo, siano sostituiti dagli articoli 44, 45, 51 e 52 della PSD2 stessa.

Questi ultimi dispongono l'obbligo di disclosure di elementi legati alla specificità dello strumento di pagamento.

Ciò significa che in generale sembrerebbe continuarsi ad applicare la Direttiva 2002/65/CE anche nel contesto degli strumenti di pagamento. Solo gli obblighi di disclosure sembrerebbero esser diversamente specificati.

5. Il coordinamento delle discipline consumeristiche con il nuovo Regolamento UE 2023/1114 del 31 maggio 2023, relativo ai mercati delle cripto-attività

Occorre, dunque, comprendere come le due direttive richiamate si coniughino con MiCAR sotto il profilo della tutela del consumatore.

Analizziamo, in primo luogo, i requisiti richiesti da MiCAR per l'ammissione e l'offerta di e-money tokens.

Occorre subito mettere in evidenza che l'art. 48, secondo comma, di MiCAR equipara espressamente i token di moneta elettronica alla moneta elettronica ("I token di moneta elettronica sono considerati moneta elettronica").

La disciplina prevede che nessuno all'interno dell'Unione possa offrire o chiedere l'ammissione alla negoziazione di e-money tokens se non sia l'emittente di tali gettoni di moneta elettronica (art. 48) (fatta sempre salva la possibilità per l'emittente di delegare l'attività di offerta al pubblico o di ammissione alla negoziazione a una persona terza previo consenso scritto).

Prima di offrire e-money tokens o di chiedere l'ammissione di questi alla negoziazione su una piattaforma di trading, l'emittente deve pubblicare un libro bianco (e una sintesi di questo) sul proprio sito web (art. 51). Il White Paper deve essere notificato alle autorità competenti.

L'elenco delle indicazioni da fornire tramite il White Paper, contenuto nell'art. 51 di MiCAR, segue l'impostazione della Direttiva 2002/65/CE e della PSD2, prevedendo anche ulteriori obblighi di disclosure e, pertanto, si può affermare che il rispetto della disciplina MiCAR comporti contestualmente anche il rispetto di quanto previsto in tali direttive, in particolare di quanto previsto dalla PSD2 che, come si è detto, in tema di tipi di informazioni da fornire, è l'unica applicabile, in quanto deroga alla direttiva sulla commercializzazione a distanza dei servizi finanziari.

Non ci sono problemi di compatibilità con la disciplina relativa al supporto durevole, perché il libro bianco deve essere pubblicato sul sito dell'emittente e comunicato dalle autorità competenti. La comunicazione può dirsi, dunque, immodificabile (con riferimento al periodo in cui è fornita) e, pertanto, idonea a integrare gli estremi della comunicazione dell'informazione su "supporto durevole", previsto dalla direttiva 2002/65/CE.

Su richiesta di chi possiede e-money tokens, l'emittente è tenuto a rimborsare il valore dei token in fondi diversi dall'e-money, cioè in banconote o in moneta bancaria[6]. Più precisamente l'art. 49, comma 4, prevede quanto segue: "Su richie-

[6] Cfr. la definizione di fondi contenuta nell'art. 4, par. 1, n. 25, della Direttiva (UE) 20115/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/CE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64.

sta di un possessore di un token di moneta elettronica, l'emittente di tale token di moneta elettronica lo rimborsa, in qualsiasi momento e al valore nominale, pagando in fondi diversi dalla moneta elettronica il valore monetario del token di moneta elettronica detenuto al possessore del token di moneta elettronica". Nel White Paper devono essere indicate le condizioni di rimborso (art. 49, comma 5).

Questa forma di tutela è addirittura più forte del recesso.

Ciò non toglie che, ad oggi, il consumatore possa anche esercitare il recesso previsto dalla direttiva 2002/65/CE.

Un discorso analogo si può fare anche tenendo conto della disciplina che grava sugli emittenti e sugli offerenti di asset-referenced tokens sotto il profilo delle informazioni e del recesso.

Anche su tali soggetti incombe, infatti, l'obbligo di redazione di un White paper e una sintesi di questo redatta con parole facili e comprensibili. Nella sintesi deve essere indicata la possibilità di avvalersi del diritto di riscatto.

Anche in questo caso, l'elenco delle indicazioni da fornire tramite il White Paper segue l'impostazione delle due Direttive di cui si è detto, prevedendo anche ulteriori obblighi di disclosure. Sembra, pertanto, possa dirsi che, anche in questo caso, il rispetto della disciplina MiCAR comporti contestualmente anche il rispetto di quanto previsto in tali direttive.

Il libro bianco, approvato dalle Autorità, deve essere pubblicato sul sito dell'emittente e comunicato dalle autorità competenti all'ESMA che lo inserisce nel registro dei White Papers degli emittenti di token collegati ad attività messo a disposizione del pubblico sul sito web di detta Agenzia europea. Anche in questo caso, la comunicazione può dirsi, dunque, immodificabile (con riferimento al periodo in cui è fornita) e, pertanto, idonea a integrare gli estremi della comunicazione dell'informazione su "supporto durevole", previsto dalla direttiva 2002/65/CE.

Anche con riferimento alla cessione di asset-referenced tokens, non è previsto il recesso ma è previsto il rimborso e il diritto di riscatto.

Una tutela forte, dunque, ma che non esclude, per le ragioni già dette sopra con riferimento alla disciplina relativa agli e-money tokens, la possibilità di esercitare il recesso.

Qualche considerazione adesso sul rapporto fra obblighi che gravano sui prestatori di servizi, come definiti in MiCAR, e il rispetto degli obblighi disposti dalla Direttiva 2002/65/CE e dalla PSD2.

Per MiCAR "servizio per le cripto-attività" è:

qualsiasi servizio e attività elencati di seguito in relazione a qualsiasi cripto-attività:

a) prestazione di custodia e amministrazione di cripto-attività per conto di clienti;

b) gestione di una piattaforma di negoziazione di cripto-attività;
c) cambio di cripto-attività con fondi;
d) scambio di cripto-attività con altre cripto-attività;
e) esecuzione di ordini di cripto-attività per conto di clienti;
f) collocamento di cripto-attività;
g) ricezione e trasmissione di ordini di cripto-attività per conto di clienti;
h) prestazione di consulenza sulle cripto-attività;
i) prestazione di gestione di portafoglio sulle cripto-attività;
j) prestazione di servizi di trasferimento di cripto-attività per conto dei clienti.

Nel considerando 79 di MiCAR si legge quanto segue: "Al fine di garantire la tutela dei consumatori, l'integrità del mercato e la stabilità finanziaria, i prestatori di servizi per le cripto-attività dovrebbero sempre agire in modo onesto, corretto e professionale e nel migliore interesse dei loro clienti. I servizi per le cripto-attività dovrebbero essere considerati "servizi finanziari" quali definiti nella direttiva 2002/65/CE nei casi in cui soddisfano i criteri di tale direttiva. Se commercializzati a distanza, anche i contratti tra i prestatori di servizi per le cripto-attività e i consumatori dovrebbero essere soggetti alla direttiva 2002/65/CE, salvo esplicita disposizione contraria del presente regolamento. I prestatori di servizi per le cripto-attività dovrebbero fornire ai loro clienti informazioni complete, corrette, chiare e non fuorvianti e avvertirli dei rischi connessi alle cripto-attività. I prestatori di servizi per le cripto-attività dovrebbero rendere pubbliche le loro politiche tariffarie, istituire procedure di trattamento dei reclami e adottare una politica solida per individuare, prevenire, gestire e comunicare i conflitti di interesse".

Se commercializzati a distanza, dunque, tutti i contratti stipulati fra i fornitori di servizi di crypto-asset e i consumatori dovrebbero esser sottoposti alla disciplina della Direttiva 2002/65/CE, a meno che MiCAR stessa non disponga diversamente.

Il Considerando 90, inoltre, dichiara che "Alcuni servizi per le cripto-attività, in particolare la prestazione di custodia e amministrazione di cripto-attività per conto dei clienti, il collocamento di cripto-attività e i servizi di trasferimento di cripto-attività per conto di clienti, potrebbero sovrapporsi ai servizi di pagamento quali definiti nella direttiva (UE) 2015/2366".

Ritorna il problema relativo all'applicazione, anche in questo contesto, di quanto previsto dalla PSD2, sempreché, ovviamente, si sia in presenza di servizi di pagamento, così come definiti da quest'ultima (e, forse, non è inutile precisare che non tutti i servizi per le cripto-attività elencati in MiCAR integrano gli estremi della PSD2).

Si deve, pertanto, cercar di comprendere quale possa esser il rapporto fra la disciplina contenuta nelle due direttive e quella contenuta nel Regolamento.

Le informazioni che i fornitori di servizi di cripto-attività devono fornire all'autorità competente per ottenere l'autorizzazione sono molto dettagliati e gravosi (art. 59).

Ai sensi dell'art. 66 di MiCAR, i prestatori, quando gestiscono una piattaforma di negoziazione di cripto-attività, scambiano cripto-attività con fondi o altre cripto-attività, prestano consulenza sulle cripto-attività o prestano servizi di gestione del portafoglio di cripto-attività, i prestatori di servizi per le cripto-attività forniscono ai loro clienti hyperlink ai White Paper sulle cripto-attività concernenti le cripto-attività in relazione alle quali prestano tali servizi.

I fornitori devono rendere pubbliche le loro politiche di prezzi, costi e commissioni in un punto visibile del sito.

MiCAR prevede poi obblighi di informazione specifici legati al tipo di servizio e anche obblighi legati alle comunicazioni da dare ai clienti con riferimento alle condizioni per considerare il loro ordine definitivo

A me sembra, nuovamente, che il livello di informazioni copra quanto previsto dalla Direttiva 2002/65/CE e dalla PSD2, quando applicabile.

Non essendoci, però, una precisa esclusione, a me sembra che ancora una volta possano operare le due direttive in punto di recesso.

La disciplina precedente e MiCAR si presentano, dunque, come in parte sovrapponibili e in parte complementari.

Il legislatore europeo ha volutamente seguito, con riferimento agli obblighi di informazione, l'impostazione delle direttive di cui ci siamo occupati in questa sede.

Il rispetto di MiCAR, dunque, determina, con riferimento al profilo degli obblighi di disclosure e di forma, il rispetto anche delle direttive poste a tutela (anche) del consumatore.

Allo stato il recesso resta disciplinato dalle direttive consumeristiche.

Insieme ad altri studiosi, avevo auspicato che il legislatore europeo intervenisse sul punto in sede di eventuale approvazione della Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva 2011/83/UE per quanto riguarda i contratti di servizi finanziari conclusi a distanza e abroga la direttiva 2002/65/CE.

Il legislatore europeo sembra non aver accolto l'auspicio.

Mario Libertini

Il giurista e le nuove tecnologie

Sommario: 1. Lo shock digitale: l'illusione di uno spazio giuridico assolutamente libero. – 2. La fase di assestamento: i giganti del web e la pretesa di autoregolazione; l'intelligenza artificiale e la tutela del segreto. – 3. Verso una crescente regolazione pubblica dei mercati e dei servizi digitali.

1. Lo shock digitale: l'illusione di uno spazio giuridico assolutamente libero

Con la formula "Law and Technology" si trattano una serie di fenomeni caratterizzati dall'impatto di nuove tecnologie, affermatesi negli ultimi decenni. Il campo è sterminato. Questo convegno tratterà approfonditamente molti di questi fenomeni, ormai comunemente riconosciuti mediante proprie formule (*LawTech, FinTech, CorpTech* ecc.). In questa riflessione introduttiva vorrei formulare solo alcune osservazioni generali sull'impatto che le tecnologie digitali, nel loro insieme, hanno avuto non solo sulla cultura e sulla società, ma anche nell'esperienza giuridica.

L'insorgere dei nuovi mercati digitali ha creato uno shock culturale. All'inizio si è intravista, nel nuovo mondo della comunicazione digitale, una nuova dimensione di libertà assoluta, in cui ogni individuo si sarebbe potuto esprimere senza necessità di ricorrere ad intermediari. Inoltre, il mondo digitale presentava una capacità e velocità di innovazione, quali non si erano mai viste nella storia. La "deferenza per l'innovazione"[1], inquadrata nell'egemonia liberistica affermatasi attorno agli anni Novanta del secolo scorso, dopo la caduta dei regimi comunisti, ha fatto il resto. Internet e i nuovi mercati digitali sembravano muoversi in uno "spazio giuridico vuoto", in cui la *rule of law* era sconosciuta, e piuttosto sostituita da una sorta di *rule of the web* (*"The first* rule of the web *is there are no rules";* frase che viene attribuita a Tim Berners-Lee). Si arrivò a formulare una proposta di dichiarazione di indipendenza del Cyberspazio (Barlow 1996) e all'affermazione per cui "Code is Law" (Lessig, 1999).

---

[1] Mi permetto di richiamare M. Libertini, *Digital markets and competition policy. Some remarks on the suitability of the antitrust toolkit,* in *Orizzonti del diritto commerciale,* 2021, 337 ss.

A questa situazione ha contribuito anche la scelta storica del Governo statunitense di conferire la proprietà dei protocolli internet ad una *corporation* privata *no profit* (ICANN), con il vincolo dell'assoluta neutralità della rete (neutralità verso tutte le tecnologie e verso tutti i contenuti). Scelta storica, che ha consentito l'accesso facile ed economico ad un *domain name* da parte di moltitudini di soggetti della più diversa natura.

Questa condizione è stata sostenuta anche da alcune scelte giuridiche pubbliche, in particolare nell'ordinamento statunitense. In tal senso è quella che è stata definita[2] "regola costituzionale del *World Wide Web,* dettata dalla sec. 230 del *Communications Decency Act* statunitense del 1996", che stabilisce l'immunità, per gli operatori del Web, da qualsiasi censura attinente ai contenuti, al contempo riconoscendo loro la facoltà di darsi regole di "moderazione". Regola rafforzata dal *Digital Millenium Act* del 1998 per ciò che riguarda le violazioni del diritto d'autore. L'Europa ha sostanzialmente seguito, fino al recente *Digital Services Act,* questi orientamenti.

Questa ideologia di uno spazio giuridico vuoto, governato da un ordine spontaneo, ha portato all'idea della non vincolatività, nel web, delle regole statali (fossero quelle del diritto d'autore come quelle sulla tutela dei dati personali, come perfino le norme tributarie e penali).

Si è trattato di un'ideologia pervasiva, che non è stata professata solo dalle grandi imprese innovatrici, i c.d. *Web Giants* (in realtà: imprese trasformatesi rapidamente da start-up a colossi), ma è stata condivisa da tanti piccoli operatori del web, dagli *influencer* agli *youtuber,* e dai tanti giovani che hanno realizzato piccoli commerci di oggetti svariati (spesso a contenuto creativo).

Il fenomeno si collega drammaticamente alla crisi delle strutture istituzionali e delle *élites* nelle democrazie occidentali e al diffondersi dell'ideologia populista, con tutti i suoi pericoli. La punta avanzata di questo fenomeno è nel movimento *Cypherpunk.* Ma anche in Italia abbiamo avuto un'esperienza diretta di ciò (si pensi alla "ideologia" di Casaleggio, che è stata all'origine del movimento 5 stelle).

Rimanendo nella dimensione più propriamente giuridica, deve notarsi che si è creata la consuetudine per cui la regola istituzionale può essere vista come un incidente di percorso da minimizzare negli effetti pratici, ma non come un dato vincolante ed orientativo della condotta degli operatori del web. Così, p.e., è considerato normale che *YouTube* (ma la menzione vale come maggiore esem-

---

[2] S. Mannoni – G. Stazi, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio,* Editoriale Scientifica, Napoli, 2021, 44.

pio, perché tale condotta è tipica e generalizzata) cancelli un contenuto nel caso in cui il titolare del diritto lo richieda, ma non svolga alcuna cernita preventiva sull'esistenza di diritti di esclusiva che potrebbe rendere illecita la pubblicazione di quel contenuto.

Naturalmente, tutto ciò non sarebbe potuto avvenire senza la condivisione, più o meno dichiarata, dei poteri pubblici. Ma, accanto a ciò, deve riconoscersi – e questo è un passaggio fondamentale – che il fenomeno non si sarebbe mai realizzato senza un largo consenso popolare (del resto, questo consenso si spiega anche perché siti come Wikipedia o YouTube hanno realizzato grandi operazioni culturali positive, fornendo l'accesso libero, a tutti i soggetti interessati, a grandi banche-dati, anche di elevato livello culturale).

2. La fase di assestamento: i giganti del web e la pretesa di autoregolazione; l'intelligenza artificiale e la tutela del segreto

Superata la fase pionieristica, si è avvertito che, nello spazio, in apparenza giuridicamente vuoto, della rete, si erano innestati fenomeni secondari di enorme importanza e dimensione. Il più noto è la crescita di grandissime imprese (i "giganti del Web"), dotate di un enorme potere di mercato. Fino a pochi anni fa, queste imprese sono cresciute ed hanno agito in una condizione di immunità di fatto dalle norme antitrust.

Ma devono essere segnalati altri fenomeni importanti. Il diffondersi dell'economia digitale ha portato ad un enorme processo di automazione della vita quotidiana e della produzione economica, come anche dell'amministrazione pubblica e della giustizia. Questi fenomeni sono, all'apparenza, meno dirompenti: anche i robot ed agenti artificiali possono essere visti come "cose" oggetto di proprietà (e fonte di responsabilità a carico dei loro proprietari). C'è però anche qui un fenomeno di "evasione" dal diritto istituzionale: gran parte della produzione di AI si svolge sotto la copertura del segreto commerciale, che qui funziona come segreto di fatto, insuscettibile di *reverse engineering*. I processi di *self-learning* dell'agente artificiale sono, in larga parte, inaccessibili agli stessi costitutori dello strumento. Si è diffusa la metafora per cui la produzione di creazioni dell'AI avviene in una *black box*.

Si è quindi verificato un fenomeno sorprendente: il più grande processo di innovazione verificatosi nella storia economica – cioè quello costituito dall'affermarsi dell'economia digitale – è avvenuto senza un ricorso strutturale agli strumenti giuridici fondamentali di sostegno dell'innovazione, quali sono stati i diritti di proprietà intellettuale (in particolare: il brevetto e il diritto d'autore).

In questa prospettiva, le discussioni sulla razionalità o meno della protezione di algoritmi e dati mediante diritti di proprietà, e di proprietà intellettuale in particolare[3], appare irrimediabilmente astratta, a fronte di un'esperienza imponente di copertura di algoritmi e dati mediante il segreto, in una linea di continua evoluzione della struttura degli algoritmi stessi. In sostanza, i tempi di evoluzione degli algoritmi sono così rapidi da apparire incompatibili con i tempi ordinari della costituzione, registrazione e difesa di diritti di proprietà intellettuale[4].

Nel frattempo, si è verificato un terzo fenomeno importante: gli operatori del web, ritenendosi legittimati ad operare in uno spazio giuridico vuoto, si sono autoinvestiti di un potere regolatorio proprio. Le manifestazioni più vistose di questo *trend* sono quelle dei giganti del web con le loro *policy* di selezione dei contenuti e perfino di arbitrato interno. Altrettanto significativa è l'evoluzione verso modalità contrattuali il cui contenuto è interamente determinato dalla grande impresa digitale (così nel *digital advertising*).

Questo fenomeno di regolazione privata si è, a un certo punto, evoluto (senza che venissero meno le precedenti manifestazioni). Correntemente, si discutono ormai tre età della (pur recentissima) storia del web: Web 1, in cui l'inserimento di contenuti nel web era prevalentemente unidirezionale; Web 2, incentrato su fenomeni di comunicazione interattiva (social networks); Web 3, caratterizzato da circuiti chiusi decentralizzati[5].

Quest'ultima fase ha dato luogo a fenomeni nuovi di circuiti chiusi (in cui la *blockchain* è stata la tecnica vincente), con l'immissione in circuito di messaggi crittografati e con l'impiego della tecnologia DLT (*Distributed Ledger Technology*). Ciò ha portato all'affermazione degli *smart contracts* e delle criptovalute.

La dottrina più avveduta ha sostenuto che non esistono ragioni per riconoscere che gli *smart contracts* costituiscano una zona franca rispetto all'applicazione delle norme di diritto generale sui contratti, ma ha dovuto altresì riconoscere che la tecnica impiegata rende difficoltoso o impossibile il ricorso ad alcuni rimedi istituzionali standard [p.e. una dichiarazione di nullità rischia di rimanere ineffettiva e il solo rimedio possibile si concentra sulle restituzioni;

---

[3] G. Muscolo, *Big Data, algoritmi, intelligenza artificiale: perché proteggerli con un brevetto?,* Quaderni di Astrid – Il Mulino, Bologna, 2022, vol. III.

[4] Cfr. M. Dhenne – A. Di Bernardo – A. Gorius – M. Marfè – D. Mohammadian – P. Ollivier, *The Current Ip Framework Still Performing Well In Its Supporting Function of Introducing New Technologies Into the Market?,* in *les Nouvelles – Journal of the Licensing Executives Society,* Dec. 2021, 297.

[5] N. Dabit, *What is Web 3? The Decentralized Internet of the Future Explained,* in *FreeCodeCamp,* Sept. 8, 2021.

il recesso *ex lege* è anch'esso ineffettivo in mancanza di un adattamento (che potrebbe avvenire su base prettamente volontaria) dei *software* impiegati][6].

Questi rilievi pongono un problema fondamentale di politica del diritto: a rigore, un'attività economica che utilizza programmaticamente strumenti tecnici volti ad eludere l'applicazione di norme imperative di diritto dovrebbe essere considerata di per sé illecita e dovrebbe giustificare l'applicazione di misure repressive. C'è però certamente da valutare l'importanza del *trade off* con l'innovazione e la difficoltà di reprimere, o anche solo, regolamentare fenomeni che hanno assunto carattere globale. Tutto ciò dovrebbe portare, comunque, al riconoscimento dell'urgenza di introduzione di meccanismi di regolazione pubblica di nuovi fenomeni, che a loro volta dovrebbero essere costruiti su base sovranazionale.

Questa urgenza si appalesa ancor più se si tiene conto degli interessi dell'utenza della *blockchain*. Vi sono certamente, nell'impiego di questa tecnica, vantaggi di rapidità, certezza, riduzione di costi di transazione, ma vi è anche il rischio elevato di utilizzo per attività illecite. I *cryptoasset* scambiati mediante *blockchain* garantiscono l'anonimato degli operatori e quindi le operazioni di riciclaggio[7]. Su ciò si innesta, poi, un mercato speculativo che ha ad oggetto i *cryptoasset* stessi (e che non meriterebbe, come tutti i mercati puramente speculativi, particolare incentivazione). I vantaggi (rapidità e basso costo delle transazioni) non controbilanciano i rischi. La certezza delle transazioni è un vantaggio, ma crea anche rigidità.

In questa materia, il fenomeno delle criptovalute ha un'importanza centrale. Esso ha dato luogo ad un'esperienza straordinaria, anche sul piano culturale. Ciò perché la pretesa di svolgere una funzione monetaria ha portato le criptovalute ad intrecciare la loro esistenza con una molteplicità di fenomeni della vita reale, ed ha così determinato una serie di casi giurisprudenziali, più che in altri spazi occupati dalle tecnologie digitali. Nel corso dell'ultimo decennio si è formato un *corpus* di casi giudiziari – in materia penale, tributaria, fallimentare, ma anche civilistica generale – che possono essere citati a merito della nostra giurisprudenza e saranno oggetto di apposite relazioni in questo convegno.

Rimane però il problema della regolazione dell'attività in sé. Per verità, non mancano i dati normativi che potrebbero essere applicati estensivamente. P.e., l'art. 50 d.lgs. 231/2007 e s.m.i. vieta, in termini generali, i conti anonimi e l'art. 63

---

[6] Per i punti sopra richiamati v. M. Maugeri, *Smart contracts e disciplina dei contratti,* Il Mulino, Bologna, 2021.

[7] V., p.e., F. Fontana, *Criptovalute e rischi di riciclaggio,* in *Rivista italiana dell'antiriciclaggio,* 2020, 355 ss.

dello stesso d.lgs. dispone, in caso di infrazione, una sanzione amministrativa pecuniaria (dal 20 al 40% del saldo). Inoltre, i fornitori di valuta virtuale e di portafogli virtuali sono tenuti agli obblighi informativi antiriciclaggio. C'è anche una norma (art. 17-*bis,* c. 8-*bis,* d.lgs. 13 agosto 2010, n. 141, sui contratti di credito ai consumatori), che impone ai "prestatori di servizi relativi all'utilizzo di valuta virtuale" l'obbligo di iscrizione al registro dei cambiavalute e la soggezione alla relativa vigilanza amministrativa. E tuttavia, le tecniche di "disintermediazione" proprie della DLT fanno apparentemente scomparire l'esistenza di un soggetto organizzatore del sistema e tendono a mettere in scacco non solo le regolazioni amministrative sopra menzionate, ma anche le nostre regole di responsabilità civile. Può continuare a pensarsi, tuttavia, che una modalità tecnica privata, che rende impossibile l'attuazione di obblighi di legge, comporti un'esenzione dagli stessi? Certamente no, ma la regolazione delle criptovalute – come ha sottolineato in interventi pubblici il presidente della CONSOB Savona – è ancora insufficiente. Le ambiguità e le debolezze della regolazione europea e nazionale delle criptovalute è spesso denunziata[8].

3. Verso una crescente regolazione pubblica dei mercati e dei servizi digitali

La spinta verso una regolazione pubblica avanzata dei mercati digitali si sta tuttavia manifestando, ma, per ora, in una direzione solo parziale.

La spinta più forte è nata dall'osservazione che lo sviluppo dei mercati digitali ha fatto emergere una realtà ben diversa da quella preconizzata nell'ideologia libertaria iniziale. Si sono formati i "giganti del web", dotati di enorme potere di mercato. Le autorità pubbliche hanno favorito la crescita astenendosi dall'intervenire (p.e. nelle *killer acquisitions*) o anche fornendo incentivi per la ricerca industriale (Mazzucato). Tutto per deferenza verso le nuove tecnologie.

Ciò ha portato ad una reazione, che ha invocato interventi contro lo strapotere delle grandi piattaforme digitali e al proliferare di interventi di autorità antitrust e di proposte di nuova regolazione (in particolare, il regolamento europeo *Digital Markets Act* [Reg. 1925/2022/UE).

È in corso una "riscossa dello Stato", come sostengono alcuni[9]? Diciamo meglio: una reazione dei poteri pubblici (in prima linea la Commissione UE)? Apparentemente sì, a livello europeo. E questa reazione dev'essere valutata po-

---

[8] Cfr. M. Tola, *Valute virtuali tra sovranità monetaria e tutela costituzionale del risparmio,* in *Nuove Leggi Civili Commentate,* 2021, 1375 ss.

[9] S. Mannoni – G. Stazi, *Sovranità.com – Potere pubblico e privato ai tempi del cyberspazio,* Editoriale Scientifica, Napoli, 2021.

sitivamente, ma anche tenendo conto che il carattere globale del fenomeno richiederebbe risposte altrettanto globali. Discutibili sono, a mio avviso, le rivendicazioni di autonomia della nostra AGCM. Significativa, e, a mio avviso, degna di attenzione, è la recente decisione del TAR Lazio[10], che ha sospeso la decisione che imponeva rimedi comportamentali ad Amazon per il rischio di una attuazione diversificata di misure differenti a livello europeo e italiano.

Un punto rilevante è che la reazione dei poteri pubblici sembra concentrarsi, per ora, soprattutto sull'azione dei grandi operatori digitali, che sono facilmente individuabili e, pur essendo molto potenti, non sono impermeabili all'intervento pubblico. Deve però riconoscersi che, in realtà, non si ferma qui. La reazione sembra avviata anche a tutto campo, per ciò che riguarda il funzionamento dell'economia digitale. Anzi, è in cantiere un'imponente opera di nuova regolazione. Basti pensare alla proposta di *Data Governance Act* (novembre 2020) e alla più recente proposta di regolamento sull'uso dei dati (*Data Act,* febbraio 2022); a quello sull'impiego dell'AI (aprile 2021), che individua una serie di impieghi vietati ed un'altra di impieghi "ad alto rischio", soggetti a pervasiva regolazione. Per quanto riguarda i *crypto-asset* c'è la proposta di un altro importante regolamento (c.d. MICA: settembre 2020). Il modello organizzativo è quello, ormai standard nel diritto europeo, di una rete di autorità nazionali coordinate da un'autorità centrale europea. Nel complesso, si tratta di un'enorme sfida regolatoria, che dovrebbe maturare nel giro di un paio d'anni e dovrebbe far crescere la statura politica dell'UE.

La reazione sembra insufficiente, invece – come si notava prima in relazione alle criptovalute – a fronte dei fenomeni di massa, realizzati da miriadi di operatori medio-piccoli, che continuano a muoversi come se operassero in uno spazio giuridico vuoto.

[10] TAR Lazio – Roma, sez. I, 10 marzo 2022, n. 1530.

Michele Colajanni

La crittografia, le tecnologie *blockchain* e le molteplici applicazioni

1. Introduzione

L'arte e la tecnica di trasformare le informazioni al fine di renderle ininteligibili sono antiche quanto le più remote civiltà della storia. Non sorprende, quindi, che l'uomo le abbia affinate nel tempo e applicate inizialmente a tutti gli ambiti più critici del governo, quali la difesa e l'intelligence. Con la diffusione dei computer, di Internet e di algoritmi standard di crittografia, l'utilizzo si è diffuso a tutta la società digitale che la sfrutta, talvolta inconsapevolmente, per l'accesso sicuro a tutti i servizi informatici in rete. Al contempo, questa espansione pone molteplici sfide di cui due sono rilevanti per l'obiettivo di questo articolo:

1) la crittografia quale unico mezzo per la tutela della riservatezza e argine alla pervasività del controllo reso possibile dalla società digitale globalmente interconnessa;
2) le applicazioni della crittografia e di altre tecnologie quali mezzi per realizzare sistemi decentralizzati e disintermediati alternativi ai sistemi autoritativi centralizzati.

L'articolo affronta queste domande fondamentali senza l'ambizione di esaurire due dei temi più complessi per la (ri)definizione dei diritti e dei poteri nell'ambito della società digitale e interconnessa in cui viviamo. In particolare, nella Sezione 2 si esamina il tema della controllabilità pervasiva che ogni società digitale rende possibile nonché le diatribe relative agli ostacoli e alle opportunità posti dalla crittografia a tali fini. Nella Sezione 3 si introducono le tecnologie *blockchain*, appartenenti al più vasto ambito dei sistemi basati su registri distri-

buiti. Le relative applicazioni sono trattate nella Sezione 4, a livello di criptovalute con particolare riguardo al sistema Bitcoin, e nella Sezione 5 relativamente a *smart contract* e *organizzazioni autonome decentralizzate* basate su piattaforma Ethereum. Le conclusioni sono sintetizzate nella Sezione 6.

2. Digitalizzazione, controllo e crittografia

Vi sono molteplici tecnologie che hanno rivoluzionato la vita umana, ma nessuna è stata così dirompente e rapida quanto l'informatica. Il perfezionamento e la pervasività dei computer, delle reti e della digitalizzazione di tutta l'informazione continuano a produrre effetti espansivi di tipo esponenziale. I dati in forma digitale e i metodi automatici per la loro acquisizione ed elaborazione consentono a pochi di controllare enormi masse di cittadini-utenti. Una tale efficacia e pervasività di controllo con pochi uomini e molti strumenti non ha riscontro nella storia umana. L'utente, che è il principale fornitore di dati, appare scarsamente interessato alle conseguenze, in quanto percepisce di essere ripagato da una miriade di servizi falsamente gratuiti e apparentemente indispensabili. Ne possono approfittare i grandi provider di servizi digitali e i governi degli Stati che hanno il controllo sui sistemi di comunicazione, di pagamento e delle piattaforme digitali incluse quelle *social*. L'unico vero ostacolo all'acquisizione massiva dei dati è rappresentato dalla crittografia che oggi è utilizzata per l'accesso sicuro a tutti i principali servizi informatici con la conseguenza che più dell'80% delle comunicazioni in rete risultano cifrate. Di conseguenza, se da un lato, si tutela la riservatezza dell'utente rispetto a pervasive campagne di acquisizioni dati, dall'altro risulta più complesso effettuare indagini mediante intercettazioni analogiche tradizionali con la conseguente necessità di rivolgersi ai ben più invasivi *trojan* o "captatori informatici". Da qui emergono discussioni infinite sul valore etico della crittografia che, proprio perché ricorrenti, fanno ipotizzare che talvolta si dichiari di voler risolvere il secondo problema con il vero obiettivo di contrastare il primo. Altrimenti, non vi sarebbe necessità di alimentare periodicamente tale dibattito quando è evidente che il giudizio dipende solo dagli attori in gioco e non dalla tecnologia in sé. Non ci sarebbe, infatti, discussione se dalla parte degli utilizzatori della crittografia vi fossero pedofili, trafficanti di droga e terroristi, e dall'altra le Forze dell'Ordine. Parimenti, non vi sarebbe quando da una parte vi sono giornalisti e attivisti democratici e dall'altra dispotici regimi totalitari che proibiscono e contrastano in modo esplicito ogni forma di crittografia. I dubbi sul significato effettivo della discussione emergono nel momento in cui entrano in gioco le democrazie e i loro cittadini.

2.1. La schizofrenia europea sulla crittografia

Il dibattito emerge periodicamente anche in Europa, dove la crittografia è valutata in modo altalenante. Da un lato, la crittografia viene descritta come lo strumento essenziale per garantire la privacy e la sicurezza della società e dei mercati digitali dell'Europa. Dall'altro, si sostiene che essa svolga un ruolo pericoloso per mascherare attività criminali di diversa natura, che rappresenti un ostacolo alle forze dell'ordine e che quindi vada indebolita. Se da un lato si promulgano iniziative come ePrivacy, Digital Market Act e Digital Service Act che tutelano la privacy dei cittadini e delle aziende europee, dall'altro periodicamente riappaiono scellerate proposte legislative, che non a caso devono schermarsi dietro reati socialmente odiosi, tese a indebolire o violare la crittografia mediante *backdoor* o necessità di deposito di chiavi di cifratura[1]. Non vi è né potrebbe esservi alcun informatico o esperto di cybersecurity a favore di simili proposte, in quanto la crittografia rappresenta l'unica vera barriera di aziende e persone contro i criminali informatici, l'ultima labile difesa della residuale privacy dei cittadini della società digitale contro multinazionali e organizzazioni alla ricerca incessante e redditizia di dati sempre più personali. L'errore europeo è doloso o, nella migliore delle ipotesi, dovuto a scarsa competenza tecnologica in quanto la crittografia moderna, con la potenza computazionale a disposizione di tutti, non si può indebolire: o esiste in forma robusta o non esiste.

Fortunatamente, è la stessa agenzia europea per la cybersecurity ENISA a evidenziare tutti i rischi delle proposte anti-crittografia[2]. Indebolire la crittografia non rappresenta una soluzione in quanto si mettono a rischio e potenzialmente sotto controllo milioni di utenti legittimi, mentre i gruppi organizzati possono sviluppare e utilizzare nuovi strumenti di crittografia e di comunicazione sotterranea che al privato sarebbero impediti. La storia dimostra continuamente che è molto difficile limitare l'innovazione tecnica attraverso misure legislative e che i criminali, a differenza dei cittadini, sono nella posizione migliore per sfruttare tutte le alternative tecnologiche. Inoltre, la percezione dell'esistenza stessa di backdoor può danneggiare e inibire l'innovazione europea e soprattutto può minare le aspirazioni per una società digitale sicura e orientata alla privacy pienamente abbracciata all'Europa. Infine, ENISA ribadisce che le giuste aspirazioni

---

[1] Si faccia, ad esempio, riferimento all'iniziativa n. 2022/0155 del maggio 2022: *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*.

[2] *ENISA's Opinion Paper on Encryption: Strong Encryption Safeguards our Digital Identity,* reperibile all'indirizzo: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption.

delle forze dell'ordine devono essere soddisfatte mediante il ricorso a strumenti mirati e innovativi di infiltrazione e crittoanalisi, come ben dimostra il successo dello smantellamento della rete Encrochat[3] da parte dell'agenzia Europol, il sequestro di wallet di criptovalute e l'arresto di alcuni criminali. Non è, al contempo, accettabile né raccomandabile per gli imprevedibili effetti a cascata sfruttare scorciatoie basate sull'uso di backdoor e sull'indebolimento indiscriminato della crittografia per tutti i servizi e i cittadini europei.

In sintesi, è spiacevole osservare che, al fine di contrastare la crittografia, alcuni rappresentanti di quella stessa Europa, che si fa paladina mondiale della privacy, utilizzano artificiosi espedienti di impatto sociale concernenti pedofili, trafficanti di droga e terroristi, in quanto non hanno la forza politica di porre sul tavolo la vera questione: in una società digitale, uno Stato democratico, pur avendone la possibilità tecnologica, deve esercitare o meno il diritto di controllo di tutte le comunicazioni private dei propri cittadini e non soltanto di quelle dei sospettati o indagati? Domanda complessa che non consente risposte superficiali soprattutto nel momento in cui tutte le piattaforme digitali si espandono a livello globale e hanno come prevalente modello di business la monetizzazione dei dati personali.

2.2. La vena libertaria dell'informatica

I tentativi di contrasto alla crittografia da parte di alcuni rappresentanti dell'Europa e del mondo anglosassone rafforzano la convinzione di taluni cittadini di essere oppressi, controllati e perseguitati dai "regimi" in cui vivono e da non ben definiti potentati economici. Questa è una tragica verità in tutte le dittature e autocrazie moderne in cui il governo ha il controllo sui sistemi di comunicazione, di pagamento e dei servizi digitali. Per quanto riguarda i Paesi democratici e liberali, con molteplici aziende digitali in competizione, è lecito esprimere qualche dubbio. Tuttavia, non importa quanto queste sensazioni siano autentiche o quanto siano causate da disturbi paranoidi di personalità. L'aspetto interessante è che vi siano gruppi sinceramente convinti di tale verità e che, di conseguenza, condividano la necessità di collaborare per contrastare "ogni sistema centralizzato, inevitabilmente oppressore". Nel caso specifico di interesse, risulta rilevante l'evenienza in cui tali gruppi siano costituiti da persone competenti di informatica che, con piena consapevolezza, hanno scelto la crittografia quale strumento per proteggersi, ma anche per provare a proporre alternative organizzative al sistema centralizzato esistente.

---

[3] *Europol smantella una rete telefonica criptata usata dai gruppi criminali,* Corriere della Sera, 11 marzo 2021.

I lavori pionieristici degli anni Ottanta di David Chaum, inizialmente affiliato alla prestigiosa Università di Berkeley a San Francisco e poi a quella di Amsterdam, hanno il pregio di essere caratterizzati da titoli espliciti[4]. A dimostrazione di una vena libertaria alla base di molta ricerca informatica fiorita in California dagli anni Sessanta in poi, è rivelante che i principali articoli siano stati pubblicati sull'autorevole rivista informatica *Communication of the ACM*. Oggi tra i nipoti morali di quei pionieri vi sono gli uomini più ricchi e potenti del pianeta che hanno saputo sfruttare al meglio tutte le possibilità del digitale e dell'interconnessione globale nonché le debolezze di una società tuttora ancorata a princìpi, politiche e norme proprie di un mondo fisico. Tuttavia, senza rifarsi allo spirito libertario fondativo non si comprenderebbero molte realtà no profit dell'informatica che influenzano da decenni il mondo digitale con rilevanti conseguenze socioeconomiche. I movimenti del software open source, l'hacking etico, Wikipedia e Wikileaks, TOR, le Fondazioni EFF, Linux e Apache, gli open proxy, ma anche la lotta permanente alla censura, al ricorso alla crittografia debole, al controllo statale e al diritto di autore contengono un non malcelato desiderio movimentistico per il cambiamento dell'ordine esistente tramite la tecnologia digitale. È da quest'humus che a cavallo degli anni Ottanta-Novanta emergono vari gruppi antagonisti, tra cui Cypherpunk è quello di maggior rilievo per l'ambito di interesse. Il nome, che echeggia ironicamente il filone letterario distopico *cyberpunk*, rileva già un programma politico: lo sviluppo della tecnologia digitale, dei computer personali, di Internet e della crittografia consentono di ipotizzare un futuro senza Stato centrale, controllore e oppressore per definizione, anche se fondato su leggi e regole democratiche. La rilevanza e l'impatto sociale che può avere la tecnologia digitale rispetto al tradizionale mondo fisico è evidenziato con lucidità in due celebri manifesti[5]. I cripto-anarchici rifiutano la violenza come mezzo rivoluzionario in sintonia con Proudhon e anzi non mirano proprio a combattere il sistema esistente, ma a sostituirlo con meccanismi ritenuti più adatti alla società digitale. In estrema sintesi, partono dal rifiutare l'identità anagrafica statale a favore dell'utilizzo di pseudonimi, propongono la sostituzione di sistemi centralizzati (controllabili) con sistemi distribuiti geograficamente non facilmente sorvegliabili, e soprattutto promuovono il rimpiazzo del denaro con moneta digitale crittata. Tutto ciò, si dichiara lucida-

[4] D. Chaum, *Untraceable Electronic Mail, Return Addresses, and digital pseudonyms,* 1981; D. Chaum, *Blind Signatures for Untraceable Payments,* 1983; D. Chaum, *Security without Identification: Transaction Systems to Make Big Brother Obsolete*, 1985; D. Chaum, A. Fiat, M. Naor, *Untraceable Electronic Cash,* 1988.

[5] T. May, *The Crypto Anarchist Manifesto*, 1988; E. Hughes, *A Cypherpunk's Manifesto*, 1993.

mente, porterebbe al fine dello Stato autoritario mediante il collasso del sistema fiscale centrale che sarebbe impossibilitato a tenere traccia delle transazioni finanziarie. Non si pensi a utopici quanto vacui sognatori. Si tratta di persone tecnicamente competenti, ben consapevoli del livello di provocazione della proposta e che in trent'anni si sono mossi con pazienza e meticolosità perpetrando tuttavia i medesimi princìpi fondativi. Da tempo, l'anonimato delle comunicazioni e la decentralizzazione sono sistemi accettati e consolidati dalla società digitale. Pertanto, il nuovo vero attacco al sistema è la creazione autonoma di valuta in quanto va a erodere lo storico potere degli stati di essere l'unica entità autorizzata a battere moneta. Questi aspetti saranno approfonditi nelle prossime sezioni. Per ora, è opportuno sottolineare che spesso si è portati a considerare solo gli aspetti superficiali della digitalizzazione, ad esempio esaltando la possibilità di automazione di alcune attività e la maggiore efficienza nella gestione delle informazioni. In realtà, la rivoluzione digitale determina impatti profondi a tutti i livelli (sociale, legale, economico, gestionale, lavorativo, relazionale) con mutue interdipendenze che ne stanno incrementando esponenzialmente gli effetti. Nel momento di passaggio, con una rapidità mai sperimentata in precedenza, da una società fisica a una digitale e interconnessa, si delineano molteplici sfide, ma anche nuove provocazioni che emergono inizialmente a livello accademico, di tipo sia filosofico sia tecnologico, ma poi con molteplici ricadute concrete. Il dibattito sull'accentramento-decentramento del potere nella forma e nell'organizzazione degli Stati è di antica data[6]. Il modello centralizzato è ben noto e consolidato, e tutti i governi centralizzati hanno caratteristiche simili. Al contrario, i Paesi decentralizzati possono essere molto diversi (dagli Stati federali con ampio grado di autonomia a strutture regionali sotto stretto controllo del governo centrale), ma in tutti rimane un'Autorità centrale riconosciuta convenzionalmente dalle entità partecipanti che non confutano la fiducia nell'Autorità né la sua capacità di rilasciare risorse, attestarne e controllarne il valore, gestire e conservare traccia affidabile di tutte le attività normative. Per motivi operativi, l'Autorità centrale può delegare il potere fiduciario ad altre autorità, come nei contesti federali e poi locali delle municipalità, pur conservando una relazione gerarchica. Tuttavia, nella storia le convenzioni cambiano, come è accaduto per il denaro che è passato da *token* con valore intrinseco a *token* con valore nominale fino all'attuale crescente tendenza alla dematerializzazione. La rivoluzione digitale non può non avere impatti dirompenti.

---

[6] A. de Tocqueville, *La democrazia in America*, 1835-1840; *L'Antico regime e la Rivoluzione*, 1856.

3. Sistemi centralizzati e sistemi distribuiti

Nel momento in cui si passa da una tradizionale società fisica a una digitale e interconnessa, il dibattito su accentramento *vs* decentramento del potere può estremizzarsi in entrambi i sensi. Da un lato vi sono esempi di Paesi non democratici che, grazie alla digitalizzazione di informazioni e comunicazioni, riesce a controllare i propri cittadini con un'efficienza e pervasività mai sperimentata nella storia umana. Dall'altro, la medesima tecnologia consente non solo di ipotizzare, ma di realizzare modelli organizzativi differenti che non tentino neanche di passare tramite un dibattito giuridico-politico. Non per mancanza di volontà quanto per l'attuale impossibilità di conciliare qualsiasi forma giuridica intrinsecamente nazionale a un contesto connaturato all'immaterialità e sovrannazionalità. Di conseguenza, diventa insidioso e dirompente porre la seconda domanda: per il corretto funzionamento di una società (oggi digitale e interconnessa) è indispensabile che i cittadini ricorrano a un'entità centralizzata che svolga il ruolo di terza parte fidata o al contrario possono esistere altri schemi decentralizzati e paritetici in grado di garantire analoghe funzionalità?

La risposta che emerge da tanti anni di attività di ricerca informatica è affermativa. Utilizzando una combinazione di tecnologie crittografiche, di funzioni di *hashing* e di altri complessi protocolli raffinati via via negli anni, possono essere creati schemi non centralizzati in grado di garantire fiducia e autenticità del possesso di una risorsa e delle relative transazioni, oltre ad assicurare un livello di privacy addirittura superiore a quello offerto dall'Autorità centrale. Si dimostra anche la possibilità, prima teorica e poi operativa, di realizzare tra le entità partecipanti un registro digitale distribuito delle transazioni (*Distributed Ledgers Technology* o DLT) con caratteristiche di decentralizzazione, condivisibilità e trasparenza, e soprattutto garanzie assolute di sicurezza in termini di immutabilità e verificabilità dei dati. Vi sono molteplici modi per realizzare un DLT, ma il più noto e diffuso è rappresentato dal sistema *blockchain*, che consiste in un database distribuito in cui i blocchi (contenenti un insieme di transazioni) formano una catena. Ciascun blocco è caratterizzato da un hash, un codice alfanumerico univoco, calcolato sulla base del contenuto stesso. Il blocco successivo inizia con lo stesso hash così da permettere la verifica che le informazioni contenute non siano state manipolate né possano essere manipolate nel futuro. Infatti, non è consentita alcuna modifica dei blocchi esistenti nella catena, ma solo operazioni di aggiunta in fondo, previo consenso da parte dei nodi partecipanti, de facto i computer che fanno parte della rete blockchain. Questi hanno il compito di conservare e divulgare in tempo reale le copie aggiornate delle transazioni effettuate. Ogni volta che un nuovo blocco è generato e aggiunto alla catena, una copia è distribuita a tutti i nodi partecipanti alla rete. La continua sincronizzazio-

ne garantisce che tutti i nodi abbiano la possibilità di avere le stesse informazioni aggiornate. Questo registro pubblico ordinato temporalmente, incorruttibile e a prova di manomissione è la funzione notarile fondamentale che può essere utilizzata per molteplici scopi in sostituzione della fiducia garantita a tutte le parti da una singola autorità centrale riconosciuta come tale.

Tuttavia, nel momento in cui viene a mancare l'autorità centrale, la blockchain deve essere integrata con un ulteriore protocollo che consenta di raggiungere il consenso tra partecipanti che non si conoscono, non hanno stabilito alcun rapporto pregresso di fiducia, possono avere interessi contrastanti e addirittura essere ostili o malevoli. Tra le possibili proposte prese in considerazione per offrire tale garanzia, alla votazione e alla casualità della *proof of stake*, su cui si ritornerà nella Sezione 5.2, si è preferita inizialmente la competizione insita nella cosiddetta *proof of work*. I nodi partecipanti possono competere per "sigillare" un blocco tramite *mining* che nella pratica informatica equivale a dover determinare la soluzione di un problema matematico complesso legato alle caratteristiche del codice hash risultante dal blocco. Purtroppo, ogni scelta ha delle conseguenze, e la decentralizzazione al posto di un'autorità centrale di riferimento comporta inefficienze e costi elevati. Infatti, il mining è un processo risolutivo a forza bruta senza scorciatoie algoritmiche; è computazionalmente molto oneroso, richiede hardware potente e tanta energia, e chi ha più risorse è favorito nella competizione. Dopo la fase pionieristica, sono nati vari colossi internazionali dedicati al mining, quali BIT Mining, Blockchain Technologies, Canaan, HUT, Marathon Digital, Riot Blockchain, Xive Bitmain. Un'inefficienza intrinseca è che solo il "vincitore" del mining viene ricompensato; tutti gli altri concorrenti sprecano risorse. In tempi di costi energetici in continua crescita, nessun Paese cerca di attirare i miner come nel recente passato, e molti addirittura li ostacolano. The Cambridge Centre for Alternative Finance è il centro studi più accreditato per tener traccia dello stato attuale e passato delle attività di mining nei diversi Paesi[7]. Ad esempio, evidenzia che la Cina, che ospitava circa il 50% dell'attività mondiale dei miner, da maggio 2021 ha proibito tali attività al fine di contenere i consumi energetici e il trading speculativo. Da qui, si è verificata una storica e repentina migrazione dei miner verso il Kazakistan che, godendo di surplus energetico, li ha favoriti nell'ipotesi di lucrosi guadagni per il Paese. Dopo pochi mesi, il governo si è dovuto ricredere in quanto nella strategia aveva considerato gli aspetti di generazione energetica, ma non di distribuzione. La rete elettrica kazaka è risultata antiquata e non ha retto alla crescita impetuosa di richiesta energetica da parte dei miner. In conseguenza, si sono verificati black-out conti-

[7] Mappe e informazioni sono reperibili al sito https://ccaf.io.

nui con disservizi riflessi su tutte le altre attività produttive del Paese, fino a scatenare i disordini sociali del gennaio 2022 repressi nel sangue. Di converso, non vi sono stati i benefici fiscali attesi, confermando i rischi parassitari delle attività di mining industrializzato.

È importante sottolineare che tutti i *miner* devono essere nodi, ma non tutti i nodi sono miner, in quanto il primo miner che risolve il problema diffonde la soluzione agli altri. Tutti i nodi partecipanti hanno la possibilità di verificare la soluzione che è, per scelta progettuale accorta, un'operazione semplice e computazionalmente non onerosa. Una volta verificata, il nuovo blocco è aggiunto alla catena che rimane ordinata temporalmente, e il miner può ricevere la sua ricompensa in criptovaluta. Esistono diversi tipi di blockchain, ma l'unica con le vere caratteristiche di indipendenza, anonimato e basata su consenso distribuito è quella definita pubblica e *permissionless*, in cui chiunque può partecipare come nodo. Le altre versioni, private e/o *permissioned*, non sono altrettanto paritetiche e dirompenti, sebbene possano trovare interessanti applicazioni in alcuni settori industriali soprattutto per la gestione controllata di filiere di approvvigionamento.

4. Blockchain per la gestione di criptovalute

Il primo obiettivo, raggiunto dopo vent'anni di ricerche, prove ed errori, e ottenuto anche grazie all'evoluzione tecnologica e alla pervasività delle reti, ha consentito di individuare le tecnologie e i protocolli per riuscire a garantire fiducia tra partecipanti inaffidabili senza il ricorso a un'autorità centrale. Dal punto di vista non solo teorico, un grandissimo risultato le cui ricadute sono ancora in atto. D'altro canto, una volta individuate tali soluzioni, era abbastanza prevedibile che la prima applicazione fosse rivolta alla creazione e alla gestione di denaro che non necessitasse delle funzioni di una Banca Centrale.

Il ruolo degli accademici, in particolare degli esperti di crittografia e di sistemi distribuiti, e dei gruppi cypherpunk è stato tanto determinante quanto raramente sottolineato al di fuori di contesti specialistici[8]. I presupposti e le fondamenta del successo planetario della criptovaluta Bitcoin lanciata nel 2008 arrivano da lontano. DigiCash e Bit Gold sono due dei tentativi più famosi degli anni Novanta. I meriti del protocollo di mining basato su *proof of work* sono da ascriversi principalmente a Hashcash di Adam Back, sviluppato all'inizio non per la gestione di criptovalute, ma per contrastare lo spam e gli attacchi di tipo Denial-of-Service. Il

[8] Usman W. Chohan, *Cryptoanarchism and Cryptocurrencies,* SSRN, 2017 (revisionato nel 2020).

primo libro contabile di tipo DLT che permettesse scambi di valuta in completo anonimato[9] è stato proposto da Wei Dai nel 1998 a sostegno della criptovaluta B–money proprio sulla mailing list cypherpunk. Sebbene B-money non sia mai stato lanciato come strumento valutario operativo, il suo ruolo teorico e tecnico è stato riconosciuto nel celeberrimo articolo[10] da parte del "creatore" della più famosa criptovaluta Bitcoin firmatosi Satoshi Nakamoto, uno pseudonimo che richiama ai princìpi dell'anonimato di questo humus cultural-tecnologico.

Il sistema Bitcoin integra tutte le soluzioni di successo proposte in precedenza: dall'anonimato al *distributed ledger*, fino al mining basato su *proof of work*. Inoltre, con un raffinato algoritmo, il sistema prevede che il numero massimo di *bitcoin s*ia definito a priori (21 milioni) e che la quantità emettibile nel tempo cresca rapidamente all'inizio e poi sempre più lentamente fino a stabilizzarsi intorno al 2030. Definendo un limite massimo, Nakamoto ha creato una moneta deflazionistica destinata ad apprezzarsi nel tempo proprio per la sua rarità. Non tutte le criptovalute hanno un simile limite. Ad esempio, Ethereum non lo prevede, Ripple ha stabilito 100 miliardi, Litecoin 84 milioni. Poiché il mercato complessivo delle criptovalute è stimato in qualche migliaio di miliardi di dollari, rappresenta una micro-percentuale del mercato totale delle valute tradizionali stimato in milioni di miliardi di dollari. Per questo motivo o per sottovalutazione delle possibilità di successo, nel passato le criptovalute hanno impensierito relativamente gli Stati e le Banche centrali dei Paesi democratici, ma fin da subito le Forze dell'Ordine e la Magistratura. Date le peculiarità di anonimato e disintermediazione, molti leciti utilizzatori sono interessati all'incorruttibile funzione notarile abilitata dal registro pubblico distribuito a prova di manomissione. Altri apprezzano la possibilità di trasferimento del valore senza autorizzazione, censura e controlli. D'altro canto, per le medesime caratteristiche, non sorprende che siano diventate anche le valute preferite dai criminali, dagli operatori di riciclaggio ed evasione fiscale, forse da qualche intelligence e dagli speculatori con elevata predilezione al rischio in quanto le criptovalute sono caratterizzate da estrema volatilità e dall'assenza di qualsivoglia sistema per la gestione del rischio. Senza dimenticare che la cupidigia di poco avveduti investitori li sta rendendo vittime di molteplici frodatori che usano le criptovalute come esca per "garantire" interessi improbabili. La New Financial Technology di Silea rappresenta il caso italiano 2022 di una lunga lista internazionale fondamentalmente basate su sche-

---

[9] Definito da W. Dai come un "*anonymous, distributed electronic cash system*", 1998, reperibile all'indirizzo https://nakamotoinstitute.org/b-money/.

[10] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* 2008, reperibile all'indirizzo https://bitcoin.org/bitcoin.pdf.

mi Ponzi aggiornati, che comprende, tra le altre, la fiorentina Bitgrail, la bulgara Onecoin, l'indiana Bitconnect e la rumena Bitclub.

È interessante osservare anche le tendenze e le reazioni che si stanno verificando in molti Paesi. Ad esempio, poiché in Africa le connessioni e gli smartphone risultano più pervasivi e affidabili dei servizi bancari, i trasferimenti e le rimesse di denaro in criptovaluta stanno crescendo esponenzialmente. Controlli fiscali più serrati possono determinare analoghi effetti. Ad esempio, dopo molteplici accertamenti nazionali sui *money transfer* si è notata una riduzione significativa dei trasferimenti di valuta Italia-Cina e una contemporanea impennata delle transazioni in criptovalute verso lo stesso Paese. Impossibile non ipotizzare una correlazione. Alcuni Paesi, tra cui Algeria, Cina, Egitto, Iraq, Marocco, Qatar, Tunisia proibiscono esplicitamente ai privati la compravendita di criptovalute e vietano alle loro istituzioni finanziarie sia di trattare criptovalute sia di fornire servizi di consulenza e supporto a privati e aziende, con sanzioni che arrivano sino alla carcerazione. In altri 42 Stati, il bando è implicito[11]. La crescente tendenza inibitoria non sorprende, in quanto più le criptovalute si diffondono più si comprendono le effettive limitazioni alla sovranità monetaria e all'imponibilità fiscale nonché alla possibilità di esercitare un reale potere di controllo[12]. Attività di contrasto all'anonimato addizionale fornito dai sistemi di mixaggio di valuta, che aggregano molteplici transazioni di criptovaluta, sono iniziate anche nei Paesi occidentali soprattutto per motivi fiscali e di contrasto al riciclaggio[13]. D'altro canto, la sovrannazionalità intrinseca al sistema di criptovalute rende complessa l'applicabilità e l'efficacia di limitazioni previste da norme nazionali.

Il possesso di bitcoin e le operazioni sono effettuate tramite *wallet*, un software installabile su PC, smartphone o chiavetta USB. In alternativa, è possibile usu-

---

[11] Dati reperibili da *Regulation of Cryptocurrency Around the World,* Global Legal Research Directorate, Law Library of Congress, Nov. 2021.

[12] P. Vigna e M.J. Casey, *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order,* St. Martin's Press, gennaio 2015.

[13] Nell'agosto 2022, il Dipartimento del Tesoro statunitense ha improvvisamente inserito Tornado Cash (un'app di mixaggio valuta per utenti della criptovaluta Ethereum) e molteplici indirizzi associati a tale servizio nella lista nera delle organizzazioni tipicamente riservata a terroristi e nazioni ostili. D'altro canto, nella tradizione tecnologica dei colpi e contraccolpi, questa mossa senza precedenti ha dato maggiore impulso a progetti simili di *coin mixing*, quali CoinJoin, BlockBlend e Wasabi Wallet, e ha fatto aumentare le quotazioni della criptovaluta Monero che ha sempre puntato al massimo anonimato *by design*. La vera domanda è se questa del Tesoro rimarrà un'azione chirurgica mirata, se è un "suggerimento" all'autolimitazione per tutta la comunità delle criptovalute, o se addirittura rappresenta l'inizio di una lunga battaglia contro l'anonimato per favorire la fiscalità, ostacolare il riciclaggio e il finanziamento di attività criminali e terroristiche.

fruire di un servizio online di *exchange*. La Direttiva 2018/843 del Parlamento Europeo ha riconosciuto ufficialmente le criptovalute, stabilendo tuttavia che i fornitori di servizi di wallet dovranno applicare controlli sistematici sulla propria clientela per porre fine al regime di anonimato associato a tali monete virtuali. Di nuovo, tale direttiva trova applicazione solo nei confronti dei provider europei, mentre i cittadini del nostro continente possono facilmente continuare a usufruire del regime di anonimato ricorrendo a qualche fornitore extra-europeo. Il wallet è, infatti, identificato esclusivamente da un codice anonimo costituito da un valore alfanumerico tra i 25 e i 36 caratteri, rappresentabile per comodità mediante un QR code. Il wallet non memorizza i bitcoin, ma le chiavi private che dimostrano la proprietà dei bitcoin medesimi. La risorsa da gestire è un token digitale, e il mining consente sia la convalida delle transazioni sia la generazione di nuovi bitcoin; in realtà, oggi, frazioni di questi noti come *satoshi*. Le transazioni sono registrate in un blocco di dimensione massima di 1 Mbyte. La blockchain del sistema Bitcoin rappresenta il registro delle transazioni di criptovaluta. Come ogni blockchain, consente solo l'aggiunta, ma non la rimozione di blocchi e tantomeno la loro modifica. Il codice del wallet è l'unico dato da comunicare per le transazioni. Se il possessore ha l'accortezza di non collegare mai tale identificativo al suo nome o allo pseudonimo usato in altri contesti (vi sono vari esempi di clamorosa superficialità social), vi è garanzia di anonimato. D'altro canto, l'immutabile blockchain tiene traccia visionabile di tutte le transazioni, quindi un solo errore può compromettere l'anonimato di tutte le attività del possessore del wallet. La mancanza di un'autorità terza a garanzia non consente sbagli e l'attenzione preventiva deve essere massima: i trasferimenti di bitcoin non sono reversibili. Se si comunica un codice sbagliato e la transazione va a buon fine, i bitcoin sono persi per sempre. Analogamente, in caso di dimenticanza o sottrazione delle credenziali per accedere al wallet.

Il software alla base del sistema Bitcoin regola anche la difficoltà del mining in modo che siano necessari circa 10 minuti per validare un nuovo blocco. Maggiore è la potenza di calcolo messa a disposizione dai miner, maggiore sarà la difficoltà del problema da risolvere. L'aggiustamento della difficoltà avviene ogni due settimane, quindi ci possono essere periodi in cui il tempo per validare un blocco di transazioni è maggiore o minore rispetto all'obiettivo dei 10 minuti, che rappresenta il tempo medio per le due settimane. Le ricompense per la validazione del blocco e le commissioni delle transazioni contenute nel blocco stesso sono accreditate automaticamente all'indirizzo del miner. Garantire la tempistica di validazione è importante per la politica monetaria del sistema Bitcoin in quanto il processo di mining rappresenta l'unico modo mediante il quale nuovi bitcoin sono messi in circolazione. Mantenendo questi ritmi, il 97% dei bitcoin sarà stato "minato" nel 2029. Poiché il limite di bitcoin che potranno

essere messi in circolo è impostato a 21 milioni, l'ultimo verrà emesso nel 2140. Questo meccanismo fa sì che non esista alcun metodo per immettere nuovi bitcoin più velocemente di quanto previsto dalla politica monetaria (caratteristica che rispecchia la scarsità e la difficoltà "estrattiva"). È di per sé degno di nota che il Bitcoin abbia previsto fin dall'inizio una politica monetaria e abbia progettato e realizzato una solida tecnologia per realizzarla. Va anche tenuto presente che da tempo il Bitcoin e molte altre criptovalute sono uscite dall'iniziale penombra. Bitcoin è quotato ufficialmente, ha il suo codice internazionale BTC ed è definito "sistema di pagamento valutario internazionale". Analoga sorte per le altre principali criptovalute, quali Ether (ETH), Solana (SOL), Avalanche (AVAX), Binance Coin (BNB), Tron (TRX), Ripple (XRP), Litecoin (LTC), che stanno diventando da un lato un'alternativa presa in seria considerazione anche da aziende e fondi di investimento, dall'altro sistemi sempre soggetti a rischi truffaldini o speculativi a causa dell'estrema volatilità. Non è questa la sede adatta per analizzare le migliaia di criptovalute esistenti in quanto è un mondo in continua evoluzione. Ogni analisi rischia di risultare obsoleta al tempo della pubblicazione e certamente nel momento della lettura di questo articolo.

5. Piattaforma Ethereum per la gestione di nuove applicazioni

Il successo di Bitcoin ha stimolato, con obiettivi concorrenziali o integrativi, molteplici iniziative di cui la più degna di nota è rappresentata dal sistema Ethereum. Questo progetto, che va ben oltre l'emissione e governo di criptovaluta, può a tutti gli effetti essere considerato un esempio di utilizzo della tecnologia blockchain per la gestione di una nuova generazione di applicazioni e servizi.

A differenza di Bitcoin, il cui inventore o gruppo di inventori conserva l'anonimato sin dal 2008, Ethereum ha un creatore noto: Vitalik Buterin, uno dei geni precoci che l'informatica talvolta attira e valorizza. Nato in Russia nel 1994, si trasferisce con la famiglia a Toronto nel 1999. Appassionatosi sin da giovanissimo all'informatica, si interessa alle criptovalute e nel 2011 lascia gli studi e fonda *Bitcoin Magazine*. Da qui, matura l'idea di utilizzare analoghi princìpi per creare un sistema che potesse andare ben oltre gli usi esclusivamente finanziari di Bitcoin. A tale scopo, progetta la piattaforma Ethereum e nel 2013, a 19 anni, pubblica il suo articolo-manifesto fondamentale[14]. Tale pubblicazione attira importanti sviluppatori software, tra cui Gavin Wood, Joseph Lubin e Jeff Wilcke, che si uniscono al progetto divenendo

[14] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,* 2014, reperibile in originale all'indirizzo https://coins2life.com/wp-content/uploads/2021/02/Ethereum-whitepaper.pdf o in forma aggiornata all'indirizzo: https://ethereum.org/en/whitepaper/.

co-fondatori della piattaforma Ethereum. Questo gruppo si muove come una tipica startup e nel 2014 avvia una raccolta fondi per finanziare il progetto. Raccoglie circa 31.000 bitcoin che al tempo valevano circa diciotto milioni di dollari e oggi circa seicento milioni (con il cambio a 20.000$ per bitcoin). I partecipanti alla raccolta fondi ricevettero in cambio la valuta di Ethereum nota come *Ether*.

Bitcoin ed Ethereum non sono progetti concorrenti, sfruttano soluzioni tecnologiche simili, ma con visioni, obiettivi e impieghi differenti. In pratica, Ethereum realizza per il software quello che Bitcoin è riuscito a ottenere per la criptovaluta: garantire la fiducia tra parti inaffidabili eliminando l'intermediazione e la necessità di una terza parte autoritativa. Ethereum crea una piattaforma decentralizzata estremamente flessibile per sfruttare la forza della blockchain per una vasta gamma di applicazioni con cui riesce a passare dal concetto di database distribuito di tipo esclusivamente informativo (le transazioni) proprio della DLT alla possibilità di gestire computazioni distribuite che, per le intrinseche caratteristiche di versatilità del software, possono riguardare qualsiasi tipo di applicazione. Ad esempio, mediante la piattaforma peer-to-peer di Ethereum è possibile gestire proprietà di dispositivi fisici (*smart property*) e di risorse digitali *Non Fungible Token* (NFT), supportare complesse applicazioni a sostegno di risorse digitali governabili mediante codice che attua le regole previste (*smart contract*), fino a realizzare futuribili *organizzazioni autonome decentralizzate* (DAO). Ethereum utilizza la sua criptovaluta digitale *Ether* come incentivo motivatore per partecipare alle inizialmente onerose attività di validazione degli smart contract ed eseguire le relative applicazioni. Tuttavia, come detto, non nasce per uno scopo finanziario, ma molto più ambizioso e avveniristico come evidenziato anche dal sito di Ethereum[15] che appare come un frenetico cantiere in continua evoluzione: un segno di vitalità e di prevedibili sviluppi grazie alle profonde competenze informatiche dei fondatori e alla partecipazione di centinaia di migliaia di sviluppatori, tecnici, designer, utenti e appassionati. A differenza della recente industria delle criptovalute che promuove la narrativa libertaria dei gruppi Cypherpunk a fini di marketing senza prestare particolare attenzione ai reali valori fondativi, sebbene non vi siano evidenze di relazioni dirette, Ethereum fornisce gli strumenti tecnologici per realizzare proprio le utopiche visioni dei gruppi Cypherpunk in cui la società possa auto-organizzarsi sulla base di sistemi fiduciari non centralizzati[16]. Ethereum si può ben vedere come una piattaforma distribuita su

[15] https://ethereum.org.

[16] DJ Pangburn, *The humans who dream of companies that won't need us,* giugno 2015, reperibile all'indirizzo: https://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them.

larga scala che opera sulla propria blockchain e che consente la creazione ed esecuzione di applicazioni decentralizzate automatizzando l'esecuzione di ordini precedentemente programmati in *smart contract*. Allo scopo di fornire una piattaforma versatile, Ethereum mette a disposizione il linguaggio di programmazione Solidity (Turing-completo in quanto in grado di implementare qualsiasi tipo di algoritmo) che offre sia funzioni predefinite sia la possibilità di creare nuove funzioni. Gli sviluppatori Ethereum operano su una rete peer-to-peer, sulla quale creano e gestiscono smart contract grazie alle risorse computazionali dei nodi della rete stessa. Chi mette a disposizione la propria potenza computazionale per consentire alla piattaforma di funzionare viene remunerato in Ether. In realtà, il prezzo per la creazione, gestione ed esecuzione di uno smart contract non è misurato in Ether, dal valore troppo elevato rispetto a quanto richiesto dai contratti tipici, ma in *Gwei* (l'analogo di *satoshi* di bitcoin), equivalenti a un miliardesimo di un Ether.

5.1. *Smart contract*

In termini informatici, uno smart contract risulta essere un insieme di regole e politiche ben definite implementate in codice Solidity. Il software è poi memorizzato nella blockchain e può essere utilizzato per regolamentare una transazione tra due o più entità all'interno della blockchain. Il tutto è collegato a condizioni *trigger*: al verificarsi di queste condizioni, si esegue la relativa parte di software. L'esecuzione può attivare nuove transazioni e nuove condizioni. Viene, con la solita enfasi, definito "smart" in quanto il codice è in grado di verificare se determinate condizioni, definite in base al contratto, sono avvenute e, nel caso, eseguire automaticamente le azioni conseguenti nel momento in cui le condizioni previste si sono verificate (con un tipico modello *if then*). Proprio per questi automatismi integrati, gli smart contract possono essere visti come "agenti" software autonomi ospitati dalla piattaforma distribuita di Ethereum che è in grado di eseguirli. La piattaforma si occupa di attuare le regole previste senza alcuno o scarso intervento; pertanto, vi è garanzia che le azioni predefinite avvengano al momento giusto. Quando uno smart contract è invocato da un messaggio o da una transazione, viene eseguito il codice specifico, previo controllo sulla disponibilità del saldo di Ether e della disponibilità sul proprio store delle coppie di chiave/valore che sono necessarie per monitorare continuamente tutte le variabili persistenti. Di conseguenza, non è sempre corretto considerarli come veri contratti da rispettare o a cui attenersi automaticamente, in quanto tutto dipende dall'algoritmo che uno smart contract implementa. Per questo motivo, nella stesura e attivazione di uno smart contract, bisogna essere estremamente precisi e prendere in considerazione tutte le eventualità. Le parti che sottoscrivono il contratto devono scegliere con cura le

condizioni, le clausole e le fonti di dati su cui il contratto è chiamato ad attenersi, in quanto lo smart contract elabora, in maniera deterministica, le informazioni che vengono raccolte all'interno o all'esterno (mediante *oracolo*). In questo modo, si ha la certezza di un'esecuzione sulla base delle condizioni che si sono venute a verificare, escludendo qualsiasi forma di interpretazione, di intermediazione e di ripensamento. Nella realtà pratica, i problemi sorgono proprio per questi aspetti di perentorio determinismo. Ad eccezione di alcuni smart contract estremamente semplici, è molto insidioso assumere che le parti siano aprioristicamente in grado di prendere in considerazione tutte le condizioni e tutte le relative azioni da eseguire nel caso in cui tali condizioni si verifichino. Inoltre, per verificare un contratto prima della sottoscrizione non vi sono molte parti in causa che possono ritenersi in grado di interpretare autonomamente e correttamente codice scritto non in linguaggio naturale, ma in linguaggio Solidity. In pratica, è temerario ipotizzare che l'implementazione dello smart contract concordato venga tradotto in Solidity in modo esatto, senza errori dolosi o colposi di programmazione e soprattutto senza che il software contenga insidiose vulnerabilità sfruttabili da un attaccante informatico. Tutta la storia del software insegna esattamente il contrario.

5.2. Da *proof of work* a *proof of stake*

A differenza di Bitcoin e di altre criptovalute consolidate basate su *proof of work*, Ethereum sta modificando l'idea di base del suo funzionamento dal tradizionale meccanismo di validazione competitivo basato su *proof of work* a quello denominato *proof of stake*. Tale cambiamento dirompente (definito *The Merge*) è previsto per la metà di settembre 2022, e comporterà molteplici vantaggi in termini di maggiore scalabilità e velocità di gestione delle transazioni. Il processo di convalida delle transazioni diventerà molto più semplice e soprattutto eliminerà la concorrenza tra i validatori. Ciò farà diminuire le tariffe degli Ether necessari per le transazioni comportando un vantaggio per gli utenti, ma ridurrà gli interessi degli attuali miner industrializzati. Si prevede che tale cambiamento ridurrà del 90-100% le necessità energetiche necessarie a supportare la blockchain di Ethereum e la sua impronta di carbonio, andando nella moderna direzione della sostenibilità digitale. Solo questo annuncio ha fatto impennare il valore degli Ether. La *proof of stake* è un meccanismo di consenso cooperativo e non competitivo che si basa su un sottoinsieme di utenti volontari della rete. Per diventare validatori (operazione nota come *staking*), gli utenti devono investire bloccando nella blockchain Ethereum almeno 32 Ether. I validatori hanno lo stesso compito dei miner per quanto concerne il consenso basato su *proof of work*: ordinare transazioni e creare nuovi blocchi così che tutti i nodi possano concordare sullo stato della rete. I validatori sono scelti in modo casuale, in parte in funzione di quanti Ether hanno "investito",

e sono responsabili del controllo e della conferma dei blocchi che non creano. La prova richiede l'impiego di molteplici validatori che devono concordare che una transazione è accurata. Una volta che un numero sufficiente di nodi verifica la transazione, questa viene aggiunta alla blockchain e tutti i validatori coinvolti ricevono un premio. Gli Ether stake di un validatore fungono da garanzia e incentivano un comportamento corretto. Un validatore può perdere parte del suo stake se risulta offline e non partecipa alla validazione o addirittura può perdere l'intero stake in caso di collusione intenzionale. La proof of stake comporta una serie di miglioramenti in termini di efficienza computazionale: non occorre molta energia per il mining dei blocchi e tutte le attività sono utili; vi sono minori barriere all'ingresso, in quanto non serve hardware sofisticato né per creare nuovi blocchi né per validarli. Di conseguenza, ci si attende che la proof of stake porti un gran numero di nuovi nodi partecipanti alla rete Ethereum. La necessaria maggiore scalabilità dell'architettura sarà ottenuta, oltre che dalla proof of stake, dall'utilizzo dello *sharding*, un processo informatico ben noto mediante il quale un database viene suddiviso orizzontalmente per ripartire il carico. Nel contesto di Ethereum, lo sharding ridurrà la congestione della rete e aumenterà il numero di transazioni al secondo creando nuove catene, dette shard, che garantiranno a Ethereum più capacità di archiviazione e acceso ai dati, ma che non verranno usate per eseguire codice[17]. Lo sharding permette l'espansione mantenendo la decentralizzazione in alternativa alla necessità di aumentare la dimensione del database esistente che avrebbe reso Ethereum meno accessibile da parte dei validatori. Con le shard chain, i validatori dovranno solo salvare/eseguire i dati dello shard che stanno convalidando e non dell'intera rete (come succede ora), aumentando la rapidità e riducendo drasticamente i costi. Tutte queste iniziative mirano alla scalabilità, alla semplificazione e, in sintesi, al significativo miglioramento dell'accessibilità dell'architettura. Ethereum intende raggiungere un numero potenzialmente illimitato di partecipanti come se fosse una nuova Internet "computazionale" regolamentata da smart contract. Gli utenti dovranno poter eseguire il software Ethereum su un computer portatile o addirittura su uno smartphone, anche perché lo sharding faciliterà l'installazione ed esecuzione dei client Ethereum senza la necessità di affidarsi a intermediari.

5.3. Organizzazioni autonome decentralizzate (DAO)

La strategia di semplificazione tecnologica e computazionale di Ethereum mira a sfruttare la legge fondamentale di Metcalfe, che ricorda come il valore di

[17] V. Buterin, *Why sharding is great: Demystifying the technical properties,* aprile 2021; reperibile all'indirizzo: https://vitalik.ca/general/2021/04/07/sharding.html – Altri dettagli in: https://ethereum.org/it/upgrades/sharding/.

un qualsiasi tipo di interconnessione (fisica, wireless, sociale, servizi) sia proporzionale al quadrato del numero degli utenti partecipanti. Riuscirci estendendo anche le tipologie di applicazioni è una delle grandi scommesse del prossimo futuro del mondo cripto. D'altro canto, la tecnologia blockchain e degli smart contract è estremamente flessibile e consente di decentralizzare e automatizzare qualsiasi attività digitale. L'ipotesi, oggi divenuta realtà, è addirittura di poter fondare delle organizzazioni di beni e persone, definite *Decentralized Autonomous Organization* (DAO), che siano auto-regolamentate mediante uno o più smart contract senza la presenza di un organo centrale. Le DAO offrono proprio i requisiti ipotizzati e desiderati dalle comunità Cypherpunk come trasparenza, decentramento, accessibilità e sicurezza. Rappresentano un nuovo modo per realizzare organizzazioni autonome e autogestite consentendo di unire persone e organizzazioni attorno a un obiettivo o interesse comune. Tali gruppi DAO possono auto-organizzarsi come unità decisionali in modo innovativo rispetto alle inevitabili modalità gestionali gerarchiche delle organizzazioni pubbliche e private tradizionali. Tutte le operazioni dell'organizzazione dipendono da un insieme specifico di regole codificate in uno o più smart contract. I DAO eliminano la necessità di intermediari e delle tradizionali gerarchie nella gestione di un'organizzazione in quanto il funzionamento dipende dal processo decisionale organizzativo collettivo attraverso la governance decentralizzata tramite smart contract. Di conseguenza, le DAO hanno anche un impatto sul modo in cui le organizzazioni possono essere strutturate e sul modo in cui le persone possono essere gestite e valorizzate all'interno delle aziende in termini di premialità e di responsabilità. In effetti, la maggior parte dei problemi e dei conflitti nelle organizzazioni emergono da discrepanze rispetto alle regole definite, ambiguità che gli smart contract impediscono inerentemente. Tuttavia, è anche importante interrogarsi sulle insidiose implicazioni della governance delle DAO prima di trarre conclusioni solo positive sulla loro praticabilità e desiderabilità.

- Il primo limite è sulla fattibilità operativa in quanto tutte le risorse coinvolte devono essere anticipatamente digitalizzate e rese disponibili sulla piattaforma Ethereum.
- Dal punto di vista sociale, c'è da chiedersi se si desideri realmente vivere in una organizzazione o addirittura società deterministica, binaria, senza alcuna sfumatura e interpretabilità, senza possibilità di ripensamenti nell'esecuzione algoritmica di tutte le azioni previste e prevedibili, e senza alcuna possibilità di ricorrere a un avvocato o a un giudice per tutelarsi nel caso di scenari imprevisti. Una prospettiva che si avvicina pericolosamente ad alcuni scenari distopici della letteratura.
- La governance decentralizzata nei DAO si basa principalmente su meccanismi di voto e sul consenso dei membri del DAO il cui potere è determinato in

funzione del numero di token posseduti. Sebbene le DAO abbiano lo scopo di garantire un'accessibilità senza limitazioni, un gruppo specifico di investitori può accumulare quote importanti di token DAO e ottenere un elevato potere di voto e di veto anche relativamente a cambiamenti delle regole o all'introduzione di nuovi smart contract.

- Infine, le organizzazioni autonome decentralizzate possono rivelarsi un incubo normativo, soprattutto a causa della mancanza di regole e regolamenti definiti per la tassazione e la gestione delle DAO. Non essendoci alcuna singola entità responsabile di tutte le decisioni dell'organizzazione, è abbastanza difficile attuare norme civili e penali per le DAO.

Va, tuttavia, segnalato che iniziano a esservi interessanti tentativi per fornire un supporto legale a questo tipo di organizzazioni[18], come previsto anche da altri analisti[19]. Altre iniziative emergono a livello di singoli stati federali. Il Wyoming, con un emendamento alla propria legislazione, è risultato il primo stato a riconoscere le organizzazioni di tipo DAO. La nuova legge, in vigore da luglio 2021, ha riconosciuto la DAO come una nuova forma di società a responsabilità limitata, al punto che alcuni l'hanno definita una mossa per fare del Wyoming "il Delaware del digitale". Sono seguiti il Vermont e il Tennessee ed è probabile che altri procederanno lungo questa strada anche in Asia.

Ad oggi, queste strutture organizzative del tutto innovative trovano crescente impiego nello svolgimento di qualche migliaio di attività di impresa (in realtà, a settembre 2022, circa 230 realmente attive) con qualche milione di partecipante. Per questo successo crescente, le DAO sono considerate il prossimo grande passo nell'evoluzione della rete, talvolta definita *Web3*, che sta anche provando a integrarsi con i molteplici mondi virtuali degli NFT e del metaverso in una recente *Open Metaverse Alliance for Web3* (OMA3)[20]. Indipendentemente dai giudizi etici e giuridici, va preso atto che esiste un mondo tecnologico in incredibile fermento, dove convivono giovani e big player digitali, che si sta sviluppando nel disinteresse della società, ma anche di gran parte della politica, dell'economia e

---

[18] M. Jennings and D. Kerr, *A Legal Framework for Decentralized Autonomous Organizations – Entity Features and Entity Selection,* 2021; reperibile agli indirizzi: https://a16zcrypto.com/wp-content/uploads/2022/06/dao-legal-framework-part-2.pdf e https://a16z.com/2022/05/23/dao-legal-frameworks-entity-features-selection/; Miles Jennings and David Kerr, "How to pick a DAO legal entity", 2022, reperibile all'indirizzo: https://a16zcrypto.com/dao-legal-entity-how-to-pick/.

[19] Z. Smith, *The Legal Status of Decentralized Autonomous Organizations: Do DAOs Require New Business Structures? Some States Think So,* The Heritage Foundation, giugno 2022; reperibile all'indirizzo: https://www.heritage.org/government-regulation/commentary/the-legal-status-decentralized-autonomous-organizations-do-daos.

[20] https://www.oma3.org/.

del diritto. Sebbene alcuni analisti siano scettici sulle possibilità di reale successo di simili iniziative, non è da escludere l'evenienza che il mondo "tradizionale" si scoprirà ancora una volta in ritardo a inseguire e limitare con strumenti inadeguati l'ancor più incontenibile e difficilmente regolamentabile mondo digitale del prossimo futuro.

6. Conclusioni e prospettive

Dagli antichissimi algoritmi e protocolli crittografici riservati a poche élite si è arrivati alla possibilità di utilizzo quotidiano e generalizzato della crittografia nell'ambito della società digitale. Questo strumento è l'unico mezzo di tutela della riservatezza dei dati dei cittadini rispetto a controlli pervasivi, ma crea difficoltà alle indagini, e pertanto è spesso oggetto di insidiose offensive anche in Europa.

Inoltre, sulla base di protocolli crittografici e di registri digitali distribuiti quale la blockchain, si stanno realizzando servizi digitali innovativi in cui le parole d'ordine prevalenti sono anonimato, decentralizzazione e regolamentazione algoritmica. Sebbene più note, le criptovalute rappresentano una parziale quanto rilevante applicazione. Ancora più dirompenti dal punto di vista economico e giuridico potrebbero risultare i cosiddetti *smart contract* e le *organizzazioni autonome decentralizzate*.

Tra le molteplici ricadute, un aspetto importante che si sta valutando è la sostenibilità di tutte queste cripto iniziative. Sebbene alcuni dei grandi gruppi stiano provando a impegnarsi con relativo successo nel *green mining*, in tempi di costi energetici elevati, si mette in discussione la sostenibilità stessa dell'impianto della blockchain e della validazione competitiva insita nella *proof of work* delle blockchain orientate alle criptovalute tradizionali[21]. Per questo motivo, la ricerca sta valutando soluzioni più eco-sostenibili inclusa la validazione basata su *proof of work*. Tra le tante iniziative, molteplici motivazioni fanno ipotizzare che Ethereum sia la piattaforma destinata ad avere maggiori impatti nel prossimo futuro. La considerazione nasce da molteplici osservazioni: non si limita alla gestione di criptovalute; a differenza di altri sistemi stabilizzatisi, dopo dieci anni, Ethereum è ancora in continua evoluzione da molteplici punti di vista: tecnologico (scalabilità e miglioramento della velocità di gestione delle transazioni), energetico (passaggio da *proof of work* a *proof of stake*), accessibilità (possibilità di un maggior

[21] *There is not enough energy in the whole world to power a decentralized finance ecosystem on the scale that blockchains want.* [Bloomberg, luglio 2022].

numero di utenti e di validatori grazie alla necessità di minori requisiti hardware), e soprattutto applicativo (per ora, smart contract, NFT, DAO, ma anche quant'altro la fertile mente degli sviluppatori continuerà a ideare).

In sintesi, lo slancio del cambiamento tecnologico sta accelerando con rilevanti conseguenze sociali, economiche e legali. Costruire un futuro digitale maturo richiede di modificare e rimodellare gran parte delle modalità con cui abbiamo operato per secoli. E occorre agire con rapidità per non trovarsi a rincorrere *metaversi* che stanno diventando mondi irraggiungibili a norme e princìpi, con rischiose conseguenze per gli stessi partecipanti.

Ugo Bechini

Blockchain, questioni giuridiche

Sommario: 1. Introduzione. – 2. Questioni giuridiche.

1. Introduzione

Sono particolarmente onorato di prendere la parola in questa prestigiosa sede, ed è uno speciale privilegio che il *panel* sia presieduto dalla più illustre degli specialisti nostri, la professoressa Giusella Finocchiaro. Solo il suo grande garbo fa sì che tale presenza non si trasformi in un motivo di imbarazzo: a ben vedere, quel che sto per fare è l'equivalente di un palleggio sotto gli occhi di Cristiano Ronaldo.

Il mio incipit La farà anzi senz'altro dubitare dell'opportunità dell'invito rivoltomi, e del quale ringrazio di cuore. Inizio dicendo: *ventuno*.

È il prodotto di 3 per 7, ovviamente. Che dire invece di 92.648.497? Arrivare al risultato (7.621 x 12.157) non è lavoro da poco, mentre l'operazione inversa, anche con la più banale calcolatrice incorporata nel cellulare, sarà questione di un attimo. Lavorando con numeri composti da centinaia di cifre, come si fa nelle applicazioni correnti, la moltiplicazione resta eseguibile in qualche decimo di secondo, mentre l'operazione inversa è compito mostruoso, misurabile in mesi di attività di un grande calcolatore. È probabile che con il *quantum computing* la cosa sia destinata a cambiare in termini quantitativi, anche se non dal punto di vista concettuale (non direttamente, almeno).

Questa asimmetria (si parla di *one way functions*, funzioni matematiche "a senso unico") è il mattoncino sulla quale si basano moltissime applicazioni con cui anche noi giuristi abbiamo acquisito familiarità negli ultimi decenni: basti citare la firma digitale, l'accesso protetto ai siti web, la Blockchain. La comune origine le porta tra l'altro a condividere una caratteristica: la controintuitività. Non è d'immediata percezione come Tizio possa custodire un registro e nel contempo gli sia impossibile alterarlo. O come sia possibile possedere tutti i dati che consentono di controllare se una firma è vera, senza poter provare ad imitarla. O come, senza aver preventivamente convenuto un codice riservato, Trenitalia possa leggere il numero della mia carta di credito ed un malfattore no, anche se intercetta tutti i dati che Trenitalia ed io ci scambiamo.

Da questa generalizzata controintuitività[1] discende un importante corollario: del tradizionale buonsenso, allenato su situazioni tradizionali, in questo campo è meglio non far uso. Ragionamenti del tipo: *con i documenti cartacei è così, quindi…* sono quasi sempre l'anticamera del disastro.

Una minima digressione che mi sta molto a cuore. Scimmiottare nel mondo digitale *i gesti* tradizionali non conduce da nessuna parte. Occorre replicare, e se possibile migliorare, *le sicurezze* del mondo cartaceo. Si sente talora argomentare: visto che ormai tutti usano Internet, bisogna poter votare o vendere un immobile via rete. Un approccio a mio modesto avviso completamente sballato: se si può ricreare in Rete il livello di sicurezza che i contesti tradizionali ci hanno sinora garantito, benissimo, ma dato che talora così non è, in campana.

2. Blockchain, questioni giuridiche

La Blockchain, dunque[2]. Ometto ogni descrizione che sarà offerta in modo più adeguato da altri relatori[3]. Ai presenti fini basti dire che tale tecnologia è in grado di

---

[1] Che non riguarda solo i giuristi, o in generale chi manchi di un background matematico. Questa tecnologia fu scoperta nei laboratori dei servizi segreti britannici, e nonostante il suo formidabile interesse militare, i responsabili dell'epoca si risolsero alla fine ad accantonarla: a causa della sua controintuitività si temeva contenesse una falla logica sfuggita agli analisti. La storia (che, lo si creda o meno, ha un momento davvero commovente) è narrata da S. Levy in *Crypto: how the code rebels beat the government, saving privacy in the digital age*, Viking, New York 2001, p. 313.

[2] Chi scrive si fa gran vanto di aver suggerito insieme a Sabrina Chibbaro, in un articolo apparso nel 2013 sulla *Rivista del Notariato* (p. 276, in coda a nota 13) come *soluzioni crittografiche simili a quella che sta a fondamento (ad esempio) del sistema Bitcoin* possano consentire il trasferimento di posizioni giuridiche in forma digitale anche senza avvalersi di un'autorità centrale come Montetitoli. La perifrasi in corsivo (o meglio: quella che appare oggi come una perifrasi) è dovuta al fatto che, all'epoca, il termine *Blockchain* non era ancora entrato nell'uso (in letteratura tecnica era sporadicamente apparso *block chain*, staccato). Per quanto microscopico, è probabile che si tratti del primo riferimento alla Blockchain nella letteratura giuridica italiana. Sono trascorsi solo nove anni, ma a dar retta a Bill Gates potrebbero valere per ventisette, o forse ottantuno. Bill Clinton ha infatti raccontato che il fondatore di Microsoft, in un colloquio, ebbe a sostenere che l'informatica viaggia tre volte più veloce dell'industria tradizionale, che a sua volta sarebbe tre volte più veloce del settore pubblico. *Noi due*, concluse Gates rivolgendosi al Presidente degli Stati Uniti d'America allora in carica, *siamo fuori sincrono a fattore nove* (out of sync by a factor of nine: *Bill Clinton, The Debriefing,* in *Wired, December 2000, https://www.wired.com/2000/12/clinton-2/).*

[3] Segnalo, per chi ha familiarità con l'inglese, un'eccellente trattazione di taglio accademico, assai più vasta ed approfondita della presente: è quella di Benito Arruñada, docente presso la prestigiosa Università Pompeu Fabra di Barcellona: *Blockchain's Struggle to Deliver Impersonal Exchange,* in *Minnesota Journal of Law, Science & Technology*, 2018, 19, 55-105. Il lavoro è reperibile online presso https://ssrn.com/abstract=2903857 o http://dx.doi.org/10.2139/ssrn.2903857, e lo raccomando vivamente a quanti desiderassero approfondire il tema, anche per la ricchezza dell'apparato di note. Le conclusioni cui approda Benito Arruñada sono analoghe a quelle qui proposte.

mantenere in modo più che affidabile quel che promette: creare, senza l'intervento di un'autorità centralizzata, un sistema di registri capaci di mantenere traccia indelebile ed immodificabile di determinate operazioni che possono riguardare monete virtuali o qualunque altro oggetto. La Blockchain crea fiducia dal nulla, senza alcun bisogno che i partecipanti al sistema abbiano ragione di fare affidamento l'uno sull'altro, o semplicemente che si conoscano. Più controintuitivo di così...

La Blockchain conserva dati, non li crea. In qualche caso questo non è un problema. Una valuta digitale esiste solo sulla Blockchain; non ha dunque senso chiedersi se il dato che colà rinvengo corrisponda alla realtà. *Il dato è il bene*.

Pensiamo invece ad un possibile utilizzo in campo immobiliare. Blockchain non andrà a sostituire il Giudice od il Notaio, che producono i dati destinati ad alimentare l'archivio, ma il Conservatore dei Registri Immobiliari. C'è un'emergenza in corso che lo raccomandi? Non mi risulta[4].

Non sempre è così. Un esempio. Nella prima metà del 2018 fece notizia la decisione del *Lantmäteriet*, i registri immobiliari svedesi, di valutare l'adozione della Blockchain. Approfondendo appena un poco[5] si apprendeva però che quei registri versano in uno stato penoso, anni luce indietro rispetto all'Italia: l'aggiornamento ha mesi di ritardo, non accettano documenti in forma elettronica[6] e via dicendo. Trovandosi a XXI secolo inoltrato in queste condizioni, e non potendosi contare in Svezia su notai appartenenti ad una delle grandi famiglie del notariato mondiale, potrebbe in effetti essere una buona idea adottare un

---

[4] In oltre un quarto di secolo di attività come notaio non ricordo un solo Cliente che mi abbia rappresentato, neppure in via di remota ipotesi, la preoccupazione che un Conservatore potesse falsificare a suo danno le risultanze dei Registri Immobiliari.

[5] Un buon articolo è quello di S. Anand apparso sul *Wall Street Journal* il 6 marzo 2018: *A Pioneer in Real Estate Blockchain Emerges in Europe*.

[6] A titolo di confronto, i registri italiani hanno livelli di aggiornamento che si misurano in ore ed accettano sistematicamente titoli digitali sin dall'inizio del corrente secolo: sia consentito all'uopo il rinvio ad un volumetto (*Il Modello Unico Informatico*, IPSOA, Milano 2011) curato da Gea Arcella, Valerio Auriemma, Sabrina Chibbaro, Marco Dolzani, Vincenzo Gunnella, Michele Nastri, Caterina Valia e da chi scrive. Mi è stato spesso fatto osservare, soprattutto in occasioni congressuali negli USA, come sia in definitiva poco credibile una simile rivendicazione d'efficienza da parte di un Paese come l'Italia, non particolarmente rinomato (per amor di Patria uso questa formula) per il rispetto della legge. Tale approccio mi pare sia da capovolgersi. In Svezia, ove la legalità è parte integrante della cultura locale, si possono tutto sommato sopportare (ma sino a quando?) registri poco efficienti; altrove è preferibile che gli scambi siano presidiati da sistemi inflessibili. Sia detto col massimo rispetto (ed in fondo non faccio altro che apparentare i Paesi che sto per citare al mio…) ma non credo sia un caso se Colombia e Moldova vantano sistemi informatici tra i più avanzati al mondo per la verifica dei documenti destinati alla circolazione internazionale (la cosiddetta *e-Apostille*); inutilmente si cercherebbero analoghe infrastrutture in Svezia, Svizzera o Germania.

sistema integralmente nuovo (basato, perché no, su Blockchain), che istituisca in modo creativo un'innovativa rete di *Gatekeepers*. Definirlo un caso pilota mi sembra però fuorviante, se non si chiarisce il contesto; l'invito, rivolto ai Paesi che hanno l'unica colpa di possedere sistemi funzionanti, a gettarli alle ortiche, mi pare poi meritevole solo di un secco rinvio al mittente.

Se invece qualcuno pensa di sopprimere Giudici o notai nel nostro Paese, è ipocrita farsi scudo della Blockchain. Si proponga pure, se lo si desidera, di eliminare il titolo autentico per la trascrizione, accontentandosi della firma digitale, e si lascino in pace gli incolpevoli Conservatori. Grava però sui proponenti l'onere di dimostrare come si possa replicare senza pubblici ufficiali lo stesso livello di sicurezza cui siamo abituati, quando in altre esperienze è sufficiente un minore livello di qualificazione dei notai (penso qui in particolare agli Stati Uniti[7]) a creare una situazione terribilmente incerta. Quasi tutti gli acquirenti a stelle e strisce si dotano infatti di una costosa assicurazione (la *title insurance*) e richiedono i servizi aggiuntivi di un avvocato[8]. Il tutto con costi che quasi sempre eccedono quelli di un notaio europeo, che è invece tutto ciò di cui hanno da noi bisogno gli acquirenti di immobili.

Casi particolari possono raccomandare soluzione particolari, come nella repubblica ex sovietica della Georgia, i cui leaders ritengono probabile un'invasione russa[9], prima o poi, e sanno che molti immobili sarebbero in tal caso assegnati ai collaborazionisti locali. L'idea è dotarsi di una Blockchain con molti nodi, uno dei quali installato in Georgia, certamente, e gli altri in Svizzera, Germania, USA, Francia, Italia, Giappone, Olanda eccetera. Quando arrivano i russi, ragionano i georgiani, noi distruggiamo il nodo locale; quando se ne vanno, recuperiamo i dati ante invasione dai nodi stranieri e ripartiamo da lì. Quel che si dice avere le idee (tragicamente) chiare. Ma, di nuovo: è un problema di conservazione del dato.

I motivi per preferire una Blockchain non debbono necessariamente essere così drammatici. Se ad esempio una serie di operatori del mondo dello *shipping*, con base in luoghi diversi come EU, USA e Cina, intendono varare un sistema per tracciare i containers, nessuno tra loro può ragionevolmente proporsi come il Conservatore della situazione, l'unico detentore del dato informatico destinato a

---

[7] Nel 2008 alla redazione nel *New York Daily News* furono sufficienti novanta minuti di lavoro per trasferire la proprietà dell'Empire State Building nei registri immobiliari. I giornalisti indicarono come testimone della stipula Fay Wray, l'attrice che King Kong tiene in mano sul celebre grattacielo, e come notaio il rapinatore Willie Sutton: https://www.nydailynews.com/news/money/90-minutes-daily-news-steal-empire-state-building-article-1.353477.

[8] Si veda F. Rizzo, *Acquisto di un bene immobile negli Stati Uniti: procedimento e costi*, www.federnotizie.it/acquisto-di-un-bene-immobile-negli-stati-uniti-procedimento-e-costi/.

[9] Mi è capitato spesso di presentare il caso, ma in occasione di questa relazione a Castel Capuano l'ho fatto col cuore pesante: era trascorso un mese appena dall'invasione russa dell'Ucraina.

far fede tra le parti. Blockchain appare in un simile contesto come un'eccellente soluzione, una sorta di Ginevra (nel senso della città) dei tempi della Rete.

Venendo più vicino a noi: si può pensare ad utilizzare la Blockchain per gestire flussi di dati in cui intervengono operatori eterogenei. È il caso dei decreti ingiuntivi, su cui hanno voce in capitolo Giudici, Cancellieri, Ufficiali Giudiziari, Avvocati e Notai. Niente da eccepire in via di principio: resta però da capire perché non si possa installare presso la Cassazione, il Ministero della Giustizia od il Consiglio Nazionale del Notariato un bel sistema centralizzato, intrinsecamente più economico, più facile da manutenere e meno energivoro[10]. Qualcuno dovrebbe insomma spiegare in modo persuasivo perché non ci si possa fidare del Palazzaccio, di via Arenula o di via Flaminia[11].

Vorrei dedicare la seconda parte del mio intervento ad una vicenda di alcuni anni fa, che trovo di valenza giuridica non banale: il caso *TheDAO*.

Se Tizio loca la sua casa al mare per il mese di agosto, non sarà considerato troppo paranoico se, incontrando il suo avvocato, gli chiederà cosa si debba fare laddove l'inquilino al primo di settembre non abbia ancora levato le tende. Se invece, titolare di un Bancomat con limite di prelievo di 100 euro, chiederà in quali conseguenze legali possa incorrere in caso di prelievo di 200 euro, sarà giudicato almeno un po' bizzarro. È lo sportello automatico, o meglio il software che lo governa, a rendere impossibile un prelievo superiore al tetto.

Dato però che l'avvocato, da buon giurista, non ha fiducia illimitata né negli uomini né nelle loro creazioni, che si chiamino software od hardware (né nella legge, se è per questo) immaginerà che il software abbia un bug, che l'hardware si guasti, oppure che vengano caricati per errore biglietti da 100 euro nel cassetto delle banconote da 50, e darà le risposte del caso. Non pochi tra gli informatici ritengono però che questi rischi siano trascurabili, rispetto all'incertezza che regna nei rapporti giuridici governati da strumenti tradizionali. Ed alcuni tra loro crearono *TheDAO*[12].

---

[10] La necessità di condurre in sincrono una pluralità di macchine reca di per sé tali conseguenze.

[11] Ad essere pignoli bisognerebbe menzionare una traversa, via Gravina, ove una recente palazzina a basso impatto energetico, appositamente realizzata, ospita i servizi informatici del notariato italiano ed una parte di quelli del notariato europeo.

[12] Si può forse ricavare un'idea di massima delle aspettative che i guru della materia riponevano in *TheDAO* da questo brano di A. Cleary da *Here Is How The DAO Will Soon Become The Greatest Threat Banks Have Ever Faced*, in *frontera.net*, 25 maggio 2016: [...] *the DAO solves the principal-agent problem – which is the source of almost all mismanagement in traditional corporate and fund management structures. By removing delegated power from directors and placing it directly in the hands of owners the DAO removes the ability of directors and fund managers to misdirect and waste investor funds. The people who dislike this are, of course, the directors and fund managers who greatly enjoy their current privilege of using the money raised from investors without having to fully account for it – power without responsibility.*

DAO, come termine generico, sta per *Decentralized Autonomous Organization*. L'esempio prototipale, risalente all'aprile 2016, è noto per antonomasia come *TheDAO*. Si trattava di un sistema online di investimento governato solo da un software (rectius: *consistente* solo in un software![13]) privo di sedi fisiche o di dirigenti umani; una sorta di SICAV robotizzata; gli investimenti da farsi col capitale raccolto erano decisi dagli investitori per votazione. Il sistema era installato su Ethereum, una piattaforma Blockchain, ed i pagamenti venivano eseguiti in una criptovaluta nota come Ether. Tutte le regole di funzionamento del sistema si assumevano[14] incorporate nel software. Ne discendeva che le operazioni eseguibili sul sistema non potevano dirsi lecite od illecite, regolari od irregolari, ma solo consentite o meno dal software[15], un po' come nell'esempio appena proposto del Bancomat. L'incarnazione perfetta di una fortunatissima formula di Lawrence Lessing, *Code is Law*[16].

Senonché il software di *TheDAO* un difetto lo aveva, e di quelli clamorosi: non aggiornava istantaneamente il saldo dopo ogni prelievo. Agendo rapidamente, era quindi possibile prelevare la propria giacenza moltissime volte. Il guaio venne rilevato a poco più di un mese dal lancio, tra maggio e metà giugno 2016, ma che fare? Una Banca tradizionale avrebbe potuto bloccare il sistema in attesa

---

[13] Si potrebbe a questo punto discorrere di *smart contract,* ma non amo l'espressione, soprattutto in quanto designa una figura che non è né *smart* né *contract*, come dimostra S. Chibbaro in *Blockchain e smart contract*, agendadigitale.eu 8 marzo 2019. Colgo l'occasione per ringraziare l'Autrice che mi segnalò la vicenda di *TheDAO* quando ancora era in svolgimento.

[14] Nel materiale esplicativo di *TheDAO* poteva leggersi: *Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code* [...] Brano riportato da R. Morrison, N.C.H.L. Mazey e S.C. Wingreen a p. 7 di *The DAO Controversy: The Case for a New Species of Corporate Governance?*, paper pubblicato il 27 maggio 2020 da *Frontiers in Blockchain*, www.frontiersin.org.

[15] La questione si pone in termini diversi quando, nell'implementare informaticamente una procedura disciplinata dalla Legge, il software non consente operazioni che la norma non escluderebbe. Col *Caso Grosseto* il notariato italiano ebbe ad affrontare la problematica quasi trent'anni fa: Tribunale Grosseto, 31 maggio 1993, in *Rivista del Notariato*, 1998 (*sic*), p. 1243.

[16] Il programma informatico è la legge; *Code is Law* è anche il titolo di un suo articolo apparso il primo gennaio 2000 sull'*Harvard Magazine*, dal quale traggo questo frammento, che mi pare dimostri come allo studioso americano debba essere riconosciuto un realismo ed un'onestà intellettuale che non sempre si riscontrano nei contesti in cui la sua celeberrima espressione viene osannata: *For here's the obvious point: when government steps aside, it's not as if nothing takes its place. It's not as if private interests have no interests; as if private interests don't have ends that they will then pursue. To push the antigovernment button is not to teleport us to Eden. When the interests of government are gone, other interests take their place. Do we know what those interests are? And are we so certain they are anything better?*

di un rapido aggiornamento software, ma qui non vi era alcuna porta cui bussare. Ogni fan della Blockchain che si rispetti vi dirà che è impossibile fermare una Blockchain una volta lanciata; in termini generali è forse un'esagerazione, ma per *TheDAO*, almeno in quel momento, fu proprio così, ed il software difettoso continuò a funzionare com'era.

Il 17 giugno 2016, come ormai ben prevedibile, un utente sfruttò abilmente la vulnerabilità eseguendo prelevamenti a raffica per un totale di circa 50 milioni di dollari oltre la disponibilità di conto, circa un terzo del patrimonio di *TheDAO*, la cui comunità entrò comprensibilmente in fibrillazione. Ed a quel punto accaddero almeno due cose interessanti per un giurista.

L'anonimo autore dell'operazione (o qualcuno che la rivendicava) si rivolse formalmente alla furibonda comunità degli utenti di *TheDAO*, protestando la correttezza del suo operato. Non s'era detto che *Code is Law*? Se il software mi ha consentito di farlo, vuol dire che si poteva fare. Si dichiarò anzi deluso da quanti lo definivano un ladro[17].

Non meno interessante fu la reazione della comunità. La maggior parte degli utenti concordò un'operazione tecnicamente detta *fork*: decisero di congelare la Blockchain originaria, riportare indietro l'orologio ad un momento anteriore all'esecuzione dell'operazione in discussione, e ripartire da lì con una nuova catena.

Uno dei fondatori di *TheDAO*, Christoph Jentzsch, dando prova di possedere ampie scorte di faccia tosta o serie carenze sul piano dell'educazione civica (o forse entrambe) scrisse: *Although some do question the analogy "code is law". I do not. We just found out that we have a supreme court, the community!*[18] E ne andava pure fiero: il suo articolo si intitolava *What an accomplishment!* (Che successo!)[19].

---

[17] *I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank The DAO for this reward [...] I am disappointed by those who are characterizing the use of this intentional feature as "theft." I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law* [...]. Brano riportato a pagina 7 del lavoro di Morrison, Mazey e Wingreen, citato a nota 14. Peccato solo per quel riferimento alle leggi degli Stati Uniti. Si potrebbe discutere della sua correttezza tecnica in relazione ad uno Stato federale, certo, ma soprattutto: che contraddizione per un sacerdote del *Code is Law!*

[18] *Alcuni pongono in discussione l'analogia* Code is Law*; io no. Abbiamo appena scoperto di avere la nostra Corte Suprema, la comunità!*

[19] Consultato il 20/11/21: blog.slock.it/what-an-accomplishment-3e7ddea8b91d.

In ordine sparso. La decisione è stata adottata dagli altri utenti, cioè dalle vittime della sottrazione, e dunque dai controinteressati. Inoltre: si sarebbe mossa tutta la comunità se in luogo di 50 milioni di dollari, un colpo letale per l'intero sistema, fossero stati 10.000 euro sottratti al conto della zia Guglielmina? Infine: la decisione è stata assunta contraddicendo platealmente le regole sino al giorno prima dichiarate immutabili.

Provo adesso a mettere i concetti in fila: gli investimenti di zia Guglielmina, o di chiunque altro, sarebbero tutelati da un'assemblea (a) composta dai controinteressati, la quale (b) non è tenuta ad esaminare istanze o ricorsi, (c) può ignorare il contenuto degli accordi in vigore, e (d) non ha un corpus predeterminato di norme o principi cui attenersi.

A quest'ultimo proposito: se prestiamo fede a Wikipedia[20], che almeno in siffatte materie è però fonte autorevole, molti sostenitori della soluzione adottata ritenevano di poter agire in quanto l'operazione, pur non essendo illegale (ci mancherebbe: *Code is Law!*) era *unethical*. E con questa si farebbe davvero l'*en plein*: in materia di etica la possibilità di individuare un terreno comune tra un operatore di Wall Street, un dirigente del Partito Comunista Cinese, un Francescano e Greta Thunberg (per dire) mi pare a dir poco fantasiosa (Greta ed il Francescano, magari …). In concreto: totale arbitrarietà delle decisioni.

I sistemi Blockchain, criptovalute in testa, anziché farci evolvere verso nuove e più avanzate realtà, rischiano insomma di cancellare secoli di civiltà giuridica. Lawrence Lessing[21] ammoniva che eliminare lo Stato non ci conduce magicamente in Paradiso (*teleport us to Heaven*). A giudicare dal caso *TheDAO*, è più verosimile che si tratti di un'autostrada per l'inferno[22].

Autorevolissimi specialisti (prima fra tutti Primavera De Filippi[23]) ritengono che il rischio principale insito nei sistemi basati su blockchain sia quello di una tirannia del codice[24]. Personalmente sono più preoccupato, molto più preoc-

---

[20] Voce *The DAO (organization)*, consultata il 20/11/21.

[21] Citato a nota 16.

[22] Si veda (e soprattutto si ascolti) youtu.be/l482T0yNkeo.

[23] Non saprei raccomandare abbastanza il suo splendido *Blockchain and the Law*, Harvard University Press 2019, con Aaron Wright. Il volume della bocconiana De Filippi, che insegna ad Harvard e Parigi, è disponibile anche in francese (*Blockchain & Droit – Le Règne du code*, Dicoland 2019) ma, a quanto ad oggi mi risulta, non in italiano.

[24] *Decentralized blockchain-based application may well liberate us from the tyranny of centralized intermediaries and trusted authorities, but this liberation could come at the price of a much larger threat – that of falling under the yoke of the tyranny of code*. Sono le parole che concludono il libro citato alla nota precedente (p. 210).

cupato, della tirannia di un'indistinta comunità di utenti, guidati da una "élite" che evidentemente non ha molto di meglio da fare che passare le giornate al computer[25]. Ancor più dell'algocrazia[26], la dittatura dell'algoritmo, mi terrorizza l'oclocrazia, la dittatura della folla[27], o forse meglio la regressione verso forme tribali di diritto.

Questa è la riflessione che più tenevo a consegnare ad una così qualificata platea di giuristi, che ringrazio per l'attenzione.

[25] Nel programma di *TheDAO* (si veda a nota 12) ciascun utente avrebbe studiato e selezionato gli investimenti proposti. Chi ne ha il tempo? E se lo ha: possiede le necessarie competenze? Credo che normalmente una cosa escluda l'altra. Come si sarà intuito, non sono un fan della democrazia diretta a tutto campo. Secondo una celebre battuta, che faccio senza riserve mia, si chiama democrazia diretta perché c'è sempre qualcuno che la dirige.

[26] Espressione che mi risulterebbe esser stata coniata da A. Aneesh, *Global Labor: Algocratic Modes of Organization*, in *Sociological Theory* 27, no. 4 (2009), p. 347.

[27] D'altronde gli stessi P. De Filippi ed A. Wright (a pagina 36 dell'opera citata alla nota 23) riconoscono che l'evoluzione dei sistemi Blockchain è un *political process*. Ed un iter politico non governato da regole certe non è democratico, almeno nel senso contemporaneo del termine.

Lorenzo Lentini

Conferimenti di criptovalute e società di capitali*

Sommario: 1. Premesse definitorie e qualificatorie. – 2. Problematiche in tema di conferimento e prime esperienze applicative. – 3. Prospettive.

1. Premesse definitorie e qualificatorie

Nel campo dell'innovazione finanziaria il fenomeno delle criptovalute ha via via acquisito una rilevanza non trascurabile, al punto da irrompere nel lessico comune e suscitare l'attenzione delle istituzioni su scala internazionale.

La criptovaluta può essere classificata come una *species* del *genus* "*crypto-asset*", inteso come sequenza di «registrazioni digitali rappresentative di diritti (...) create, conservate e trasferite mediante tecnologie basate su registri distribuiti»[1] ("DLT"): un "prodotto", dunque, della tecnologia "*blockchain*".

In particolare, la criptovaluta è costituita da una rappresentazione digitale di valore caratterizzata, a livello tecnico, dall'impiego di meccanismi crittografici, mediante i quali i partecipanti a un sistema possono ottenere la circolazione di valore, con un sensibile livello di sicurezza e tracciabilità, senza il coinvolgimento di un'autorità centrale ovvero di istituti bancari[2].

Le criptovalute non vengono infatti emesse da autorità monetarie, ma sono il frutto (*rectius* il "corrispettivo") dell'attività di privati (c.d. *miners*) i quali, attraverso il dispendioso impiego di *software* avanzati e macchine con elevata potenza computazionale, risolvono complessi problemi matematici.

Una volta "estratte", le criptovalute sono conservate in appositi portafogli elettronici (c.d. *e-wallets*), gestiti da operatori specializzati e accessibili soltanto ai soggetti in possesso di un particolare sistema di chiavi. Esse, quindi, sono

* L'Autore ringrazia per la preziosa collaborazione alla stesura dell'intervento Sofia Frangipane, diplomata presso la SSPL dell'Università degli Studi di Brescia.

[1] CONSOB, *Le offerte iniziali e gli scambi di cripto-attività,* Documento per la discussione, 19 marzo 2019, p. 6.

[2] Cfr. A. Monti, *Per un'analisi critica della natura giuridica delle criptovalute* in *Riv. Ragion Pratica*, Il Mulino, 2018, p. 362.

trasferite elettronicamente, scambiate con moneta legale o con altre criptovalute ovvero utilizzate per l'acquisto tradizionale di beni.

La tecnologia che rende possibili tali operazioni, nota come *blockchain,* si fonda su una rete di computer-nodi, ciascuno dei quali partecipa alla formazione del registro, caratterizzato da appositi "blocchi", immodificabili e collegati tra loro in modo da formare una "catena": orbene, le regole della *blockchain* impongono che ogni nodo debba approvare i blocchi precedenti, al fine di garantire l'integrità e la tracciabilità dell'operazione.

Se il funzionamento tecnico delle criptovalute appare – almeno agli esperti del ramo – generalmente chiaro, ben più controverse risultano la funzione economico-sociale e la qualificazione giuridica.

Al riguardo una tendenziale convergenza di vedute si ha nell'esclusione della equiparazione tra criptovaluta e "denaro"[3]: a prescindere dall'adesione a teorie di matrice statalista ovvero economico-funzionale in ordine alla definizione della moneta, infatti, l'obiezione principale è data dalla considerazione secondo cui le criptovalute non hanno corso legale nel territorio nazionale[4] e che, pertanto, l'uso delle criptovalute come mezzo solutorio richiede l'accettazione del creditore[5].

Peraltro, anche a voler concedere che la funzione di strumento di scambio sia efficacemente conseguita, le altre funzioni tipicamente attribuite alla moneta "tradizionale" (unità di conto e riserva di valore) sono difficilmente individuabili nelle criptovalute, alla luce della marcata volatilità che storicamente ha caratterizzato dette entità, determinando fluttuazioni di valore nel tempo che, unite all'impossibilità genetica di attuare politiche monetarie di segno espansivo o restrittivo, appaiono inconciliabili con la funzione di riserva di valore (in disparte, sotto questo profilo, il carattere di "infecondità"[6] che connota le criptovalute virtuali, atteso che solo «i crediti liquidi ed esigibili di somme di denaro producono interessi di pieno diritto»[7]).

La diversità ontologica tra criptovaluta e moneta *fiat* e, più in generale, la netta cesura rispetto alle caratteristiche del sistema finanziario tradizionale (peraltro

---

[3] Cfr. Banca d'Italia, *Occasional Paper*, 18 marzo 2019, n. 484.

[4] La Risoluzione dell'Agenzia delle Entrate n. 72/E del 2016 afferma che «la circolazione dei Bitcoin, quali mezzi di pagamento, si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge».

[5] L'estinzione di un debito pecuniario con criptovaluta configura quindi una *datio in solutum* ex art. 1197 c.c., posto che ai sensi dell'art. 1277 c.c. "*i debiti pecuniari* si estinguono con *moneta avente corso legale* nello Stato al tempo del pagamento e per il suo *valore nominale*".

[6] Così definito da D. Fauceglia, *La moneta privata. Le situazioni giuridiche di appartenenza e i fenomeni contrattuali*, in *Contratto e impresa* 3/2020, p. 1266.

[7] Cfr. art. 1282 c.c.

rimarcata dagli stessi ideatori del *bitcoin,* primo esempio apparso nel 2009[8]) non esaurisce lo sforzo di qualificazione del fenomeno, persistendo la necessità di sussumere le criptovalute all'interno di categorie che siano note al giurista.

A livello normativo si segnala il d.lgs. 25 maggio 2017 n. 90 – che ha introdotto la lettera *qq)* nell'art. 1, co. 2, del d.lgs. 21 novembre 2007, n. 231 – poi modificato dal successivo d.lgs. 4 ottobre 2019, n. 125, recante attuazione della dir. UE 2018/843 del Parlamento Europeo del 30 maggio 2018[9], ai sensi del quale la criptovaluta è definita una «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente».

La richiamata definizione opera in negativo ("*non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale"),* valorizzando al contempo la coesistenza delle due funzioni essenziali della criptovaluta: scambio e investimento.

Nello stesso solco si pone la Proposta di Regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività[10], definite «rappresentazioni digitali di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga».

Per quanto riguarda la giurisprudenza, il Tribunale di Firenze[11] ha affermato che «*le criptovalute (...) possono essere considerate "beni" ai sensi dell'art. 810 c.c., in quanto oggetto di diritti, come riconosciuto oramai dallo stesso legislatore nazionale, che le considera anche, ma non solo, come mezzo di scambio (...)*», ritenendo che il rapporto tra l'intermediario gestore della piattaforma di scambio e deposito di criptovalute e i clienti-investitori potesse essere assimilato a un deposito irregolare.

A livello generale taluni commentatori hanno osservato, da un lato, che le criptovalute non possono essere considerate beni materiali, difettando il requisito della corporeità, stante la loro «intrinseca natura, talmente immateriale da

---

[8] "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"* è il messaggio codificato all'interno del *genesis block* di Bitcoin.

[9] Relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.

[10] Il c.d. "Regolamento MiCA" si propone di fornire una maggiore certezza del diritto, sostenendo l'innovazione e offrendo maggiori garanzie a tutela dei consumatori e degli investitori".

[11] Sentenza n. 18 del 21 gennaio 2019, declaratoria del fallimento di una società che gestiva la menzionata piattaforma di *exchange.*

rimanere addirittura diffusa all'interno di una rete di comunicazione elettronica»[12] e, dall'altro lato, che alla qualificazione come bene immateriale osterebbe il principio del numero chiuso e della tipicità dei diritti su beni immateriali.

Tale obiezione, certamente fondata in assenza di una previsione legislativa, potrebbe ritenersi superabile a seguito dell'imminente entrata in vigore del citato Regolamento UE in materia di mercati delle cripto-attività, stante l'introduzione nell'ordinamento, sia pure per mezzo di una normativa a carattere settoriale, di una nuova *asset class* costituente potenziale oggetto di investimento[13].

In particolare, si discuterebbe di beni immateriali costituiti dall'insieme di dati registrati sulla *blockchain*, fungibili (omogenei, privi di individualità e aventi le stesse proprietà, scaturenti dal medesimo registro informatico) e di quantità limitata (predefinita a monte dai rispettivi creatori[14]).

Infine, qualche anno prima, il Tribunale di Verona (24 gennaio 2017) aveva ritenuto la criptovaluta uno «*strumento finanziario*[15] *costituito da una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un software open source e ad una rete peer to peer*», sia pure ai diversi fini dell'applicazione della disciplina a tutela dell'investitore.

2. Problematiche in tema di conferimento e prime esperienze applicative

La soluzione alla questione se le criptovalute possano essere oggetto di conferimento risente del dibattito intorno alla funzione da assegnare in via preminente al capitale sociale.

---

[12] F. Di Vizio, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali: le discipline e i controlli*, in *Riv. dir. pen. cont.* 10/2018, p. 17.

[13] Già a legislazione vigente, peraltro, le criptovalute potrebbero rientrare nella nozione di "prodotti finanziari", laddove oggetto di un investimento avente natura "finanziaria", comportando l'impiego di capitale, cui è strettamente correlata l'assunzione di un rischio, a fronte di un'aspettativa di rendimento di natura finanziaria.

[14] Particolarmente interessante sotto questo profilo è la decisione della United States District Court, District of Massachusetts, Civil action n. 18-10077-RWZ COMMODITY FUTURES TRADING COMMISSION v. MY BIG COIN PAY, INC. et al. Memorandum of Decision, September 26, 2018, che ha qualificato la criptovaluta come *"commodity"*, ossia come bene fungibile, il cui prezzo viene determinato dal mercato sulla base dei meccanismi di domanda e offerta (l'ammontare massimo di valuta in circolazione è infatti generalmente fissato *a priori),* avente le medesime caratteristiche indipendentemente da chi lo produce.

[15] Sul punto va tuttavia osservato che il d.lgs. 58/98 adotta, in linea con la normativa sovranazionale, una elencazione puntuale delle *asset class* costituenti "strumenti finanziari" e che gli "strumenti di pagamento" risultano espressamente esclusi dalla definizione *ex* art. 2, co. 2 del testo unico. Pare preferibile fare riferimento alla categoria aperta dei "prodotti finanziari" di cui all'art. 1, comma 1, lett. u) del testo unico, comprendente «ogni altra forma di investimento di natura finanziaria».

Muovendo dalla disciplina della società per azioni, la tesi secondo cui il capitale sociale funga principalmente da garanzia per i creditori, siccome costituito da entità suscettibili di espropriazione forzata, è da tempo minoritaria in dottrina.

Più convincente appare l'orientamento secondo cui la garanzia per i creditori rappresentata dal capitale sociale operi in via indiretta, nella misura in cui l'ordinamento appresta un insieme di regole di composizione e disposizione del patrimonio, tendente a favorire la prospettiva di soddisfacimento delle pretese creditorie.

In particolare, avuto riguardo alla sua c.d *funzione vincolistica,* il capitale sociale si traduce in una frazione del patrimonio netto che i soci si sono impegnati a non distogliere dall'attività dell'impresa, che non possono ripartirsi durante la vita della società e che in tal senso costituisce una forma di garanzia patrimoniale per i creditori (questi ultimi possono infatti contare su un attivo patrimoniale che ecceda le passività)[16]. Tale tesi trova conforto nelle disposizioni della Direttiva 2012/30/UE (c.d. "Seconda Direttiva Societaria"), il cui considerando n. 5 afferma che *"sono necessarie norme dell'Unione per salvaguardare il capitale, che costituisce una garanzia per i creditori".*

Da una differente prospettiva la dottrina rimarca la funzione organizzativa del capitale sociale, in quanto idoneo a rappresentare la "misura" di diritti patrimoniali e amministrativi inerenti alla partecipazione.

Infine, maggioritaria oggi è la tesi che attribuisce al capitale sociale una funzione prevalentemente produttivistica, ossia la funzione di dotare la società dei mezzi necessari per il perseguimento del proprio oggetto.

In punto di entità conferibili, la citata Seconda Direttiva prevede all'art. 7 che il capitale sottoscritto possa essere costituito unicamente da elementi dell'attivo suscettibili di valutazione economica, con la precisazione che tali elementi non possono essere costituiti da impegni di esecuzione di lavori o di prestazione di servizi.

La disciplina domestica (artt. 2342 c.c. e ss.), oltre a recepire detto divieto di conferimento di prestazioni di opera o di servizi[17], da un lato stabilisce che il conferimento debba essere effettuato in denaro ("se nell'atto costitutivo non è

---

[16] F. Di Sabato, *Capitale e responsabilità interna nelle società di persone*, Milano, Giuffrè, 2005, p. 86 e ss.

[17] Cfr. G. Olivieri, *I conferimenti in natura nella s.p.a*, Padova, Cedam, 1989, p. 63 e ss.: secondo l'A. le prestazioni di *facere*, ancorché suscettibili di essere valutate economicamente, non sono compatibili con l'esigenza che il bene conferito sia idoneo allo scambio, requisito quest'ultimo indispensabile per assicurare la funzione di garanzia propria del capitale sociale. Le prestazioni di opere e servizi, inoltre, risentono di una incertezza ontologica, legata alla natura delle stesse, traducendosi nella somministrazione di lavoro personale, in quanto tale dipendente dalle vicende individuali del prestatore: tale incertezza minerebbe il principio di effettività del capitale.

stabilito diversamente") e, dall'altro lato, regolamenta puntualmente il procedimento di conferimento di beni in natura e di crediti.

Le cautele apprestate dalla normativa nazionale in ipotesi di conferimenti di beni diversi dal denaro mirano ad assicurare, in armonia con il diritto europeo, il rispetto di quello che probabilmente rappresenta il principio cardine in materia di conferimenti: l'effettività del capitale sociale, declinato come necessaria ricerca della tendenziale corrispondenza tra il capitale nominale, inteso nella sua accezione di limite alla distribuzione dell'attivo, e il capitale reale.

L'inquadramento giuridico della natura delle criptovalute si profila dunque propedeutico alla soluzione della questione in esame, posto che la disciplina dettata per i conferimenti societari è diversamente modulata a seconda che l'oggetto del conferimento sia il denaro, un bene in natura, un credito o una prestazione d'opera (quest'ultima vietata nelle s.p.a., ma consentita nelle s.r.l.).

Muovendo dal principio consolidato secondo cui, nell'ambito della disciplina sui conferimenti, per "denaro" debba intendersi la valuta in cui è denominato il capitale sociale, in quanto idonea ad esprimere il valore di altri beni in ragione del proprio valore nominale, e richiamata la considerazione secondo cui la criptovaluta non può, per le ragioni in precedenza illustrate, essere equiparata alla valuta avente corso legale, deve pervenirsi alla conclusione che il conferimento di criptovalute esuli dalla disciplina prevista per i conferimenti in denaro e debba, quindi, essere assoggettato alla disciplina dettata per i conferimenti in natura[18].

Del resto, anche a volere accantonare le suesposte obiezioni teoriche, la stessa disciplina dei conferimenti in denaro pare difficilmente compatibile con i tratti tipici delle criptovalute, se solo si considera come, in assenza di una perizia di stima, risulti assai disagevole tradurre l'ammontare del bene conferito in un valore certo, anche ai fini del versamento del 25% in sede di sottoscrizione[19].

Assunto come necessitato il ricorso al procedimento previsto per i conferimenti di beni in natura e di crediti, un primo ostacolo è rappresentato dall'art. 2342, c. 3, c.c. nella parte in cui prevede l'obbligo di immediata e integrale liberazione dei conferimenti aventi a oggetto beni in natura o crediti: la *ratio* della disposizione risiede nella volontà di sterilizzare il rischio di inadempimento del socio conferente (non diversamente dalle motivazioni alla base del divieto di conferire prestazioni d'opera).

Ancorché sia dubbia l'effettiva portata della norma, ovvero se contempli un requisito di selezione delle entità conferibili ovvero costituisca una mera indicazione

---

[18] Lo stesso art. 2343 *ter* c.c. conferma tale impostazione, assoggettando i conferimenti di valori mobiliari e di strumenti del mercato monetario alla disciplina dei conferimenti in natura.

[19] Non a caso, avuto riguardo alle medesime ragioni, i conferimenti di valuta estera sono generalmente trattati con le regole previste per i conferimenti in natura.

delle modalità di esecuzione del conferimento, l'obbligo di immediata liberazione induce a ritenere non ammissibili i conferimenti di cose future o altrui, di obbligazioni negative e di prestazioni aventi a oggetto diritti personali di godimento.

Ai presenti fini, ove si acceda alla tesi secondo cui la norma postuli l'istantanea *traditio* del bene conferito, affinché sia immediatamente messo a disposizione dell'attività produttiva, non sorgono particolari questioni in relazione al conferimento delle criptovalute, ben potendo le parti assicurare detto effetto mediante consegna agli amministratori delle chiavi di accesso, con conseguente trasferimento della disponibilità giuridica e materiale del bene in capo alla società.

Non desta particolare preoccupazione il tema delle fluttuazioni cui i valori delle criptovalute tendono a essere soggetti: l'art. 2343 c.c., c. 3 e 4, prevede un procedimento di revisione della stima, entro 180 giorni dal conferimento, da parte degli amministratori, in base al quale, ove il valore dei conferimenti sia diminuito di oltre un quinto, la società deve ridurre proporzionalmente il capitale sociale (alternativamente, il socio conferente può versare la differenza in denaro ovvero recedere dalla società).

Ulteriore problematica evocata dai primi commentatori è quella che attiene all'idoneità del bene conferito a essere assoggettato all'azione esecutiva dei creditori sociali, posto che l'esito favorevole del pignoramento di una criptovaluta presuppone in concreto la collaborazione del suo titolare, unico individuo in possesso delle *password* per accedere al *wallet* elettronico ove è custodito il bene, mentre il sequestro del supporto materiale nel quale è conservato il portafoglio non sarebbe di alcun beneficio per i creditori, risultando comunque preclusa di fatto qualsiasi forma di aggressione in assenza delle chiavi di accesso.

Il suddetto rilievo può essere tuttavia superato alla luce dei più recenti approdi della dottrina secondo cui, ai fini dell'idoneità al conferimento, risulta sufficiente l'attributo della «*alienabilità, vuoi forzosa che volontaria, vale a dire come possibilità che il bene conferito venga comunque convertito in denaro da destinarsi a sua volta a soddisfare i creditori: e ciò non solo in via diretta attraverso un processo esecutivo attivato da questi ultimi ma anche in via indiretta attraverso l'iniziativa della stessa società, abbia essa ad oggetto l'alienazione autonoma del singolo bene (non sempre possibile come nel caso dell'avviamento, della ditta, dei marchi) oppure l'alienazione dell'intero complesso aziendale in cui il medesimo è inserito*»[20].

---

[20] Cfr. G. Zanarone, *Della società a responsabilità limitata*, in *Il Codice civile. Commentario*, fondato da M. Schlesinger e diretto da O. Busnelli, Milano, Giuffré, 2010, p. 218. Lo stesso G. Olivieri, ne *I conferimenti in natura*, cit., a p. 202 e ss. sosteneva che la recuperabilità non presupponesse la necessaria espropriabilità del bene, ma solo che il suo valore potesse essere realizzato «anche in via mediata attraverso una procedura di liquidazione che coinvolga l'azienda sociale nel suo complesso».

In connessione con la problematica dell'espropriabilità è stato sollevato il tema dell'anonimato che caratterizza le operazioni in criptovalute, risultando identificabili i portafogli virtuali coinvolti in dette operazioni, ma non i soggetti effettivi titolari, in possesso delle chiavi di accesso: di conseguenza, non essendo nota l'identità del titolare del *wallet* e in assenza di un'apprensione materiale del bene conferito, diverrebbe difficile accertare che la società sia l'effettiva beneficiaria del conferimento.

Come osservato tuttavia in dottrina[21] anche la suddetta criticità, che invero investe più la dimensione pratico-operativa che quella dell'ammissibilità sul piano teorico-giuridico, può ritenersi superata a seguito del progresso della tecnica, emergendo la disponibilità di appositi *software* con riconoscimento biometrico in grado di identificare i singoli utenti, attraverso le credenziali e i dati forniti nella fase di prima registrazione, e di ricostruire le transazioni effettuate sulle piattaforme *exchange*: una volta individuati, i gestori e i titolari dei *wallet* potrebbero, ove necessario, collaborare con l'autorità giudiziaria, fornendo le chiavi di accesso ai vari portafogli, non diversamente da quanto già accade in caso di pignoramento presso terzi (a ulteriore dimostrazione della tesi secondo cui la necessità di una collaborazione da parte del soggetto esecutato non è sufficiente a elidere l'attributo di espropriabilità del bene).

Muovendo dalle suesposte considerazioni, una lettura sistematica delle disposizioni in tema di conferimenti nelle società per azioni, che tenga conto della evoluzione normativa e dei principi affermati dalle direttive europee, porta a ritenere che i requisiti dell'entità conferibile siano fondamentalmente due (come nella s.r.l.): deve infatti trattarsi di un elemento dell'attivo, suscettibile di valutazione economica.

Per «elemento dell'attivo» si intende l'astratta idoneità del bene a contribuire allo svolgimento dell'attività economica, risolvendosi in un'utilità patrimoniale, senza che si richieda una perfetta corrispondenza biunivoca tra entità conferita e iscrivibilità nell'attivo patrimoniale.

Il secondo requisito attiene alla possibilità di attribuire al bene un valore economico sorretto da certezza logica e, in tal senso, presuppone l'esistenza di un mercato di riferimento: il valore di scambio[22] dell'oggetto del conferimento deve essere misurabile, sulla base di metodi di stima attendibili, e quantificato con precisione in un determinato momento storico.

Nel caso delle criptovalute, non rinvenendosi particolari difficoltà a ritenere integrato il primo presupposto, atteso che si discute di beni potenzialmente og-

---

[21] Cfr. G. Gitti e A. Sardini, *I conferimenti di criptoattività*, cit., p. 1314.

[22] G. Ferri jr, *Investimento e conferimento*, Milano, 2001, p. 366 ss.

getto di investimento e idonei a manifestare un incremento di valore nel tempo, l'accertamento del secondo requisito si profila più complesso, esigendo una indagine caso per caso, sulla base della singola tipologia di criptovaluta in concreto conferita.

Come è noto infatti, successivamente alla fase di collocamento (*Initial Coin Offering*), le criptovalute vengono tendenzialmente scambiate su apposite piattaforme (*exchange*), che consentono l'incontro tra domanda e offerta. Tuttavia, trattandosi di piattaforme gestite da soggetti non vigilati e nella perdurante assenza di un quadro regolamentare esaustivo e uniforme, l'effettiva capacità di ciascuna piattaforma di consentire la formazione di un prezzo "di mercato" (presupposto di una valutazione economica attendibile da parte dei terzi) è seriamente in discussione, considerata anche l'assenza di un sufficiente numero di soggetti *data provider* affidabili.

Le osservazioni appena formulate sono in larga parte replicabili in relazione alla disciplina dei conferimenti nel capitale di s.r.l.., comunque ispirata al principio generale della salvaguardia dell'effettività del capitale sociale, sia pure con alcune distinzioni[23].

Come è noto, infatti, pur in assenza di vincoli comunitari, l'art. 2464, co. 2, c.c., mutua il regime attualmente previsto dall'art. 7, par. 1, primo periodo, della Seconda Direttiva, a mente del quale «*possono essere conferiti tutti gli elementi dell'attivo suscettibili di valutazione economica*».

L'elasticità della disposizione, la cui applicazione risente dell'evoluzione di discipline extragiuridiche, induce a ritenere ammissibile il conferimento nel capitale della s.r.l. di un'ampia gamma di utilità: diritti reali e personali di pagamento, obbligazioni di *facere*, obbligazioni negative, contratti di ogni tipo.

L'autonomia rispetto al regime applicabile alle s.p.a. emerge nitidamente in tema di conferimento di prestazioni d'opera o di servizi, espressamente vietato nella società per azioni e invece ammesso nella s.r.l., a condizione che sia assistito dal rilascio di una polizza di assicurazione o di una fideiussione bancaria[24].

---

[23] Distinzioni introdotte perlopiù nel segno della semplificazione, quali il procedimento di nomina "privata" del soggetto incaricato della stima *ex* art. 2465 c.c. e il mancato richiamo dell'art. 2343, c. 3, c.c. in tema di obbligo di controllo da parte degli amministratori entro i successivi 180 giorni.

[24] Spiega, infatti, G. Ferri Jr. ne *Il conferimento "documentario"*, in *Riv. not.*, 2002, p. 1379 che «attraverso tali strumenti, viene contestualmente creata una disponibilità, presso la banca o l'assicurazione, a favore della società della quale essa potrà autonomamente usufruire». Tale adempimento servirebbe, altresì, a sostituire l'obbligo – inderogabile per i conferimenti di beni in natura e di credito nelle S.r.l. ai sensi dell'art. 2464, co. 5 c.c. – di integrale immediata esecuzione dell'apporto, che difficilmente potrebbe conciliarsi con i conferimenti di *facere*, posto che questi necessitano di una continua collaborazione del prestatore, che fornisce il proprio lavoro personale.

Avuto riguardo alla *ratio* della suddetta garanzia, a copertura del valore assegnato al conferimento, l'applicazione della norma potrebbe essere utilmente estesa a tutti i casi in cui la natura del bene conferito non ne consenta l'immediata liberazione al momento della sottoscrizione.

Giunti a questo punto della trattazione, merita un cenno l'unico precedente noto in cui si è reso necessario lo scrutinio giudiziale di una operazione di conferimento di criptovaluta: è il "caso One Coin", esaminato in sede di volontaria giurisdizione dal Tribunale delle Imprese di Brescia, con il decreto 18 luglio 2018, n. 7556, e successivamente dalla Corte d'Appello, con il decreto 24 ottobre 2018, n. 207.

La vicenda trae origine dal ricorso promosso da una s.r.l. avverso il rifiuto del notaio di iscrivere nel Registro delle Imprese la delibera assembleare di aumento di capitale, da liberare (in parte) mediante conferimento di criptovaluta: detto rifiuto poggiava, in particolare, sulla constatazione del grado di volatilità delle criptovalute, tale da impedire «una valutazione concreta del *quantum* destinato alla liberazione dell'aumento di capitale sottoscritto, né di valutare l'effettività (*quomodo*) del conferimento»[25].

Il Tribunale di Brescia rigettava il ricorso, ritenendo che la criptovaluta in questione non fosse, allo stato degli atti, un bene suscettibile di valutazione economica attendibile[26].

La Corte d'Appello, pronunciandosi sul reclamo, confermava il provvedimento di primo grado, sia pure con una motivazione più articolata: la Corte, esaminando in generale il fenomeno in questione, equiparava le criptovalute, sotto il profilo funzionale, alla moneta *fiat*, ritenendo quindi applicabile la disciplina dei conferimenti in denaro. Tuttavia la Corte, osservato che «*non è [...] dato conoscere, allo stato, un sistema di cambio per la criptovaluta, che sia stabile ed agevolmente verificabile, come per le monete aventi corso legale in altri Stati (dollaro, yen, sterlina etc.)*» e che permetta di attribuire regolarmente a una determinata criptovaluta il relativo valore in euro, giungeva a escludere *a priori* l'idoneità

[25] Più nello specifico, tale aumento veniva sottoscritto mediante il conferimento di opere d'arte per un valore complessivo di 686.000,00 euro e di 35.109,56 unità della criptovaluta denominata "One Coin", di valore stimato pari a 714.000,00 euro, come da perizia redatta *ex* art. 2465 c.c.

[26] Il Collegio rilevava trattarsi di una criptovaluta ancora in fase embrionale, priva dei «*requisiti minimi per poter essere assimilata a un bene suscettibile in concreto di una valutazione economica attendibile*»: la perizia di stima, prodotta in sede di conferimento, non era fondata su informazioni oggettivamente attendibili, attribuendo un valore che non discendeva da dinamiche di mercato, bensì dall'acritico recepimento del valore massimo riportato su una piccola piattaforma internet di scambio gestita dai fondatori della medesima criptovaluta, con meccanismi viziati da una evidente forma di «autoreferenzialità».

delle criptovalute al conferimento nel capitale delle s.r.l., non essendo possibile «*determinare il* quantum *finalizzato alla liberazione dell'aumento del capitale sociale sottoscritto*».

3. Prospettive

L'indisponibilità di una sufficiente casistica giurisprudenziale (non sono noti precedenti ulteriori a quelli espressamente citati, peraltro riguardanti casi-limite) non consente l'individuazione di un indirizzo univoco sull'argomento.

La questione non è di carattere meramente definitorio, ma ha precise conseguenze di tipo operativo: dalla natura giuridica che si vuole assegnare alle criptovalute dipende, in definitiva, l'applicazione della disciplina dettata in materia di conferimento di denaro ovvero di beni in natura, a tacer delle conseguenze in ordine alla struttura e ai contenuti delle perizie di stima.

A livello generale emerge una stretta relazione tra il giudizio di ammissibilità del conferimento e la possibilità di stimare in concreto, con un adeguato livello di attendibilità logica, il valore delle criptovalute conferite: in tal senso è propedeutico accertare l'idoneità del mercato di riferimento alla correttezza del processo di formazione del prezzo, ovvio presupposto di qualsiasi valutazione affidabile.

Da altra prospettiva, la definizione del problema è strettamente connessa al principio di effettività del conferimento e alla funzione che si vuole attribuire, almeno in via preponderante, al capitale sociale.

Sullo sfondo si staglia l'antica questione del rapporto tra diritto societario e beni intangibili, destinata a entrare nel dibattito tra gli studiosi in modo sempre più prepotente con la progressiva espansione delle applicazioni derivanti da *blockchain* e intelligenza artificiale.

Guido Romano

Criptovalute e moneta elettronica. I tormenti di dottrina e giurisprudenza

Sommario: 1. Premessa. *Ducunt fata…* – 2. La moneta e le sue funzioni. – 3. Le criptovalute ed il loro funzionamento. – 4. Le criptovalute e le difficoltà di un loro inquadramento giuridico. – 5. Le criptovalute come denaro. – 6. Le criptovalute come strumenti finanziari. – 7. Le criptovalute come beni giuridici. – 8. Il fondamento «pattizio» dell'utilizzo delle criptovalute. – 9. Criptovalute: la nuova frontiera della segregazione patrimoniale? – 10. Criptovalute e fenomeno societario. – 11. Criptovalute e moneta elettronica. – 12. Conclusioni.

1. Premessa. *Ducunt fata*…

Ducunt fata volentem, nolentem trahunt.

Per parlare di criptovalute e, in generale, dell'affermazione delle nuove tecnologie e del loro rapporto con la vita reale di ciascuno di noi prima ancora che con l'ordinamento giuridico, si può ben partire da questa antica affermazione che, già attribuita al filosofo greco Cleante, compare nelle *Epistole a Lucillo* di Seneca[1] e, soprattutto, chiude il poderoso ed inquietante *Il tramonto dell'occidente* che Osvald Spengler pubblicò tra il 1918 ed il 1922[2].

Al termine del trattato di fisiognomica della storia, scrive il filosofo tedesco: «ma per noi, posti da un destino in questa civiltà e in questo punto del suo divenire in cui il danaro celebra i suoi ultimi trionfi e in cui il suo erede, il cesarismo, ormai avanza silenziosamente e irresistibilmente, è strettamente definita la direzione di quel che possiamo volere e che dobbiamo volere, a che valga la pena

[1] Epistole a Lucillo, 107, 11, 5: «11. Conducimi dove vuoi, Padre e Signore dell'alto cielo: non esiterò a ubbidirti; sono pronto. Se non volessi, dovrei seguirti piangendo e dovrei subire di malanimo ciò che potevo fare volentieri. Il fato guida chi è consenziente, trascina chi si oppone. 12. Sia questa la nostra vita, siano queste le nostre parole; il destino ci trovi pronti e attivi. È grande l'anima che si abbandona al destino: ma è meschina e vile se lotta contro di esso e disprezza l'ordine dell'universo e preferisce correggere gli dèi piuttosto che se stessa. Stammi bene».

[2] O. Spengler, Il tramonto dell'Occidente. Lineamenti di una morfologia della storia mondiale, ed. italiana, Longanesi, 2008, p. 1398.

di vivere. A noi non è data la libertà di realizzare una cosa anziché l'altra. Noi ci troviamo invece di fronte all'alternativa di fare il necessario o di non poter fare nulla. Un compito posto dalla necessità storica sarà in ogni caso realizzato: o col concorso dei singoli o ad onta di essi. *Ducunt fata volentem, nolentem trahunt*».

Del pensiero di Spengler si potrebbero capovolgere i termini della questione laddove la storia di questi ultimi decenni dimostra che il concetto di «statualità» (usiamo, per ovvie ragioni, questo termine in luogo dell'originario «cesarismo») lascia il passo oggi alla tecnologia ed al danaro e, anzi, verrebbe da dire visto il tema che stiamo per trattare, ad un nuovo concetto di danaro finanche completamente sganciato dalla autorità pubblica che, in passato, ne ha sempre garantito l'effettività e la conseguente fiducia.

Ma, invertito l'ordine dei fattori, resta all'interprete quella impressione di «subire» gli eventi e di non potere disporre della libertà necessaria per realizzare una cosa anziché un'altra: il trionfo della tecnologia sarà in ogni caso realizzato o con il nostro concorso o, comunque, ad onta della nostra volontà.

2. La moneta e le sue funzioni

L'ideazione delle criptovalute[3] – e, in particolare, del *bitcoin* che ne costituisce l'espressione più diffusa – risale al 2008 per opera di Satoshi Nakamoto

[3] In generale, per una prima valutazione, sotto il profilo giuridico, del fenomeno delle criptovalute e, in particolare, dei *bitcoin*, si vedano: G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, in *Not.,* 2020, 23; R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf.*, 2017, 1, 27; A. Caloni, *Bitcoin: profili civilistici e tutela dell'investitore*, in *Riv. dir. civ.*, 2019, 159 ss.; M. Cian, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca, borsa, tit. cred.,* 2019, I, 315; M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, in *Riv. dir. civ.*, 183; V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, in *Banca, borsa, tit. cred.*, 2018, I, 747 ss.; ID., *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi*, in M. Cian, C. Sandei, *Diritto del Fintech,* Milano, 2020, 215 ss.; G. Finocchiaro, *Le cripto-valute come elementi patrimoniali assoggettabili alle pretese esecutive dei creditori*, in *Riv. dir. proc.,* 2019, 87; D. Fauceglia, *La moneta privata. Le situazioni giuridiche di appartenenza e i fenomeni contrattuali,* in *Contr. impr.,* 2020, 1253; G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del* bitcoin*: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. inform.*, 2015, 415; P. Iemma, N. Cuppini, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *dirittobancario.it*; M. Krogh, *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, in Not., 2018, 2, 155; Id., *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, in *Not.*, 2018, 663; G. Lemme – S. Peluso, *Criptomoneta e distacco dalla moneta legale: il caso* bitcoin, in *Riv. dir. banc.*, 2016; F. Moliterni, *Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione,* in F. Maimeri, M. Mancini (a cura di),

(probabilmente uno pseudonimo sotto il quale si cela un gruppo di lavoro): da quella data, tuttavia, sono innumerevoli le monete virtuali create ed utilizzate in mercati più o meno estesi.

Proprio perché si tratta di un fenomeno assai recente, non vi è ancora concordia in ordine alla loro natura ed alle correlate funzioni: d'altra parte, le difficoltà di inquadrare giuridicamente il fenomeno delle criptovalute riflette la circostanza che non esiste, a livello normativo, una definizione di «moneta»[4], la quale risente di condizionamenti storici molto forti.

Tradizionalmente si afferma che la moneta assolve le funzioni di *mezzo di scambio*, di *riserva di valore* e di *unità di conto*. Al fine di assolvere alla prima delle funzioni cennate, è necessario che la dazione della moneta sia accettata in pagamento e, quindi, ai fini dell'acquisto di altri beni o servizi. La funzione di riserva di valore (o di liquidità) consiste, invece, nell'attitudine della moneta di assicurare la conservazione nel tempo del proprio potere di acquisto, potendo essere oggetto di risparmio per una successiva spendita[5]. Infine, la moneta assu-

---

Le nuove frontiere dei servizi bancari e di pagamento tra PSD 2, criptovalute e rivoluzione digitale, Quaderni di Ricerca Giuridica della Banca d'Italia, 2019; M. Passeretta, *Il primo intervento del legislatore italiano in materia di "valute di virtuali"*, in *Nuove leggi civ.*, 2018, 5, 1171; Id., *Bitcoin: il* leading case *italiano*, in *Banca, borsa, tit. cred.*, 2017, 471; R. Razzante, *Bitcoin: tra diritto e legislazione*, in Not., 2018, 383; G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contr. Impr.,* 2019, 257; M. Rubino De Ritis, Bitcoin: *Una moneta senza frontiere e senza padrone? Il recente intervento del legislatore italiano*, in *Giustiziacivile.com*; Id., *Obbligazioni pecuniarie in criptomoneta* (nota a Lodo Arb. Marcianise, 14 ottobre 201), in *Giustiziacivile.com*; M. Semeraro, *Moneta legale, moneta virtuale e rilevanza dei conflitti*, in *Riv. dir. banc.*, 2019, II, 239; N. Vardi, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei* bitcoin, in *Dir. inform.*, 2015, 443

[4] M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 191 il quale osserva che il codice civile omette di definire la moneta finanche allorquando disciplina le obbligazioni pecuniarie, vale a dire proprio quelle obbligazioni che «hanno ad oggetto una somma di danaro». Infatti, le obbligazioni pecuniarie sono riguardate da una prospettiva «funzionale», come è reso evidente dall'art. 1277 c.c. che enunzia non già una definizione della moneta, ma semplicemente «la regola in forza della quale i debiti pecuniari si estinguono con moneta avente corso legale nello Stato al valore nominale».

[5] In questo modo, la moneta diviene strumento di capitalizzazione di valori: così, M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 188. Come nota V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, cit., 754 «il concetto di riserva di valore non è un connotato esclusivo della moneta in senso proprio, perché ogni strumento finanziario, ogni merce, ogni bene economico costituisce una riserva di valore. Il problema del tracciamento dei trasferimenti di valori che riciclano il denaro sporco è proprio anche dei trasferimenti di valore che non sono costituiti da moneta, ed è accentuato nei casi in cui lo strumento di trasferimento è caratterizzato da anonimato».

me la funzione di unità di conto allorquando costituisce lo strumento di misurazione del valore dei beni, dei servizi e di altri attivi patrimoniali.

Le funzioni della moneta ora sommariamente esposte hanno dato vita alle diverse teorie ricostruttive[6] che hanno, di volta in volta, posto l'accento su una o sull'altra funzione.

Superata la dottrina metallistica del denaro che, esaltando la funzione di strumento di scambio e di misura di valore, concludeva ritenendo che il denaro (e, dunque, la moneta) deve avere valore intrinseco, all'inizio del novecento si è affermata la dottrina statalistica della moneta secondo la quale soltanto lo Stato può creare, sotto la propria autorità, la moneta attribuendole il potere liberatorio delle obbligazioni pecuniarie (corso legale) e l'impossibilità per il creditore di rifiutarla come mezzo di pagamento (corso forzoso). Il merito di questo orientamento è stato quello di sganciare il concetto di denaro dal valore intrinseco del bene che costituisce, in un determinato ambito, la moneta stessa. In questa prospettiva, il denaro è essenzialmente una creazione dello Stato e, dunque, un «segno» che può essere privo di un effettivo e reale valore intrinseco.

Successivamente, però, si è affermata, in particolare nella scuola liberale austriaca, una dottrina che pone l'accento sulla dimensione fattuale e funzionale della moneta: la moneta assolve le proprie funzioni non già perché possiede un valore intrinseco ovvero perché è emessa da una autorità statale, ma perché diviene, *di fatto*, accettata nell'ambito di una comunità in un determinato momento storico[7]. In altre parole: è moneta ciò che, in determinato contesto, assume la funzione di assicurare gli scambi e, per ciò solo, assume un valore economico. Essa, dunque, diviene un «istituto di ordine sociale»[8].

3. Le criptovalute ed il loro funzionamento

In via di prima approssimazione (e evidenziato che ciascuna valuta virtuale segue le regole dettate dai propri ideatori), le criptovalute sono valute virtuali ge-

---

[6] Per una puntuale ricostruzione delle diverse teorie, cfr., M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 188 ss.

[7] V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, cit., 747 ss., spec., 751.

[8] Per usare le parole di T. Ascarelli, *La moneta. Considerazioni di diritto privato*, Milano 1928, 63; Id., *Obbligazioni pecuniarie. Art. 1277-1284*, in *Comm. Scialoja-Branca*, rist., Bologna 1968, 12, nt. 1. In particolare, l'Ascarelli poneva in luce il rapporto "fattuale" fra moneta e comunità evidenziando come non sia possibile intendere la moneta slegata dalla comunità dei soggetti che la usano come tale: ossia dall'insieme di persone che la accettano come strumento di pagamento.

nerate attraverso protocolli informatici senza la necessità di ricorrere ad autorità centrali (quali banche o autorità governative) per il loro controllo ed emissione, e liberamente scambiabili tra gli utenti del relativo circuito virtuale senza l'ausilio di intermediari[9]. Le loro caratteristiche principali, dunque, vanno individuate nella «spontaneità» e nella «diffusività» che caratterizza il momento genetico, non esistendo una entità emittente e generandosi grazie alla operatività di *software* installati su una pluralità di terminali secondo le regole create dall'ideatore e codificate nel software medesimo[10]. La criptovaluta è utilizzabile attraverso lo scambio di un «valore» (così, almeno, percepito dalla «comunità» che lo accetta) attraverso una tecnologia *peer-to-peer*, la quale prevede una serie di nodi consistenti in computer di utenti disseminati in tutto il mondo. In questo sistema, il trasferimento dei valori avviene tra portafogli virtuali e ogni transazione viene inclusa nella c.d. *blockchain* (catena di blocchi)[11], utilizzando un sistema di crittografia asimmetrica che crea indirizzi di lunghezza arbitraria[12]. La criptovaluta rappresenta, dunque, un protocollo, un insieme di regole che servono a definire il funzionamento del software utilizzato dal *network* di computer, collegati fra loro con lo scopo di creare e gestire la

---

[9] Riprendendo le parole di M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 184, il bitcoin «è un protocollo di comunicazione telematica che serve a effettuare pagamenti. La "valuta" non ha dunque alcun tratto di materialità ma si sostanzia nel procedimento stesso di crittografia. In via di prima approssimazione si potrebbe dire l'oggetto della nostra indagine come una "rappresentazione" digitale di valore, atopica sia per fonte che per oggetto (la fonte creatrice del bitcoin e i bitcoin non sono in nessun luogo se non nella rete virtuale), non governata da banche centrali o altre istituzioni pubbliche, che può essere usata in alternativa alle valute tradizionali come mezzo di scambio o detenuta a scopo di investimento (…). Il *Bitcoin* è un protocollo di comunicazione basato su un sistema algoritmico di chiavi pubbliche e private. Alla base ci sono delle sequenze di blocchi matematici (*blockchain*) condivisi da un *network*. Il processo di creazione di blocchi attraverso la soluzione dell'operazione matematica, la c.d. attività di *mining*, ovvero una sorta di "estrazione dalla miniera", ha dei costi sempre più elevati. I *bitcoin*, inoltre, tendono all'esaurimento, in quanto il sistema algoritmico ne consente la creazione fino al numero finito di ventuno milioni, la maggior parte dei quali sono a oggi già stati estratti». Secondo G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., 31, «volendo tentare di individuare le caratteristiche delle criptovalute in senso stretto (intendendosi per tali quelle che si comportano e vengono percepite alla stregua di una moneta) queste possono essere definite come dei gettoni digitali (*digital tokens*) privati, senza diritti incorporati, convertibili, a prezzo variabile che operano attraverso un protocollo elettronico gestito in modo decentrato tramite una tecnologia denominata *permissionless distributed ledger technology* (DLT) detta anche *blockchain*».

[10] M. Cian, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, cit., 317.

[11] Sul funzionamento della blockchain, si veda, in particolare, G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., 23 ss.

[12] R. Razzante, *Bitcoin: tra diritto e legislazione*, cit., 383.

valuta digitale e che consentono pagamenti *online* tra due soggetti (che quel sistema evidentemente accettano) senza la necessità della intermediazione di un ente finanziario. Il *network peer to peer* – mediante l'utilizzo delle firme digitali – «marca» temporalmente ogni transazione e le posiziona in una catena continua di prove di lavoro (*proof-of-work*) che salvaguarda dalla contraffazione digitale formando un registro, di fatto, immodificabile, quale è la *blockchain*[13].

La *blockchain* altro non è, quindi, che un registro pubblico di tutte le transazioni in criptovalute, contenute in blocchi ordinati cronologicamente e collegati tra loro. Il blocco è un file in cui sono contenute una serie di informazioni, tra cui: numero del blocco, codice *hash*, data e ora di creazione, transazioni confermate nel blocco, unità di moneta virtuale movimentate e dimensioni del blocco. Tutti i dati relativi ai blocchi (e alla *blockchain*) sono memorizzati e distribuiti su computer degli utenti che partecipano ad un determinato *network* (ad es., *bitcoin*), organizzato in modo decentralizzato e paritario, così che ogni nodo è in grado di comunicare direttamente con gli altri senza dover passare da un *server* centrale.

L'acquisto e la vendita di criptovalute avvengono attraverso una piattaforma di *exchange* che permette di scambiare criptovalute con moneta tradizionale avente corso legale in uno stato o con altri tipi di valute virtuali, secondo un determinato prezzo di mercato.

La moneta virtuale circola attraverso il sistema della doppia chiave, una chiave privata, segreta e conosciuta dal solo titolare della chiave stessa, e da una chiave pubblica associata alla chiave privata; le transazioni finanziarie risultano trasparenti e tracciabili esclusivamente tra le chiavi pubbliche. Le chiavi private, associate alle chiavi pubbliche, sono create in modo del tutto anonimo ed automaticamente dal sistema che le gestisce; su ogni chiave privata possono essere caricati i *bitcoin* acquistati all'interno del sistema o donati[14].

I *bitcoin* sono gestiti dall'utilizzatore attraverso un portafoglio digitale (*e-wallet*), installato su di un *personal computer* o su di un dispositivo mobile dal quale è possibile eseguire il pagamento della merce o del servizio acquistato: la *blockchain* registra le credenziali digitali del portafoglio elettronico dal quale è disposto l'ordine di pagamento e i dati del portafoglio digitale del beneficiario[15]. Inoltre, almeno per il caso dei *bitcoin* e delle altre monete virtuali maggiormente diffuse (ma non per

---

[13] V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, cit., 756; M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., 669.

[14] Così, esattamente, M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., 672.

[15] M. Rubino De Ritis, Bitcoin*: una moneta senza frontiere e senza padrone?*, cit., 4.

tutte le criptovalute) esiste una piattaforma multimediale di scambio dove la domanda di chi è disposto ad acquistare *bitcoin* e l'offerta di chi è disposto a venderne s'incontrano; parallelamente, è possibile trasformare il valore digitale posseduto in moneta avente corso legale attraverso il successivo accredito in conto corrente delle somme di danaro convertite oppure attraverso trattative private tra gli utenti[16].

Il singolo scambio avviene attraverso il passaggio di una sequenza alfanumerica da un utente a un altro. L'operazione è registrata sulla rete *blockchain* e, dunque, è di dominio di tutti gli utenti. La *blockchain* ha inoltre la funzione di verificare la correttezza dell'algoritmo utilizzato nell'operazione, così da controllare che lo scambio avvenga regolarmente[17].

In definitiva, le criptovalute costituiscono delle monete virtuali che, fondandosi sulla crittografia, si propongono come strumento di pagamento alternativo alla moneta tradizionale e che non sono emesse – e, anzi, risultano indipendenti – da una autorità centrale: è l'utente, che accede al sistema con una chiave privata e si interfaccia con altri utenti con la chiave pubblica, a confermare direttamente i trasferimenti in valuta virtuale»[18]. In altre parole, le criptovalute possono definirsi come «valute aperte a struttura decentrata, che cioè si fondano su meccanismi di emissione distribuiti all'interno della rete e delle quali è prevista la convertibilità da e verso forme di ricchezza tradizionali e in particolare da e verso valute aventi corso legale»[19].

Infine, la valuta virtuale può dirsi «atopica»[20], in quanto «il suo utilizzo tecnico mediante un e-wallet non richiede la preidentificazione e la localizzazione né del disponente né del beneficiario di un pagamento in valuta virtuale»[21].

4. Le criptovalute e le difficoltà di un loro inquadramento giuridico

Pur in assenza di una compiuta normativa emanata dai legislatori nazionali, diverse autorità, nazionali ed estere, sono intervenute se non per disciplinare compiutamente il fenomeno, quanto meno per svolgere una sorta di lavoro di catalogazione.

Va, in primo luogo, ricordato come il legislatore europeo sia intervenuto con la direttiva 2018/843/UE del 30 maggio 2018 che definisce le valute virtuali «una

---

[16] M. Rubino De Ritis, Bitcoin: *una moneta senza frontiere e senza padrone*?, cit., ivi.

[17] M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 185.

[18] A. Caloni, *Bitcoin: profili civilistici e tutela dell'investitore*, cit., 159.

[19] Così, M. Cian, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, cit., 315.

[20] M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 208, nt. 105.

[21] V. De Stasio, *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi*, cit., 218.

rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente».

Secondo la Banca d'Italia[22] (ma l'elencazione è stata poi ripresa dalla dottrina che si è occupata del problema[23]), le criptovalute presentano le seguenti caratteristiche: 1) sono create da un emittente privato (nel caso delle cc.dd. valute centralizzate) o, in via diffusa, da utenti che utilizzano software altamente sofisticati (nel caso delle cc.dd. valute decentralizzate); 2) non sono fisicamente detenute dall'utente, ma sono movimentate attraverso un conto personalizzato noto come "portafoglio elettronico" (cd. *e-wallet*), che si può salvare sul proprio computer o su uno *smartphone*, o che può essere consultato via *internet*, al quale si accede grazie ad una *password*. Questi portafogli elettronici sono generalmente *software*, sviluppati e forniti da appositi soggetti (c.d. *wallet providers*). Esistono poi delle piattaforme di scambio, che offrono il servizio di conversione delle valute virtuali convertibili in moneta legale; 3) possono essere acquistate con moneta tradizionale su una piattaforma di scambio ovvero ricevute *online* direttamente da qualcuno che le possiede, per poi essere detenute su un "portafoglio elettronico"; utilizzando questo portafoglio i titolari possono effettuare acquisti presso esercizi commerciali o persone fisiche che accettano le valute virtuali, effettuare rimesse in favore di altri soggetti titolari di portafogli di valute virtuali, nonché riconvertirle in moneta legale; 4) i titolari dei portafogli elettronici e i soggetti coinvolti nelle transazioni rimangono anonimi[24]; 5) le transazioni tramite le quali

---

[22] Cfr., Banca d'Italia, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015.

[23] P. Iemma, N. Cuppini, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, cit., par 2; R. Bocchini, Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, cit., 27.

[24] Le operazioni in criptovalute sono forse tracciabili in senso informatico, ma sono sostanzialmente anonime dal punto di vista della corrispondenza con il soggetto fisico del titolare effettivo. Così, G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., 31.
Secondo G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 265, le transazioni bitcoin non sono anonime, bensì pseudonime. Tutte le operazioni effettuate all'interno del sistema sono registrate e archiviate nella blockchain (ciascuna con una propria marcatura temporale), e restano liberamente consultabili, per un periodo di tempo illimitato, da qualunque soggetto, anche se questi non partecipa alla rete. L'identità degli utilizzatori, tuttavia, è parzialmente protetta dall'utilizzo della pseudonimia: infatti la blockchain non include informazioni che consentono di risalire (direttamente) alla persona che ha effettuato il trasferimento, ma soltanto alla sua chiave pubblica.

vengono trasferite sono tecnicamente irreversibili (una volta fatta la transazione non è possibile chiederne l'annullamento).

In definitiva, secondo quanto evidenziato dalla Banca d'Italia, le c.d. valute virtuali sono rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente[25].

Per parte sua, la Banca Centrale Europea (*Virtual currency schemes – A further analysis*, febbraio, 2015) ha individuato tre tipi di criptovalute e, precisamente: 1) moneta virtuale chiusa, non convertibile in moneta legale, spendibile solo all'interno di un circuito virtuale; 2) moneta virtuale unidirezionale, non convertibile in moneta reale, spendibile per il pagamento di beni e servizi online e, in alcuni casi, beni e servizi reali; 3) moneta virtuale bidirezionale che può essere acquistata e riconvertita in moneta legale senza alcun vincolo.

La medesima Banca centrale Europea[26] si è, invece, distaccata dalla definizione di criptovalute contenuta nella direttiva del 2016 e dalla definizione offerta dalla Corte di Giustizia dell'Unione europea evidenziando che «la definizione di "valute virtuali" come mezzi di pagamento di cui alla proposta di direttiva non tiene conto del fatto che in talune circostanze le valute virtuali possono essere utilizzate a fini diversi dal pagamento (…). Gli utilizzi delle valute virtuali possono comprendere prodotti di riserva di valore a fini di risparmio e investimento, come prodotti relativi a strumenti derivati, materie prime e titoli», circostanza che si rivela ancor più evidente con riferimento alle *virtual currency* di nuova generazione, basate su implementazioni più evolute del paradigma blockchain.

La Banca centrale Europea ritiene, pertanto, che sarebbe più corretto qualificare le valute virtuali «mezzi di scambio» anziché «mezzi di pagamento»[27].

---

[25] Può essere utile richiamare anche la Risoluzione n. 72/E del 2016 della Agenzia delle Entrate secondo la quale «il *bitcoin* è una tipologia di "moneta virtuale" o meglio "criptovaluta", utilizzata come moneta alternativa a quella tradizionale avente corso legale emessa da un'autorità monetaria. La circolazione dei *bitcoin*, quali mezzi di pagamento, si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge. Si tratta, pertanto, di un sistema decentralizzato, che utilizza una rete di soggetti paritari (*peer to peer*) non soggetto ad alcuna disciplina regolamentare specifica né ad una autorità centrale che ne governa la stabilità nella circolazione».

[26] Banca Centrale Europea, Parere della Banca Centrale Europea del 12 ottobre 2016 su una proposta di direttiva del Parlamento europeo e del Consiglio che modifica la Direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la Direttiva 2009/10/CE.

[27] Sul punto, G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 277.

Tale definizione si rinviene, altresì, anche nelle classificazioni operate da autorità straniere. Ad es., secondo la *Securities and Exchange Commission* (SEC), «una valuta virtuale è una rappresentazione digitale di valore che può essere scambiata digitalmente e funziona come mezzo di scambio, unità di conto o riserva di valore. *Token* o monete virtuali possono rappresentare anche altri diritti. Di conseguenza, in determinati casi, i *token* o le monete saranno strumenti finanziari e non potranno essere venduti legalmente senza registrazione presso la SEC o in base ad un'esenzione».

La definizione offerta dalla Banca d'Italia è stata, in qualche modo, recepita dal legislatore. Infatti, quest'ultimo è intervenuto, nell'ambito della disciplina antiriciclaggio, con il d.lgs. 25 maggio 2017, n. 90 che ha modificato il d.lgs., 21 novembre 2007, n. 231. L'art. 1, co. 2, lett. qq) definisce la valuta virtuale come la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente[28]. Per converso, sono (art. 1, co. 2, ff) prestatori di servizi relativi all'utilizzo di valuta virtuale le persone, fisiche o giuridiche, che forniscono a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale.

Come si vede, sia diverse autorità nazionali ed internazionali sia il legislatore, pur tentando di «descrivere» i fenomeni connessi alle criptovalute, hanno evitato di prendere posizione in ordine alla natura giuridica di esse, con la conseguenza che ancora oggi, pure a fronte di una crescita esponenziale del fenomeno, tanto riguardo al numero di valute virtuali esistenti quanto al volume d'affari conseguente al loro utilizzo, permangono intatte le incertezze relative al loro inquadramento giuridico.

Non è possibile, in questa sede, dare conto in modo approfondito di tutte le soluzioni proposte dalla dottrina e dalla giurisprudenza che, nel volgere di pochi anni, si è occupata del tema, soluzioni che spaziano dalla qualificazione delle criptovalute come moneta vera e propria, come bene giuridico ai sensi dell'art. 810 c.c., come strumento finanziario e, infine, come mezzo di pagamento.

---

[28] È stato correttamente osservato che si tratta di una definizione «in negativo», evidenziando il legislatore più le caratteristiche assenti (il non essere emesse da una banca centrale, il mancato collegamento con una valuta avente corso legale, etc.) che quelle effettivamente riscontrabili. Così, G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., 31.

La diversità dei percorsi argomentativi sottesi alle soluzioni prospettate manifesta plasticamente le difficoltà – ad oggi irrisolte e, probabilmente, irrisolvibili sulla base dei principi generali ed in assenza di un intervento del legislatore – concernenti l'inquadramento giuridico delle criptovalute. A ben vedere, ciascuno di questi inquadramenti coglie un aspetto delle criptovalute soprattutto sotto il profilo funzionale, ma, se riguardato sotto il profilo sistematico, non si presenta del tutto appagante a spiegare, in modo completo, il fenomeno.

5. Le criptovalute come denaro

Secondo alcuni, le criptovalute, almeno nelle forme (e nei casi) maggiormente evolute, rappresenterebbero un valore trasferibile per via telematica e convertibile in moneta legale, priva di un supporto metallico o cartaceo, comunque in grado di trasferire un potere d'acquisto sotto forma di disponibilità finanziaria: e ciò sarebbe sufficiente a considerarle una nuova forma di emissione di moneta[29] [30].

---

[29] In questo senso, M. Rubino De Ritis, *Obbligazioni monetarie in criptomoneta*, cit, il quale – muovendo dalla definizione di "valuta virtuale" contenuta nel d.lgs. 25 maggio 2017, n. 90 che ha modificato il d.lgs. 21 novembre 2007, n. 231, il cui art. 1, alla comma 2, lett. qq, oggi ci dà la definizione di "valuta virtuale": «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi, trasferita, archiviata e negoziata elettronicamente» – ritiene «di includere la moneta virtuale (termine più appropriato rispetto a quello di valuta virtuale, proprio perché non rappresenta in forma digitale alcuna "valuta avente corso legale" come l'euro o il dollaro) nell'ambito dell'insieme costituito dalle "monete digitali" (in cui includere la moneta elettronica): la moneta virtuale non è riconducibile direttamente ad una disponibilità finanziaria in moneta avente corso legale ed è accettata solo su base consensuale (viene correttamente denominata anche "moneta digitale complementare")».
Secondo detto autore, «in conclusione, la moneta virtuale (chiamata dal legislatore italiano "valuta virtuale") rappresenta un valore trasferibile per via telematica e convertibile in moneta legale. Si tratta, allora, di una nuova forma di emissione di moneta, priva di un supporto metallico o cartaceo, comunque in grado di trasferire un potere d'acquisto (*recte*: disponibilità finanziaria). Ne consegue l'applicazione della disciplina in tema di obbligazioni pecuniarie (…), tra cui, ad esempio, l'applicazione di interessi, ma in via diretta e non analogica, anche in considerazione della locuzione utilizzata dall'art. 1278 c.c.: moneta non avente corso legale».

[30] Non osterebbe alla qualificazione in termini moneta delle criptovalute la loro estrema volatilità. G. Arcella – M. Manente, *Le criptovalute e le loro contraddizioni: tra rischi di opacità e di eccessiva trasparenza*, cit., 35 osservano che «attualmente molte monete, seppure emesse da Stati e quindi aventi corso legale forzoso, sono ugualmente poco capitalizzate e soggette ad altissime oscillazioni di valore. In realtà, finita la convertibilità in oro, le monete fiat vengono non a caso definite anche come fiduciarie, ovvero fondate sulla fiducia nella stabilità di un certo ordinamento economico-valutario espressione a sua volta di uno Stato, d'altronde la valuta, secondo la scienza economica,

Una simile ricostruzione sarebbe resa possibile dalla circostanza che il codice civile riguarda le obbligazioni pecuniarie da una angolazione funzionale, ponendo l'accento sul modo di estinzione di esse e non già sulla loro natura o consistenza, tanto è vero che l'art. 1277 c.c. prevede che i debiti pecuniari si estinguano con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale. Ciò posto, nel concetto di «moneta non avente corso legale nello Stato», preso in considerazione dall'art. 1278 c.c., potrebbero rientrare, a differenza di quanto opinato dalla dottrina tradizionale, non solo le monete estere propriamente dette, ossia quelle che hanno corso legale in uno Stato straniero, ma anche le monete che non sono di alcun altro Stato e trovano nella scelta delle parti il loro motivo fondante[31].

Secondo una simile ricostruzione, dunque, le criptovalute potrebbero essere annoverate tra le monete non aventi corso legale nello Stato, ma da qui discenderebbe, di necessità, la qualificazione di esse in termini di vera e propria moneta e, in particolare, l'applicazione, diretta e non analogica, dell'art. 1278 c.c. ai debiti di somme di monete private[32].

In definitiva, in assenza ostacoli normativi, l'orientamento in esame giunge ad evidenziare che la criptomoneta sembra oggi funzionare come strumento di scambio, che spontaneamente – ossia senza la garanzia di una istituzione – viene utilizzato nei traffici; ne deriva che nel momento in cui la criptomoneta viene scambiata si pone anche quale misura di valore. Quanto alla capacità di capitalizzare valori – che va giudicata sulla base della capacità potenziale dello strumento (e non sulla capacità rilevatasi *ex post*) – è proprio il fatto che la criptovaluta sia scambiata tra un'indefinita platea di soggetti e in un significativo numero di operazioni a conferire alla criptovaluta la capacità ora indicata[33].

---

altro non è se non la moneta circolante in un determinato ordinamento monetario». Secondo tali autori, dal fondamento pattizio dell'utilizzo delle monete virtuali, consegue che «in fin dei conti, la principale differenza tra una moneta tradizionale e le monete virtuali è nella *governance*: ovvero le monete con corso legale sono sotto il controllo degli Stati tramite le Banche centrali, mentre le monete complementari – nella più ampia accezione del termine – tra cui le criptovalute, non sono soggette al controllo statuale ma, essendo fondate su un meccanismo puramente fiduciario, vengono accettate su base squisitamente volontaria».

[31] Così, M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 194 che ricostruisce, altresì, gli esiti dei lavori preparatori al codice civile delle norme in tema di obbligazioni pecuniarie; N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*, cit., 576. Tutti gli autori citati propongono una lettura evolutiva della norma ed evidenziano che la dottrina maggioritaria è concorde nel ritenere che l'art. 1278 c.c. si riferisca, discorrendo di monete non aventi corso legale nello Stato, alle sole monete estere.

[32] N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*, cit., ivi.

[33] M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 199 e, spec., 201.

In senso contrario[34], si è segnalato che, ad oggi, la moneta virtuale non potrebbe essere inquadrata a tutti gli effetti come «moneta» sia a volere accedere alla concezione statalistica della moneta sia ad aderire alla concezione funzionale. Le monete virtuali non possono essere qualificate come moneta perché – almeno allo stato attuale – non sono emesse da un ente controllato dallo Stato e, dunque, non possiedono la forza liberatoria delle obbligazioni con la conseguenza che il creditore potrà sempre rifiutare di ricevere un pagamento in siffatta moneta, a meno di non aver precedentemente stabilito con il debitore di attribuire efficacia liberatoria anche a questo mezzo di pagamento[35]. D'altra parte, la funzione monetaria delle criptovalute sarebbe assicurata non già dalla fiducia riposta dalla comunità nel soggetto emittente, ma dalla fiducia nelle modalità tecniche di una emissione[36].

Ma le monete virtuali non possono essere qualificate come «moneta» neppure ad accedere alla teoria economica perché esse non riuscirebbero ad assolvere i

---

[34] In senso nettamente contrario alla qualificazione in termini di moneta delle criptovalute, si è espresso M. Krogh, *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, cit., 155 il quale rileva che «il *bitcoin*, come unità di misura, non ha valore intrinseco, né diretto né indiretto, il suo valore non è legato alla ricchezza economica di una comunità, ma è dato dal volume di scambi con altre valute ed è condizionato dalla domanda e dall'offerta all'interno di un mercato virtuale. Il suo valore non è condizionato da nessun tipo di politica monetaria, non esistendo un ente sovraordinato o una banca centrale a cui sono attribuiti poteri di indirizzo o di intervento sull'emissione e circolazione della moneta; ciò costituisce, da un lato, una caratteristica essenziale ed un punto di forza del *bitcoin*, che nella sua genesi ha avuto come obiettivo principale la decentralizzazione della politica monetaria attraverso l'eliminazione di banche centrali ed intermediari e, da altro lato, rappresenta anche il suo maggior punto di debolezza essendo il valore del *bitcoin* rimesso alla volubilità del mercato senza possibilità di correzione e protezione del valore della valuta virtuale attraverso manovre di politica monetaria da parte di una banca centrale. Ciò determina un'elevatissima volatilità del valore (*rectius*: tasso) della moneta virtuale condizionato esclusivamente dal volume degli scambi, dalla domanda e dall'offerta e dalla fiducia nel sistema o più precisamente nelle piattaforme informatiche che gestiscono gli scambi. Il rischio concreto è che ad una regolamentazione legale da parte di una banca centrale o di altro intermediario finanziario si sostituisca una regolamentazione di fatto da parte di soggetti in grado di alterare le dinamiche della domanda e dell'offerta». Sul punto, anche G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del* bitcoin*: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, cit., 415.

[35] R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, cit., 29.

[36] In questa prospettiva, M. Cian, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, cit., 318 il quale osserva che «la criptovaluta, dal punto di vista della sua consistenza fenomenica e della sua vocazione, è quanto di più lontano dal denaro-merce si possa immaginare: documento digitale espressivo di un dato numerico che ha valore solo finché la comunità glielo riconosce, proprio come valore monetario. Ma se si guarda alla diffusività e alla spontaneità (da intendersi come irriferibilità ad una volontà a ciò diretta) della creazione, il fenomeno nella sua forma più moderna si manifesta senza dubbio con una sorta di ritorno all'antico».

ruoli che questa impostazione vorrebbe attribuire alla moneta. Infatti, la funzione di riserva di valore sarebbe impedita dall'estrema volatilità del suo corso, quella di mezzo di scambio dipenderebbe pur sempre da un accordo delle parti e non sarebbe imposta dallo Stato; quella di unità di conto sarebbe pregiudicata dalle stesse incertezze del mercato dei cambi[37]. In altre parole, la circostanza che l'utilizzo solamente su basi convenzionali (come si vedrà nel prosieguo) e, allo stato attuale, il limitato livello di accettazione tra il pubblico, unitamente alla elevatissima volatilità del valore, rendono difficile un inquadramento delle criptovalute come moneta[38]. D'altra parte, la criptovaluta non adempie alla funzione di «unità di conto», in quanto in nessun paese i bilanci delle imprese vengono redatti in unità di conto diverse da quelle dello Stato; parimenti, nessuno Stato accetta pagamenti di tributi in moneta virtuale non emessa da una banca centrale[39].

Peraltro, se si esclude che la criptovaluta sia riconducibile alla categoria del denaro, deve necessariamente concludersi per l'inapplicabilità della disciplina codicistica prevista per le obbligazioni in denaro[40].

L'aspetto da ultimo considerato è stato oggetto di un lodo arbitrale[41] ove l'arbitro, evidenziata la mancanza di norme che disciplinino le obbligazioni pecuniarie

---

[37] Ancora, R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, cit., 29.

[38] P. Iemma, N. Cuppini, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, cit., 28; G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 282 secondo il quale, tuttavia, ciò non vale ad escludere (aprioristicamente) la possibilità che le criptomonete siano in grado di assumere in futuro, all'esito di un processo di maturazione e nell'ambito di un contesto caratterizzato da una maggiore stabilità, attributi compatibili con il concetto di denaro in senso economico. Più possibilista, R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, cit., 28 secondo il quale, almeno con riferimento ai *bitcoin*, sarebbero perseguibili le funzioni di mezzo di scambio e di unità di misura.

[39] V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, cit., 757. Sul punto, anche M. Cian, *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, cit., 321 secondo il quale la funzione della moneta quale unità di misura del valore dei beni e dei servizi non sembra invece tendenzialmente propria delle criptovalute, in quanto anche chi accetta monete digitali a pagamento dei propri beni o servizi stabilisce il prezzo in moneta legale. In tal modo, è sempre quest'ultima a rappresentare l'unità-base di conto, mentre la determinazione del corrispettivo in valuta alternativa segue il corso di cambio, potendo così oscillare indipendentemente dall'eventuale oscillazione del valore del bene.

[40] In questo senso, G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 293.

[41] Arbitro Unico Marcianise, 14 aprile 2018, in *GiustiziaCivile.com*, con nota di M. Rubino De Ritis, *Obbligazioni pecuniarie e criptomoneta*. Il caso sottoposto all'arbitro riguardava l'azione di adempimento svolta dal professionista nei confronti del proprio cliente volta al pagamento del corrispettivo, la cui metà era stata pattuita in criptomoneta. Tuttavia, il creditore-attore aveva agito per conseguire il pagamento dell'intero corrispettivo in moneta avente corso legale.

pattuite in criptovalute, ha ritenuto di fare ricorso agli ordinari criteri di interpretazione delle leggi e, precisamente, all'art. 12, comma 2, disp. prel. c.c. a mente del quale, se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe. In questa prospettiva, al fenomeno delle obbligazioni pecuniarie pattuite in criptovalute, in mancanza di esplicita disciplina legislativa espressa, deve applicarsi, analogicamente, l'art. 1278 c.c. che regola l'adempimento delle obbligazioni pecuniarie pattuite in moneta estera (se la somma dovuta è determinata in una moneta non avente corso legale nello Stato, il debitore ha facoltà di pagare in moneta legale, al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento), in quanto entrambe le fattispecie attengono alle ipotesi di adempimento di obbligazione pecuniaria da soddisfarsi con consegna di moneta non avente corso legale nello Stato italiano. Ciò posto, la norma attribuisce, in caso di obbligazioni pecuniarie in moneta estera, al debitore la facoltà di adempiere l'obbligazione in moneta nazionale. In ragione della lettera della norma, l'obbligazione avente ad oggetto la prestazione di corrispondere moneta estera è qualificabile come obbligazione facoltativa passiva che postula un'obbligazione semplice, concernente una prestazione principale, unica e determinata dall'origine, nonché, accanto a questa, una prestazione facoltativa (della cui effettiva ed attuale esigibilità il creditore optante abbia piena consapevolezza) dovuta solamente in via subordinata e secondaria, qualora sia preferita dal creditore (obbligazione facoltativa attiva) o dal debitore (obbligazione facoltativa passiva). Nel caso di obbligazione pecuniaria di valuta straniera, il legislatore prevede, in omaggio al principio del *favor debitoris*, un'ipotesi di obbligazione facoltativa passiva. Sicché, il debitore è tenuto ad adempiere la prestazione pattuita in moneta straniera con valuta estera, ma ha facoltà di scelta di corrispondere la somma dovuta con moneta nazionale avente corso legale. Tale facoltà non è prescritta anche a favore del creditore, il quale può, anche a fronte dell'inadempimento del debitore, chiedere soltanto l'adempimento della prestazione principale: cioè il pagamento con valuta estera.

Sulla scorta di tali considerazioni, l'arbitro ha concluso affermando che il creditore di una prestazione di somma di denaro determinata in criptovaluta non può richiedere l'adempimento della prestazione in moneta avente corso legale[42]. Al contrario, il debitore dell'obbligazione pecuniaria determinata in criptovaluta è tenuto ad adempiere corrispondendo la somma in criptovaluta, ma possiede la facoltà di adempiere pagando in moneta avente corso legale.

[42] Rimane, tuttavia, salva la possibilità per il creditore di agire, a fronte all'inadempimento del debito in moneta estera, per il risarcimento del danno richiedendo soddisfazione in moneta avente corso legale.

In senso critico rispetto alle conclusioni cui giunge l'arbitro, è stato sottolineato come alle parti è data la possibilità di stabilire consensualmente le regole inerenti ai pagamenti in criptovalute, prevedendo che l'adempimento vada realizzato attraverso la dazione di una data moneta virtuale: in tal caso, il rifiuto di ricevere il pagamento in moneta virtuale sarebbe illegittimo[43]. Peraltro, una volta perfezionatosi l'accordo relativamente al corrispettivo costituito da una determinata moneta virtuale, detto accordo è vincolante per il creditore che non può più revocare il consenso prestato anticipatamente in ordine all'accettazione di quella determinata criptovaluta come strumento di pagamento[44].

Inoltre, sotto altro profilo, rimane sottotraccia un tema non toccato dall'arbitro: una volta ammesso che il creditore ha l'obbligo di richiedere il pagamento in criptovaluta così come negozialmente pattuito, il problema si sposta sulle modalità di esecuzione della sentenza, non essendo, come visto, la moneta virtuale concretamente aggredibile dal creditore.

6. Le criptovalute come strumenti finanziari

La prima occasione che la giurisprudenza di merito – segnatamente il Tribunale di Verona[45] – ha avuto per confrontarsi con la tematica in esame ha riguar-

---

[43] Così, M. Rubino de Ritis, *Obbligazioni pecuniarie e criptomoneta,* cit., il quale evidenzia la necessità per le parti di regolare compiutamente il rapporto con l'apposizione di specifiche clausole tra le quali quella di adeguamento monetario attraverso la quale limitare i rischi di oscillazione del valore dell'intervallo tra la costituzione e l'estinzione dell'obbligazione pecuniaria in moneta virtuale. Sul tema del tasso di cambio in criptovaluta al momento dell'estinzione dell'obbligazione, M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 204 e spec., 209.

[44] Ancora, M. Rubino de Ritis, Obbligazioni pecuniarie e criptomoneta, cit.

[45] Trib. Verona, 24 gennaio 2017, in *Banca, borsa, tit. cred.*, 2017, 471 con nota di M. Passaretta, Bitcoin*: il leading case italiano*. In particolare, alcuni investitori persone fisiche avevano acquistato da una società *promoter* di una piattaforma di diritto ucraino una certa quantità di moneta virtuale in cambio di moneta reale. Gli attori, tuttavia, lamentavano la nullità del contratto d'acquisto di *bitcoin* concluso con la società promotrice in conseguenza della violazione delle norme del codice del consumo (d.lgs. 6 settembre 2005, n. 206) che disciplinano e conformano gli obblighi di informazione al quale è tenuto il fornitore del servizio finanziario erogato. Il Tribunale di Verona qualifica l'attività della società promotrice del portale di acquisto e scambio di valute virtuali come prestazione professionale di servizi a titolo oneroso svolta in favore dei consumatori e, dunque, disciplinata dalla medesima legge di settore. L'attività svolta dal fornitore ricade, infatti, ad avviso del Tribunale, nell'ambito dell'erogazione dei servizi finanziari ai consumatori, poiché l'oggetto del contratto era stato l'acquisto di valuta virtuale (*bitcoin*), qualificabile alla stregua, appunto, di uno strumento finanziario. Ne deriva che, il fornitore il quale operi come promoter di una piattaforma digitale di investimenti, che abbia per oggetto la vendita di valute virtuali, è tenuto agli obblighi di

dato una ipotesi di acquisto di valuta virtuale attraverso una società promotrice finanziaria di una piattaforma di *crowfunding*.

Il Tribunale di Verona giunge a qualificare le criptovalute quali prodotti finanziari, ossia forme di investimento aventi un intrinseco valore finanziario[46], sulla base della considerazione che l'acquisto, il possesso e lo scambio di criptovalute possono comportare rischi significativi, soprattutto per coloro che ne fanno uso senza una adeguata conoscenza del fenomeno.

È stato, peraltro, osservato[47] che una simile qualificazione risulta in qualche modo problematica. Infatti, l'art. 1, secondo comma, d.lgs. 24 febbraio 1998, n. 58 (Testo unico delle disposizioni in materia di intermediazione finanziaria) pone un elenco tassativo, non suscettibile di applicazione analogica, dei diversi strumenti finanziari tra i quali non compare la moneta virtuale. In particolare, le criptovalute non rappresentano né un valore mobiliare, come è reso evidente dal fatto che non attribuiscono un diritto partecipativo in iniziative economiche ovvero un investimento in un fondo, né uno strumento del mercato finanziario, non essendo collegate ad una autorità governativa[48].

Più agevole appare, invece, la riconduzione delle criptovalute alla categoria dei prodotti finanziari in ragione dell'ampia definizione operata dall'art. 1, comma 1, lett. u), TUF secondo cui per «prodotti finanziari» si intendono gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria. Come è stato

---

informativa, specie precontrattuale, previsti dagli artt. 67-*quater, quinquies, sexies, septies, decies ed undecies*, del Codice del Consumo, nonché di quelli ulteriori previsti per gli investimenti ad alto rischio così come disciplinato dagli artt. 13, 14 e 15 dell'allegato 1 della Delibera Consob del 26 giugno 2013, n. 1859.

Questo, peraltro, il principio enunziato dalla decisione in esame: «l'operazione di cambio di valuta tradizionale contro unità della valuta virtuale bitcoin e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti è qualificabile dal lato dell'operatore come attività professionale di prestazioni di servizi a titolo oneroso, svolta in favore di consumatori. Ciò in quanto i bitcoin rappresentano uno strumento finanziario costituito da una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un software open source e ad una rete peer to peer».

[46] Più precisamente, la decisione in esame qualifica la criptovaluta e, in particolare, il *bitcoin* come uno «strumento finanziario per compiere una serie di particolari forme di transazioni *on-line*».

[47] D. Fauceglia, *La moneta privata. Le situazioni giuridiche di appartenenza e i fenomeni contrattuali*, cit., 1257, spec., nt. 13

[48] N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*, cit., 577; M. Passaretta, *Bitcoin: il* leading case *italiano*, cit., 476.

evidenziato[49], infatti, se i caratteri distintivi dell'investimento di tipo finanziario sono rappresentati da un impiego di capitali, da una aspettativa di rendimento e, soprattutto, da un rischio proprio dell'attività prescelta, direttamente correlato all'impiego di capitali, tali requisiti possono essere in qualche modo traslati anche alla criptovaluta, in quanto il soggetto interessato all'investimento, per ottenere la moneta virtuale, ha sostenuto un esborso di denaro, nell'aspettativa di ottenere un rendimento, non necessariamente corrispondente ad una somma di danaro maggiorata rispetto a quella investita, assumendo, così, su di sé un rischio connesso al capitale investito.

In altre parole, alla luce del fatto che «le criptovalute costituiscono uno strumento attraverso il quale è possibile effettuare particolari operazioni finanziarie altamente rischiose e alla luce dell'interesse degli investitori di lucrare sull'oscillazione dei cambi tra la moneta statale e le criptovalute (specialmente in periodi di particolari fluttuazioni congiunturali, le operazioni aventi ad oggetto criptovalute possono considerarsi prodotti finanziari. Pertanto, allo stato, può ritenersi il bitcoin un prodotto finanziario qualora venga acquistato con finalità di investimento, specie se a collocarlo tra il pubblico è un soggetto che professionalmente svolge attività di erogazione di servizi di investimento»[50].

La qualificazione delle criptovalute in termini di prodotti finanziari è stata in qualche modo recepita dalla giurisprudenza penale di legittimità[51]. Intervenuta

---

[49] Così, M. Passaretta, *Bitcoin:* il leading case *italiano*, cit., 477. Nel medesimo senso, R. Bocchini, Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, cit., 40; G. Rinaldi, Approcci normativi e qualificazione giuridica delle criptomonete, cit., 289 il quale evidenzia come al fine di collocare un rapporto economico all'interno dei prodotti finanziari occorre effettuare una indagine sulla causa in concreto dell'operazione alla ricerca delle finalità ad essa sottese: infatti, la natura finanziaria dell'investimento può essere valutata soltanto nell'ottica complessiva dell'operazione prospettata dall'offerente.

[50] D. Fauceglia, *La moneta privata. Le situazioni giuridiche di appartenenza e i fenomeni contrattuali,* cit., 1258, nt. 13 il quale, tuttavia, evidenzia che è però, difficile ammettere che le criptovalute, benché abbiano le caratteristiche dei prodotti finanziari, possano considerarsi a tutti gli effetti prodotti finanziari. Ad ora, infatti, appare difficile ammettere che il promoter, il fornitore di prodotti finanziari, possa esercitare la propria attività senza autorizzazione della Consob; posto che la legge riserva l'esercizio dell'attività bancaria e raccolta del risparmio (130, 131, d.lgs. 1° settembre 1993 n. 385, da ora T.U.B.), attività di prestazione di servizi di pagamento (art. 131-ter T.U.B.) nonché l'esercizio per la prestazione di servizi di investimento (art. 166 T.U.F.) ai soli soggetti legittimati.

[51] Ci si riferisce, in particolare, a Cass. pen., 17 settembre 2020, n. 26807. Un primo, breve commento della decisione richiamata, può leggersi in https://www.agendadigitale.eu a cura di F. Sarzana, *Bitcoin, il vero valore della sentenza della Cassazione su Bitcoingo.*
Merita, peraltro, di essere ricordato anche il successivo intervento della Corte di cassazione penale (Cass. pen., 26 ottobre 2022, n. 44378) che ha ribadito che la valuta virtuale deve essere considerata

a decidere, in sede cautelare, sul sequestro delle somme risultate collegate alla operazione di compravendita di bitcoin, attraverso un determinato network e poi attraverso un sito, che avrebbero determinato nel complesso, la commissione dei reati previsti dall'art. 166 tuf e dall'art. 648-*bis* c.p., la Corte di cassazione ha ritenuto che la qualificazione della criptovaluta in questione come prodotto di investimento era necessitata dal comportamento del venditore che aveva reclamizzato la vendita della moneta virtuale come proposta di investimento[52]. In altre parole, proprio in ragione dell'attività pubblicitaria svolta, la società offerente non si era comportata come un semplice intermediario, alla stregua di un cambiavalute, per la vendita, ma avrebbe svolto un ruolo attivo nell'informare e proporre investimenti, tra l'altro estremamente rischiosi, associati alle criptovalute[53].

---

strumento di investimento perché consiste in un prodotto finanziario, per cui deve essere disciplinata con le norme in tema di intermediazione finanziaria (art. 94 ss. t.u.f.), le quali garantiscono attraverso una disciplina unitaria di diritto speciale la tutela dell'investimento; pertanto, chi eroga detti servizi è tenuto ad un innalzamento degli obblighi informativi verso il consumatore, al fine di consentire allo stesso di conoscere i contenuti dell'operazione economico -contrattuale e di maturare una scelta negoziale meditata (fattispecie relativa alla sussistenza del reato di esercizio abusivo dell'attività finanziaria di cui all'art. 166 t.u.f., che nel caso concreto consisteva nella richiesta fondi online tramite finanziamento collettivo dichiaratamente pubblicizzata come offerta di investimento, e al sequestro preventivo di un wallet contenente 30 bitcoin ritenuti oggetto del delitto di autoriciclaggio di cui all'art. 648-ter c.p.).

[52] Si legge, in particolare, nella motivazione: «la vendita di *bitcoin* veniva reclamizzata come una vera e propria proposta di investimento, tanto che sul sito ove veniva pubblicizzata si davano informazioni idonee a mettere i risparmiatori in grado di valutare se aderire o meno all'iniziativa, affermando che "chi ha scommesso in bitcoin in due anni ha guadagnato più del 97%"; trattasi pertanto di attività soggetta agli adempimenti di cui agli artt. 91 e seguenti TUF, la cui omissione integra la sussistenza del reato di cui all'art. 166 comma 1 lett. c) TUF».

[53] Secondo la difesa dell'indagato, invece, l'attività di cambiavalute virtuale era stata definita dal D.Lgs. 90/17, delineando per i cambiavalute uno stato proprio e sottraendoli quindi al perimetro applicativo della normativa in materia di strumenti finanziari in quanto le valute virtuali non erano considerati prodotti da investimento, ma mezzi di pagamento (l'art. 1 comma 2 TUE prevede che "gli strumenti di pagamento non sono strumenti finanziari"); tale scelta era perfettamente coerente con l'ordinamento comunitario e, in particolare, con l'orientamento espresso dalla Corte di Giustizia UE nella sentenza pregiudiziale del 22 ottobre 2016 avente ad oggetto proprio le operazioni di cambio della valuta virtuale bitcoin contro valuta tradizionale, nella quale era stato chiarito che i bitcoin non avevano altre finalità oltre a quella di mezzo di pagamento; a fronte di tali dati era un fuor d'opera quanto affermato dal Tribunale, secondo cui i bitcoin costituiscono uno strumento finanziario, anche se lo stesso Tribunale sembrava perfettamente consapevole della assoluta incongruità della valutazione giuridica offerta, laddove compiva un generico ed impreciso riferimento ad "atti comunitari e provvedimenti Consob" e sovvertiva la gerarchia delle fonti del nostro ordinamento, ritenendo una decisione della Corte di Giustizia UE ed un decreto legislativo minusvalenti rispetto ad un parere della Banca Centrale Europea o ad un parere della Consob o ancora ad una direttiva comunitaria priva di effetto per i cittadini perché non ancora recepita dall'ordinamento interno.

In questa prospettiva, che potrebbe dirsi funzionale e soggettiva (perché prende in esame la funzione impressa all'operazione dal soggetto acquirente la criptovaluta), l'acquisto e la vendita di monete virtuali – ove oggetto di attività professionale – verrebbero ad essere disciplinate dalle norme in tema di intermediazione finanziaria. In particolare, la società *promoter* della piattaforma di scambio di valute virtuali – ascrivibile al ruolo del fornitore, ossia a qualunque persona fisica o giuridica, soggetto pubblico o privato, che, nell'ambito delle proprie attività commerciali o professionali, è il fornitore contrattuale dei servizi finanziari oggetto di contratti a distanza – è soggetta a tutti gli obblighi informativi in favore dell'investitore[54].

Tuttavia, quello che appare problematico in una simile ricostruzione deriva dal fatto che non appare logico che il motivo dell'acquisto e, dunque, il motivo che spinge una parte alla stipulazione di un contratto avente un determinato oggetto possa determinare la stessa qualificazione giuridica di quell'oggetto e, dunque, comportare l'applicazione di una disciplina settoriale di tutela dell'investitore. D'altra parte, nei singoli casi pratici che possono venire in rilievo, può divenire assai difficoltoso l'accertamento di quel motivo e, quindi, distinguere tra l'acquisto finalizzato ad un investimento e quello parificabile ad uno scambio (tra monete o valori).

7. Le criptovalute come beni giuridici

Nel dibattito sulla natura giuridica delle criptovalute, una parte della dottrina e della giurisprudenza, preso atto della impossibilità per esse di svolgere le

---

In altre parole, a qualificare l'attività prestata non come volta alla vendita di strumenti finanziari, ma come vendita di valute (ancorché non aventi corso legale), il reato di cui all'art. 166 tuf sarebbe stata non ravvisabile.

[54] Questi obblighi informativi sono stati così sintetizzati da M. Passaretta, *Bitcoin:* il leading case *italiano*, cit., 480: a) informare il consumatore in maniera inequivocabile circa il fine commerciale perseguito dal fornitore, *promoter* di una piattaforma online di investimenti; b) informare in modo chiaro e comprensibile attraverso qualunque mezzo adeguato alle tecniche a distanza, prima della conclusione del contratto ovvero subito dopo per il tramite dell'invio delle condizioni contrattuali, al fine di consentire una informazione dettagliata circa: l'identità del fornitore, l'identità del professionista che agisce nei confronti del consumatore, l'iscrizione del fornitore o della piattaforma di investimento online in un registro pubblico, anche analogo a quello previsto dall'art. 50-quinquies, comma 2o, del t.u.f. (la quale, per essere effettuata, generalmente necessita di una autorizzazione amministrativa), le principali caratteristiche del servizio finanziario offerto, il meccanismo di formazione del prezzo, i rimedi che sono attribuiti dall'ordinamento e la legislazione sulla quale il fornitore intende strutturare il rapporto con il consumatore; c) accrescere il livello di consapevolezza dell'investitore sull'alto rischio collegato all'investimento in valute virtuali.

funzioni tipiche della moneta, benché convenzionale, di unità di conto e riserva di valore, per via dell'estrema volatilità, nonché della mancanza di potere liberatorio nei pagamenti, è giunta a qualificare le monete virtuali come «beni immateriali»[55] ovvero come «beni fungibili»[56], oggetto, comunque, di trasferimenti e di transazioni. In questa prospettiva, si è osservato che le monete virtuali sono sia consumabili in ragione del loro uso (quando vengono spese) sia fungibili perché tutte le monete appartenenti alla stessa specie hanno la stessa natura e qualità, in quanto appartenenti e derivanti dal medesimo protocollo informatico[57].

Anche la qualificazione delle monete virtuali come beni giuridici[58] ai sensi dell'art. 810 c.c. non va esente da critiche e da difficoltà concettuali di inquadramento.

---

[55] T.A.R. Lazio, 27 gennaio 2020, in Soc., 2020, 566 con nota di N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*.

[56] Trib. Firenze, 21 gennaio 2019, in Banca, borsa, tit. cred., 2021, 385 con nota di V. De Stasio, Prestazione di servizi di portafoglio digitale relativi alla valuta virtuale "nanocoin" e qualificazione del rapporto tra prestatore e utente; in Dir. internet, 2019, 119 con nota di M. Krogh, La responsabilità del gestore di piattaforme digitali per il deposito e lo scambio di criptovalute; in Contr., 2019, 661 con nota di D. Fauceglia, Il deposito e la restituzione delle criptovalute; in Giustiziacivile.com con nota di M. Passeretta, Servizi di custodia e gestione di criptovalute: il fallimento del prestatore di servizi.

[57] Sulla scorta di tali premesse, il Tribunale di Firenze ha, quindi, affermato che deve essere qualificato come deposito irregolare il rapporto tra utente e prestatore di servizi di portafoglio digitale (cd. "*exchange*"), quanto alla conservazione e collocazione delle criptovalute all'interno della piattaforma, quando le criptovalute vengano conservate in *hot wallet* (portafogli configurati sui server di produzione, cioè quelli connessi a Internet e su cui sono attivi gli utenti e il portafoglio dell'*exchange*) dove queste rimangono a disposizione dell'*exchange* che ne gestisce i prelievi o le compravendite tra criptomonete diverse e tali portafogli siano controllati esclusivamente tramite il codice dell'*exchange* oppure da coloro che detengano le chiave private dei *wallet* e gli utenti non hanno la possibilità di gestire autonomamente i loro fondi senza fare uso delle funzionalità della piattaforma perché: a) gli indirizzi di deposito assegnati a ciascuno sono in breve tempo svuotati per far convogliare le criptomonete verso gli indirizzi principali dell'*exchange*; b) gli utenti non dispongono delle chiavi private: senza autenticarsi sulla piattaforma, che deve essere attiva e funzionante, per gli utenti è impossibile svolgere attività di trading, ma anche, semplicemente, ritirare i propri fondi.

[58] Propende per una simile ricostruzione, G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 292 secondo il quale detto inquadramento «è quello che appare più idoneo a racchiudere le ibride e multiformi caratteristiche di entità tanto "inafferrabili" da un punto di vista classificatorio». D'altra parte, secondo tale A., la qualificazione delle criptovalute come beni giuridici è, sostanzialmente, implicita nelle prescrizioni di cui al d.lgs. n. 90 del 2017 ed alla dir. 2018/843/UE. Se è vero, infatti, che le normative italiana ed europea segnano un esplicito e positivo riconoscimento delle valute virtuali quali mezzi di scambio, appare evidente che una determinata entità può essere un mezzo di scambio (vale a dire un qualcosa suscettibile di essere venduto, acquistato e scambiato) soltanto se è, ancor prima, un bene in senso giuridico. In senso non dissimile, D. Fauceglia, *La moneta privata. Le situazioni giuridiche di appartenenza e i fenomeni contrattuali*, cit., 1254.

In particolare, una simile qualificazione è resa incerta dalla duplice circostanza che esse non sono né beni materiali, non esistendo nella realtà, se non come sequenza numerica su di un computer, né beni immateriali, in ragione dell'inesistenza di una norma che le riconosca come tali e del conseguente contrasto con il principio di tipicità di tali beni[59].

Con riferimento al primo aspetto, va richiamato il principio del *numerus clausus* dei diritti reali[60] con la conseguenza che non può esistere un bene giuridico se l'ordinamento non prevede su di esso una situazione giuridica soggettiva attiva[61]. Inoltre, con riferimento al secondo profilo, i beni sono solo le cose che possono formare oggetto di diritti e, dunque, essi sono, per loro natura, corporali[62]. Né, in diversa prospettiva, potrebbe considerarsi la criptovaluta un bene immateriale in quanto opera dell'ingegno, perché semmai tale è soltanto il software del protocollo utilizzato, la cui titolarità sorge in capo all'inventore[63].

8. Il fondamento «pattizio» dell'utilizzo delle criptovalute

A prescindere dal corretto inquadramento del fenomeno, è certo che, allo stato, le valute virtuali non hanno corso legale e, pertanto, non devono per

---

[59] P. Iemma, N. Cuppini, La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze, cit., 7; R. Bocchini, Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, cit., 30; R. Razzante, Bitcoin: tra diritto e legislazione, cit., 383;

[60] Peraltro, recentemente ribadito da Cass., sez. un.,27 dicembre 2020, n. 28972.

[61] N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*, cit., 574 i quali evidenziano come, al momento, le valute virtuali ricevono considerazione solo nella disciplina antiriciclaggio come possibile vettore di proventi illeciti o per finanziamento del terrorismo. Da essa non potrebbe giungersi ad un riconoscimento normativo quale bene, a norma dell'art. 810 c.c. Nello stesso senso, V. De Stasio, *Prestazione di servizi di portafoglio digitale relativi alla valuta virtuale "nanocoin" e qualificazione del rapporto tra prestatore e utente,* cit., 405.

[62] Ancora, V. De Stasio, *Prestazione di servizi di portafoglio digitale relativi alla valuta virtuale "nanocoin" e qualificazione del rapporto tra prestatore e utente*, cit., 406; N. De Luca – M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento,* cit., 574 secondo i quali è un'evidente forzatura identificare il bit circolante nell'etere nella impressione di esso in una memoria di silicio: oggetto di circolazione non è il supporto fisico, ma solo ciò che esso consente di leggere.

[63] V. De Stasio, *Prestazione di servizi di portafoglio digitale relativi alla valuta virtuale "nanocoin" e qualificazione del rapporto tra prestatore e utente*, cit., 406 il quale osserva che nessuna opera creativa sottostà, invece, all'acquisto della moneta virtuale da parte di coloro che ne sono titolari e che, a stretto ragionare, sono titolari esclusivamente di una iscrizione in un registro virtuale, il cui valore economico dipende, in termini del tutto funzionali, dall'esistenza, in fatto, di un mercato delle suddette criptovalute (*rectius*: iscrizioni) e/o dalla disponibilità di altri soggetti a riceverle in corrispettivo di altre entità di sicuro valore economico.

legge essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie. Nulla osta, però, che esse possano essere utilizzate per acquistare beni o servizi nel caso in cui il venditore o il prestatore dei servizi sia disponibile ad accettarle. In altre parole, mentre la moneta avente corso legale si impone a tutti con la conseguenza che il pagamento eseguito con essa non è utilmente rifiutabile dal creditore (art. 1277 c.c.) e la sua misura è vincolata ad un valore economico legale determinato da un referente oggettivo, l'utilizzo della criptovaluta deriva esclusivamente da una fonte pattizia, nel senso che le parti di uno scambio si obbligano reciprocamente ad eseguire e, dunque, ad accettare un determinato pagamento attraverso la dazione della moneta virtuale[64].

Come è stato efficacemente affermato[65], si «prescinde da qualunque rappresentazione o movimentazione di moneta avente corso legale essendo, appunto, il "corso", la qualificazione non "legale" ma solo pattizia, frutto di una convenzione (nella forma dell'adesione ad un sistema "aperto" e poi elettronico) tra i partecipanti. In questa prospettiva, manca il riconoscimento della moneta da parte di un terzo, essendo il *bitcoin* destinatario di un potere di acquisto pattiziamente (ma non arbitrariamente) riconosciuto e, così, opponibile e "consumabile" solo tra chi pattiziamente lo riconosce: l'Autorità della "qualificazione" è pattizia, rendendo evidente la rilevanza della "percezione" dell'affidabilità della funzione solutoria del sistema; e legittimando una ricostruzione del pagamento con *bitcoin* quale *datio in solutum* tra aderenti ad un contratto plurilaterale normativo».

In definitiva, sulla base di una specifica convenzione (e soltanto sulla base di essa), l'accettazione in pagamento di monete virtuali deve ritenersi ammessa. D'altra parte, come visto, la stessa Banca d'Italia, nelle sue avvertenze più volte richiamate, ha evidenziato che «l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale».

Peraltro, nel dibattito in ordine alla possibilità di qualificare le valute virtuali come mezzo di pagamento (lecito) è intervenuta anche la Corte di Giustizia

---

[64] La fonte pattizia dell'utilizzo della criptovaluta è riconosciuta dalla Risoluzione dell'Agenzia delle entrate in precedenza menzionata ove si evidenzia che essa si «fonda sull'*accettazione volontaria* da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio *indipendentemente da un obbligo di legge*».

[65] M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Diritto della banca e del mercato finanziario*, 2017, 679, spec., 701

dell'Unione europea[66]. Secondo i giudici comunitari, la valuta virtuale a flusso bidirezionale *bitcoin*, che sarà cambiata contro valute tradizionali nel contesto di operazioni di cambio, da un lato, non può essere qualificata come «bene materiale» ai sensi dell'articolo 14 della direttiva IVA, e, dall'altro, non costituisce né un titolo che conferisce un diritto di proprietà su persone giuridiche né un titolo di natura comparabile. Ciò perché la valuta virtuale non ha altre finalità oltre a quella di un mezzo di pagamento. La Corte, così, perviene a considerare le criptovalute come «mezzo di pagamento contrattuale», concludendo che le operazioni di cambio di diversi mezzi di pagamento non ricadono nella nozione di «cessione di beni», costituendo, invece, prestazioni di servizi ai sensi dell'articolo 24 della direttiva IVA.

In definitiva, la Corte di Giustizia europea pone in risalto la funzione di strumento convenzionale di pagamento delle criptomonete, ritenendola assorbente rispetto alle altre componenti[67].

Se non vi sono dubbi in ordine alla liceità dell'uso della moneta virtuale nell'ambito di uno scambio tra soggetti che quell'uso hanno pattiziamente accettato, maggiori criticità emergono laddove la dazione di esse coinvolge non solo e non tanto la posizione delle parti di uno scambio, ma, soprattutto, la posizione dei terzi. Tale ipotesi si verifica allorquando la moneta virtuale diviene oggetto, tanto in sede di costituzione che in sede di aumento di capitale, di conferimento in una società di capitali.

Ma prima di affrontare il tema del rapporto tra criptovalute e fenomeno societario, occorre esaminare le difficoltà che le monete virtuali pongono in sede di aggressione del patrimonio del debitore.

9. Criptovalute: la nuova frontiera della segregazione patrimoniale?

Le maggiori problematiche che oggi concernono l'utilizzo delle criptomonete riguardano essenzialmente, da un lato, all'anonimato che circonda il pro-

---

[66] Corte di Giustizia dell'Unione Europea, sent. 22 ottobre 2015, nella causa C-264/2014, *Skatteverket c. David Hedqvist*. Decidendo su un caso riguardante l'applicabilità delle esenzioni dall'imposta sul valore aggiunto, previste dalla direttiva 2006/112/CE (c.d. direttiva IVA), nei confronti degli operatori che svolgono attività di cambio di valuta virtuale contro valuta tradizionale, la Corte di Giustizia ha stabilito che l'articolo 2, paragrafo 1, lettera c), della direttiva 2006/112/CE del Consiglio, del 28 novembre 2006, relativa al sistema comune d'imposta sul valore aggiunto va interpretato nel senso che costituiscono prestazioni di servizi effettuate a titolo oneroso, ai sensi di tale disposizione, operazioni, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale «bitcoin» e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti.

[67] G. Rinaldi, *Approcci normativi e qualificazione giuridica delle criptomonete*, cit., 277.

prietario e l'utilizzatore dei *bitcoin* e, dall'altro ma conseguentemente, alla impossibilità tecnica di aggredire quel «bene».

Con riguardo alla questione della individuazione del soggetto proprietario di *bitcoin*, va osservato come le operazioni in moneta virtuale sono sicuramente «tracciabili» in senso informatico, rimanendo nel registro pubblico traccia indelebile della circostanza che un (ignoto) detentore di una chiave privata, corrispondente ad una data chiave pubblica, ha trasferito *bitcoin* ad altro ignoto detentore di altra chiave privata corrispondente, a sua volta, ad altra chiave pubblica. Tuttavia, tutti questi processi si basano non sul concetto di «identificazione» del soggetto, ma su quello di «verifica» delle credenziali informatiche.

Ma ammesso che si riesca a conoscere l'identità del titolare della moneta virtuale, ciò non consentirebbe ancora di ritenere possibile l'aggressione di quel «bene» da parte dei creditori. Infatti, soltanto il proprietario di quella moneta virtuale è a conoscenza delle *password* necessarie per accedere al sistema e, dunque, di disporre di essa[68]. In tal senso anche un eventuale sequestro o confisca dei supporti fisici sui quali sia conservato il *wallet*, in assenza delle relative chiavi di accesso (che potrebbero non rinvenirsi su quei supporti), impedirebbe comunque l'aggressione da parte dei creditori sociali. In altre parole, tanto l'utilizzo (volontario) quanto la pignorabilità della moneta virtuale implicano la cooperazione del titolare dei *bitcoin*[69].

---

[68] M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., 663, spec., 675. Sulla pignorabilità della moneta virtuale e sulle difficoltà riscontrabili, cfr., G. Finocchiaro, *Le cripto-valute come elementi patrimoniali assoggettabili alle pretese esecutive dei creditori*, in *Riv. dir. proc.,* 2019, 87 il quale conclude (104) evidenziando che «la normativa ad oggi vigente è del tutto inadeguata a consentire ai creditori di assoggettare all'azione esecutiva le cripto-valute che possono comporre il patrimonio del proprio debitore: in particolare (…), le due criticità maggiori risiedono nell'individuare tali beni, nonché – soprattutto – nel sottrarli alla circolazione giuridica e alla disponibilità del debitore esecutato. La prima difficoltà, a ben vedere, è di mero fatto e non è molto diversa da quella che incontra il creditore il cui debitore abbia occultato il proprio patrimonio composto soltanto di denaro contante o oggetti preziosi: a ben vedere, anzi, la ricerca di cripto-monete nel c.d. «cyber-spazio» o «realtà virtuale», è forse più semplice che quella della cassa del tesoro sepolta chissà dove ed, in ogni caso, come si è visto, il legislatore ha già previsto dei rimedi applicabili anche alle cripto-valute. L'altro ostacolo, invece, discende direttamente dalle peculiarità tecniche proprie delle cripto-valute: pare, pertanto, auspicabile *de iure condendo* che il legislatore italiano introduca espressamente l'obbligo, sanzionato penalmente, di rivelare all'ufficiale giudiziario le proprie chiavi digitali, onde consentire il trasferimento delle cripto-valute. In difetto di collaborazione del debitore esecutato, infatti, le cripto-valute paiono risultare de facto sottratte dalla responsabilità patrimoniale di cui all'art. 2740, comma 1°, cit.».

[69] Più precisamente, del titolare della chiave privata. Così, correttamente, M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., 675. In senso almeno, in parte contrario, M. Rubino De Ritis, *Obbligazioni pecuniarie in criptomoneta* secondo il quale, malgrado l'utilizzo

In altre parole, l'anonimato che caratterizza il possesso della valuta virtuale non solo impedisce il pignoramento della valuta virtuale, ma rende la stessa una posta patrimoniale la cui gestione e le cui vicende circolatorie (volontarie e coattive) presuppongono necessariamente la collaborazione volontaria del possessore della chiave privata, impedendo di fatto ogni interferenza coattiva da parte di una terza autorità.

In questa prospettiva, il rischio attuale è che l'utilizzo di moneta virtuale divenga una nuova forma, non consentita dall'ordinamento, di «segregazione» patrimoniale ovvero di creazione di un patrimonio separato da quello del soggetto titolare della criptovaluta che, solo, può disporne. È, infatti, appena il caso di notare che un soggetto potrebbe convertire tutto o parte del proprio patrimonio in monete virtuali raggiungendo l'effetto di essere comunque titolare (peraltro, direttamente e non già attraverso ulteriori schermi) di beni che, tuttavia, non sono utilmente aggredibili dai terzi creditori.

10. Criptovalute e fenomeno societario

Una vicenda portata all'attenzione degli organi giudiziari di Brescia (Tribunale e Corte di appello) ha consentito di aprire una riflessione in ordina alla utilizzabilità della moneta virtuale quale bene da conferire in una società di capitali[70].

---

di pseudonimi, è, però, possibile tracciare le singole operazioni, per cui l'identità che si cela dietro un indirizzo resta ignota finché non sia realizzata un'operazione attraverso la *blockchain*. L'utente è identificabile, infatti, attraverso le credenziali di registrazione per l'ottenimento di quel dato indirizzo o portafoglio. Il che consente di ricostruire i soggetti coinvolti nelle transazioni e, a differenza dei pagamenti in contanti, risalire in modo completo alle movimentazioni di ciascun utente.

[70] Questo, in estrema sintesi, il caso. Una società a responsabilità limitata deliberava di aumentare il proprio capitale sociale da € 10.000,00 ad € 1.410.000,00 mediante conferimento in natura, in parte, di talune opere d'arte e, in parte, di un certo numero di unità della criptovaluta denominata "*One Coin*". Il notaio, tuttavia, riteneva la deliberazione non «sufficientemente dotata dei requisiti di legittimità per ordinarne una immediata e incondizionata iscrizione» nel registro delle imprese, censurando, in particolare, il conferimento della moneta virtuale, con riferimento al quale egli rappresentava che le criptovalute, stante la loro volatilità, «non consentono una valutazione concreta del *quantum* destinato alla liberazione dell'aumento di capitale sottoscritto» né di valutare «l'effettività (*quomodo*) del conferimento». L'amministratore unico della società interessata proponeva, dunque, ricorso ai sensi del terzo comma dell'art. 2436 c.c. con il quale chiedeva al tribunale di ordinare l'iscrizione nel registro delle imprese all'uopo evidenziando, tra l'altro, che: la perizia esibita in sede di conferimento aveva confermato il valore, quale bene, della criptovaluta; il conferente aveva provveduto al trasferimento della disponibilità della moneta virtuale in capo alla società; la stessa agenzia delle entrate consente di attribuire valore economico alle criptovalute; se è vero che possono costituire oggetto di conferimento i crediti e taluni beni immateriali, non sussistono

Sia il Tribunale che la Corte di appello di Brescia sono pervenuti al rigetto del ricorso proposto dalla società avverso al rifiuto dell'iscrizione da parte del notaio: tuttavia, i due organi giudicanti hanno seguito percorsi argomentativi significativamente diversi che, ai fini della successiva analisi, appare opportuno richiamare.

Il Tribunale – se, da un lato, non affronta la questione concernente la astratta idoneità della categoria di beni rappresentata dalle c.d. "criptovalute" a costituire elemento dell'attivo idoneo al conferimento nel capitale di una società a responsabilità limitata – ritiene che il bene concretamente conferito, la criptovaluta denominata "*One Coin*", non soddisfa il requisito di cui al secondo comma dell'art. 2464 c.c.

Il giudicante dapprima individua i requisiti fondamentali di qualunque bene al conferimento: 1) nella idoneità a essere oggetto di valutazione, in un dato momento storico (prescindendosi dall'ulteriore problematica connessa alle potenziali oscillazioni del valore); 2) nell'esistenza di un mercato del bene in questione, presupposto di qualsivoglia attività valutativa, che impatta poi sul grado di liquidità del bene stesso e, quindi, sulla velocità di conversione in denaro contante; 3) nella idoneità del bene a essere "bersaglio" dell'aggressione da parte dei creditori sociali, ossia l'idoneità a essere oggetto di forme di esecuzione forzata. Il tribunale precisa, poi, che tali requisiti devono essere specificatamente indicati nella relazione di stima di cui all'art. 2465 c.c., tanto che, se pure deve escludersi che il giudice possa sostituire integralmente la propria valutazione di merito a quella dell'esperto, deve necessariamente ammettersi la facoltà per il giudice di sindacare la completezza, logicità, coerenza e ragionevolezza delle conclusioni raggiunte dall'esperto.

---

ragioni ostative alla liceità del conferimento delle criptovalute; la criptovaluta denominata "*One Coin*" è una moneta virtuale scambiata su mercati non regolamentati soggetta alla valutazione da parte di operatori specializzati. Il Tribunale di Brescia, con decreto 25 luglio 2018 rigettava il ricorso con una decisione confermata, sebbene con una motivazione diversa, dalla Corte di appello della medesima città con provvedimento del 24 ottobre 2018.

I due provvedimenti sono stati commentati da: G. Romano, *Conferimenti societari e criptovalute. Un binomio complicato*, in *IlSocietario,* 2019; M. Natale, *Dal "cripto-conferimento" al "cripto-capitale"?*, in *Banca, borsa, tit. cred*., 2019, II, 741; F. Urbani, *Il conferimento di cripto-attività al vaglio della giurisprudenza di merito*, in *Giur. comm.,* 2020, II, 887; M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, in *Notariato,* 2018, 663; F. Bartolini, *Requisiti della criptovaluta, ex art. 2464, comma 2, c.c., ai fini del conferimento nel capitale sociale di una s.r.l.*, in *IlSocietario,* 2018. In generale, su questa tematica, G. Gitti, *I conferimenti di criptoattività*, in *Contr. impr.,* 2020, 1289 e M. Rubino De Ritis, *Conferimenti di criptomonete in società a responsabilità limitata*, in M. Irrera (a cura di), *La società a responsabilità limitata: un modello transtipico alla prova del Codice della crisi. Studi in onore di Oreste Cagnasso,* Torino, 2020, 314.

Ebbene, nel caso sottoposto alla attenzione del tribunale, la perizia di stima prodotta non presentava un livello di completezza e affidabilità sufficiente per consentire un esauriente vaglio di legittimità della delibera in esame. In particolare, come evidenziato dal giudicante, la valuta virtuale denominata "*One Coin*" non è ad oggi presente in alcuna piattaforma di scambio tra criptovalute ovvero tra criptovalute e monete aventi corso legale, con la conseguente impossibilità di fare affidamento su prezzi, determinati dalle dinamiche di mercato, attendibili. Tale criptovaluta risulta scambiata in un unico mercato costituito da una piattaforma dedicata alla fornitura di beni e servizi riconducibile ai medesimi soggetti ideatori della criptovaluta, nel cui ambito funge da mezzo di pagamento accettato. L'autoreferenzialità della moneta e, dunque, dell'elemento dell'attivo conferendo è incompatibile con il livello di diffusione e pubblicità di cui deve essere dotata una moneta virtuale che aspira a detenere una presenza effettiva sul mercato.

Inoltre, quanto alla idoneità del bene a essere oggetto di aggressione da parte dei creditori, manca, ad avviso del tribunale, nella perizia qualunque riferimento alle modalità di esecuzione di un ipotetico pignoramento della criptovaluta oggetto di conferimento, profilo da ritenere decisamente rilevante nella fattispecie, alla luce della notoria esistenza di dispositivi di sicurezza ad elevato contenuto tecnologico che potrebbero, di fatto, renderne impossibile l'espropriazione senza il consenso e la collaborazione spontanea del debitore.

In definitiva, secondo il Tribunale, emerge una moneta virtuale ancora in fase sostanzialmente embrionale che – allo stato – non presenta i requisiti minimi per poter essere assimilata a un bene suscettibile, in concreto, di una valutazione economica attendibile.

La soluzione accolta dalla Corte di appello di Brescia, sebbene analoga nelle sue conclusioni, differisce assai quanto a contenuto delle motivazioni.

La Corte ha inteso riconsiderare la stessa premessa giuridica da cui muoveva il Tribunale e, in particolare, l'astratta idoneità della criptovaluta a costituire un elemento dell'attivo idoneo al conferimento nel capitale di una società a responsabilità limitata, muovendo, invece, la propria argomentazione dall'esame della funzione di pagamento che, al pari del denaro, assume la criptovaluta, con la conseguenza che la seconda, proprio sul piano funzionale, può essere assimilata al primo, ancorché, strutturalmente, presenti caratteristiche proprie dei beni mobili: la criptovaluta, al pari della moneta avente corso legale (euro), serve per fare acquisti, sia pure non universalmente, ma in un mercato limitato, ed in tale ambito opera quale marcatore (cioè quale contropartita), in termini di valore di scambio, dei beni, servizi, o altre utilità ivi oggetto di contrattazione.

L'effettivo valore economico della "criptovaluta" non può in conseguenza determinarsi con la procedura di cui al combinato disposto dei due articoli 2464

e 2465 c.c. – riservata a beni, servizi ed altre utilità, diversi dal danaro – non essendo possibile, per le ragioni sopra esposte, attribuire valore di scambio ad un'entità essa stessa costituente elemento di scambio (contropartita) nella negoziazione. Non è, d'altro canto, dato conoscere, allo stato, un sistema di cambio per la "criptovaluta", che sia stabile ed agevolmente verificabile, come per le monete aventi corso legale in altri Stati (dollaro, yen, sterlina etc.). Discende che non è, pertanto, possibile assegnare alla criptovaluta un controvalore certo ed effettivo in euro, essendo a tal fine precluso, per le ragioni sopra esposte, il ricorso alla mediazione della perizia di stima.

Secondo la Corte, in conclusione, va condivisa l'affermazione del notaio secondo il quale «le criptovalute, attesa la loro volatilità, non consentono una valutazione concreta del *quantum* destinato alla liberazione dell'aumento di capitale sottoscritto».

Come appena evidenziato, mentre il Tribunale – pur consapevolmente non ponendosi il problema dell'astratta conferibilità di monete virtuali – aveva qualificato quel conferimento come conferimento in natura, la Corte di appello ha equiparato la criptovaluta alla moneta reale.

A questo punto, non ci si può esimere dal muovere dalla distinzione tra conferimenti in denaro ed in natura. Secondo la dottrina, nella categoria dei conferimenti in danaro devono essere inquadrate tutte – ma solo – le ipotesi in cui l'oggetto del conferimento sia rappresentato da strumenti monetari: quelli cioè che, limitandosi ad esprimere il valore di altri beni in ragione del proprio valore nominale, non si prestano, proprio per ciò, ad essere a loro volta valutati[71].

Al contrario, rientrano nella categoria residuale dei conferimenti in natura tutti quei conferimenti aventi ad oggetto entità diverse dagli strumenti monetari e, dunque, le monete straniere, i titoli di stato e gli altri strumenti del mercato monetario, poiché tali ipotesi presentano tutte, accanto al valore nominale, un valore reale (di ammontare in via di principio diverso dal primo), del quale si tratterà al momento di determinare l'importo all'esito di una apposita valutazione, al pari di quanto accade in ordine ad ogni altro conferimento in natura[72]. In altre parole, per danaro, ai fini del conferimento, deve intendersi esclusivamente la moneta legale o la moneta bancaria in senso stretto espressa nella valuta nazionale dell'euro, se il capitale nominale non è espresso in altra valuta. L'idoneità del denaro a fungere da misura del valore (senza necessità che si ponga il problema di un suo diverso "valore d'uso" che coincide con il "valore di scambio") spiega la sua piena idoneità a costituire il

---

[71] G. Ferri, *art. 2342,* in *Commentario al codice civile*, diretto da E. Gabrielli, *Della società, dell'azienda, della concorrenza*, a cura di D.U. Santosuosso, Torino, 2015, 756 ss., spec., 761.

[72] G. Ferri, *art. 2342*, cit., 762 ss.

capitale reale, come perfetto *pendant* della cifra del capitale nominale al passivo. Essendo il capitale nominale al passivo espresso normalmente nella valuta nazionale, conferimenti in valuta diversa da quello in cui è espresso il capitale nominale ed il bilancio andrebbero assoggettati alle ben diverse regole del conferimento in natura, mediante stima ed integrale liberazione, ovvero "cambiati", nel solo caso (attualmente teorico) di valute la cui conversione in euro avvenga a un tasso legale fisso[73].

Tanto chiarito, la Corte di appello ha ritenuto che la criptovaluta deve essere considerata, con riguardo al profilo funzionale, come moneta essendo destinata allo scambio di beni e di servizi. Tuttavia, in assenza di un sistema di scambio idoneo a determinare l'effettivo valore ad una data determinata, non è possibile ad essa attribuire, da un lato, un controvalore in euro e, di conseguenza, una valutazione concreta del *quantum* destinato alla liberazione dell'aumento di capitale sottoscritto.

La motivazione della Corte di appello non appare convincente, risultando in qualche modo contraddittoria. Infatti, già l'assimilazione, «a tutti gli effetti», tra criptovaluta e denaro è smentita dall'art. 1, comma 2, lett. o) d.lgs., 21 novembre 2007, n. 231 che definisce come denaro contante «le banconote e le monete metalliche, in euro o in valute estere, aventi corso legale».

Ma anche a tralasciare questo aspetto definitorio, non è chiaro se, data per ammessa l'assimilazione sopra richiamata, la Corte abbia ritenuto non conferibile la criptovaluta, intesa quale denaro, in astratto ovvero soltanto con riferimento alla criptovaluta oggetto del caso di specie. Infatti, la corte si limita ad annotare che «non è (…) possibile assegnare alla criptovaluta – in assenza di un sistema di scambio idoneo a determinare l'effettivo valore ad una certa data – un controvalore certo in euro, essendo a tal fine precluso, per le ragioni sopra esposte, il ricorso alla mediazione della perizia di stima». Non è chiara, dunque, la soluzione che la Corte avrebbe adottato ove l'oggetto di quel conferimento fosse stato un determinato numero di *bitcoin* che, al contrario, hanno tassi di conversione in valute legali regolamentati in mercati ufficiali[74].

Sotto altro profilo, l'argomentazione della Corte è, in qualche modo, tautologica poiché – anche a volere ammettere che la criptovaluta sia assimilabile alla valuta – proprio l'assenza di un sistema di «cambio» imponeva al collegio di vagliare comunque l'astratta conferibilità di essa come «valore dell'attivo» stimabile attraverso appunto la perizia. D'altra parte, se le valute straniere possono costituire l'oggetto di un conferimento in natura, nulla dovrebbe ostare a che, una volta parificata,

---

[73] V. De Stasio – G. Nuzzo, *art. 2342,* in *Le società per azioni. Codice civile e leggi complementari,* diretto da P. Abbadessa e G.B. Portale, Milano, 2016, 357.

[74] Come nota correttamente M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., 674.

sotto il profilo funzionale, moneta avente corso legale e moneta virtuale, possa pervenirsi al conferimento di questa ultima attraverso un procedimento di stima.

In questa prospettiva, una volta che il legislatore ha (d.lgs., 21 novembre 2007, n. 231, art. 1, co. 2, lett. qq.) definito la valuta virtuale come la «rappresentazione digitale di valore» utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente, l'impossibilità di conferire moneta virtuale dovrebbe trovare basi più solidi che non la semplice assenza di un sistema di cambio. In altre parole, l'assenza di un sistema di cambio, se da una parte può impedire la qualificazione del conferimento come eseguito in danaro, dall'altra, non impedisce *tout court* la possibilità che quella rappresentazione digitale di valore possa essere essa stessa oggetto di un conferimento in natura.

Più lineare – seppure nella assoluta problematicità che circonda la tematica – la motivazione del tribunale di Brescia secondo il quale, presupposta l'ascrivibilità astratta di un simile conferimento alla categoria dei conferimenti in natura, quella specifica criptomoneta ("*one coin*"): 1) non è ad oggi presente in alcuna piattaforma di scambio tra criptovalute ovvero tra criptovalute e monete aventi corso legale; 2) risulta scambiata in un unico mercato riconducibile ai medesimi soggetti ideatori della criptovaluta; 3) non appare idonea ad essere oggetto di aggressione da parte dei creditori.

Orbene, prescindendo dalla specificità del caso concreto, occorre domandarsi se la soluzione del tribunale sarebbe stata diversa nel caso in cui oggetto del conferimento fosse stata una criptovaluta (ed il pensiero non può che rivolgersi nuovamente al *bitcoin*), diffusa su larga scala e che risulta scambiabile con moneta avente corso legale secondo un rapporto di cambio. Appare evidente, infatti, che i dubbi indicati ai punti 1) e 2) sarebbero, in questo caso, certamente (e verrebbe da dire, facilmente) superabili.

Resterebbe, invece, da esaminare la questione sotto il profilo della possibile aggressione da parte dei creditori.

Limitando il discorso al solo tipo della società a responsabilità limitata, è noto che, ai sensi dell'art. 2464 c.c., possono essere oggetto di conferimento «tutti gli elementi dell'attivo suscettibili di valutazione economica».

La suscettibilità di valutazione economica va interpretata come idoneità a rappresentare un valore non solo per i soci, ma anche per i terzi, misurabile secondo parametri il più possibile oggettivi[75]. Secondo un primo orientamento,

[75] Avagliano, art. 2464, in L.A. Bianchi (a cura di), *Società a responsabilità limitata*, in *Commentario alla riforma delle società*, diretto da P. Marchetti – L.A. Bianchi – F. Ghezzi – M. Notari, Milano, 2008, 82; G. Zanarone, *Della società a responsabilità limitata*, in F.D. Busnelli (direttio da), *Il codice civile. Commentario fondato P. Schlesinger*, Milano, 2010, 217.

vi sarebbe coincidenza tra valutazione economica ed espropriabilità dei beni conferibili, dovendosi considerare valutabile economicamente solo ciò che possa essere oggetto di esecuzione forzata. Una simile ricostruzione, sbilanciata sulla funzione di garanzia del capitale, sembra superata dallo stesso art. 2464 c.c. laddove si ammette la conferibilità di opere e servizi: in questa prospettiva, la suscettibilità di valutazione economica va intesa, come è stato autorevolmente evidenziato, «quale sinonimo di alienabilità, vuoi forzosa che volontaria, vale a dire come possibilità che il bene conferito venga comunque convertito in denaro da destinarsi a sua volta a soddisfare i creditori: e ciò non solo in via diretta attraverso un processo esecutivo attivato da questi ultimi ma anche in via indiretta attraverso l'iniziativa della stessa società, abbia essa ad oggetto l'alienazione autonoma del singolo bene (non sempre possibile come nel caso dell'avviamento, della ditta, dei marchi) oppure l'alienazione dell'intero complesso aziendale in cui il medesimo è inserito»[76].

Va, quindi, verificata la compatibilità tra i principi ora indicati ed il conferimento di criptovalute. Ora, se è vero che il concetto espresso dall'art. 2464 c.c. non si risolve nella espropriabilità del bene (conferito), tuttavia, occorre chiedersi in che termini la moneta virtuale oggetto del conferimento sia suscettibile di essere convertita in denaro da destinarsi a soddisfare i diritti dei creditori e, quindi, in definitiva, sia idonea ad assolvere la funzione di garanzia patrimoniale ai sensi dell'art. 2740 c.c.

In questa indagine, non appare pleonastico osservare come la distinzione tra i concetti di espropriabilità e suscettibilità di valutazione economica sia stata ben presente nella disamina svolta dal Tribunale in primo grado secondo il quale non può, comunque, trascurarsi come la dimensione materiale del bene recuperi valenza quanto meno sotto il profilo della quantificazione del valore economico, dovendo per ciò stesso essere oggetto di analisi.

Ebbene, come si è visto precedentemente, le maggiori problematiche che investono l'utilizzo delle monete virtuali attengono, da un lato, all'anonimato che circonda il proprietario e l'utilizzatore dei *bitcoin* e, dall'altro ma conseguentemente, alla impossibilità tecnica di aggredire quel «bene». E va da sé che tali problematiche risultano amplificate nell'ambito di un fenomeno, quale quello societario, che non è costruito su un ordine binario (debitore-creditore), ma implica, di necessità, il coinvolgimento, almeno sotto il profilo dinamico, di terzi.

La combinazione dei due profili accennati – anonimato e impossibilità di pignoramento – rende assai difficoltosa la valutazione della moneta virtuale come posta dell'attivo patrimoniale, in quanto, come pure è stato correttamente osserva-

[76] G. Zanarone, *Della società a responsabilità limitata*, cit., 218.

to[77], l'incremento patrimoniale che deriverebbe dal conferimento della valuta virtuale stessa non rivestirebbe quei tratti oggettivi idonei a fondare un apprezzabile affidamento da parte dei terzi, ma creerebbe una segregazione assoluta ed impenetrabile del valore a tutto vantaggio del (solo) possessore della chiave privata.

In definitiva, appare difficile immaginare la possibilità di conferire criptovalute fin tanto che non sarà trovato un rimedio alle due criticità – anonimato ed impignorabilità – sopra accennate[78].

---

[77] M. Krogh, *L'aumento di capitale nelle s.r.l. con conferimento di criptovalute*, cit., ivi.

[78] Come si è avuto modo di osservare in sede di commento alle decisioni degli Uffici giudiziari di Brescia (G. Romano, *Conferimenti societari e criptovalute. Un binomio complicato*, cit.), ove si ammetta la possibilità di eseguire conferimenti in criptovaluta, assume un particolare rilievo il sistema dei controlli sulla stima operata dal soggetto incaricato. Tuttavia, nella società a responsabilità limitata, la disciplina è, sotto più profili, frammentaria e lacunosa non rinvenendosi norme analoghe a quelle presenti nella società per azioni. Ebbene, in primo luogo, il controllo preventivo di legalità spetta, in via esclusiva, al notaio in ragione della circostanza che il rispetto delle previsioni in materia di stima rientra tra le condizioni per la costituzione della società ex art. 2329 n. 2: il notaio, dunque, dovrà verificare non solo l'esistenza della stima, ma anche delle condizioni minime per l'assolvimento della sua funzione tipica, pur senza potere sindacarne il merito; egli potrà, dunque, sindacare l'incompletezza della stima, l'«intrinseca razionalità» e la «formale logicità e coerenza» della motivazione attraverso cui i criteri di valutazione sono stati scelti, con esclusione di ogni valutazione in ordine alla congruità della valutazione (in questo senso, M. Miola, *Stima dei conferimenti in natura e di crediti,* in A.A. Dolmetta e G. Presti (a cura di), *S.r.l. Commentario, dedicato a Portale*, Milano, 2011, 204). La norma di cui all'art. 2465 c.c. non richiama l'art. 2343 commi 3 e 4 c.c. che, da un lato, assegnano agli amministratori il compito, nel termine di centottanta giorni dalla iscrizione della società, di controllare le valutazioni contenute nella relazione di stima e procedere, in caso di fondati motivi, alla revisione di essa e, dall'altro, ove il valore dei beni o dei crediti conferiti sia inferiore di oltre un quinto a quello per cui avviene il conferimento, dispongono che la società debba proporzionalmente ridurre il capitale sociale ovvero che il socio possa versare la differenza in danaro o recedere dalla società. Una parte della dottrina ritiene non percorribile la via dell'applicazione analogica di dette norme alla società a responsabilità limitata attesa la diversificazione, sul punto, dei due regimi e la duplice circostanza, da un lato, che il mancato richiamo sarebbe il frutto della volontà (espressa anche nella legge delega) di semplificare le procedure di valutazione dei conferimenti in natura e, dall'altro, che la certezza del valore conferito sarebbe garantito dall'attestazione giurata di un soggetto iscritto in appositi albi (così, F. Tassinari, *I conferimenti e la tutela dell'integrità del capitale sociale*, in C. Caccavale, F. Magliulo, M. Maltoni, F. Tassinari (a cura di), *La riforma della società a responsabilità limitata*, Milano, 2007, 102). In questa prospettiva, non sussisterebbe più l'obbligo, per gli amministratori, di controllare le valutazioni contenute nella relazione e, ove sussistano fondati motivi, di procedere alla revisione della stima. Appaiono evidenti i pericoli derivanti dall'accoglimento di un simile orientamento. Infatti, dovrebbe concludersi nel senso che l'ordinamento non avrebbe previsto alcun rimedio per il caso in cui il valore imputato a capitale sia «gonfiato» rispetto a quello effettivo, ipotesi questa che lede tanto gli interessi dei creditori in quanto porta allo svuotamento della garanzia patrimoniale quanto quelli dei soci relativamente ad inique ripartizioni delle quote sociali. Proprio per tali ragioni, le

11. Criptovalute e moneta elettronica

Esaminate le diverse ricostruzioni apparse in dottrina ed in giurisprudenza in ordine alla natura delle valute virtuali, è ora necessario procedere ad esaminare la distinzione esistente tra queste, la moneta elettronica ed i servizi di pagamento[79].

Secondo l'art. 1, secondo comma, lett. h-*ter*, d.lgs., 1 settembre 1993, n. 385 (tub), per moneta elettronica[80] si intende «il valore monetario memorizzato elet-

---

conclusioni ora evidenziate hanno lasciato insoddisfatta parte della dottrina. Secondo alcuni autori, in particolare, la mancata riproduzione (o richiamo) nella disciplina della società a responsabilità limitata dei co. 3 e 4 dell'art. 2343 costituirebbe una vera e propria lacuna dell'ordinamento che potrebbe essere colmata attraverso l'applicazione analogica di dette disposizioni, in ragione della non eccezionalità dei rimedi e dell'*eadem ratio* che giustifica l'estensione del principio. Pertanto, anche nella società a responsabilità limitata, in caso di emersione della minusvalenza dell'apporto, la società dovrebbe ridurre proporzionalmente il capitale sociale, variando la partecipazione del conferente e salva la possibilità di questi di versare la differenza in denaro o recedere dalla società (G. Zanarone, *Della società a responsabilità limitata*, cit., 242). Altri autori, invece, giungono alle medesime conclusioni prendendo le mosse dal generale dovere di diligenza (art. 2476 c.c.) il quale, necessariamente, implica l'esistenza di un obbligo, gravante sull'organo gestorio, di verificare la corretta formazione del capitale. Gli amministratori, dunque, verificata l'insufficienza del conferimento rispetto al valore imputato al capitale, dovrebbero ingiungere al socio di provvedere all'integrazione, pena l'applicazione della disciplina dell'art. 2466 (M. Miola, *Stima dei conferimenti in natura e di crediti,* 206).

Ebbene, a volere ammettere la conferibilità di monete virtuali, gli amministratori, anche di una società a responsabilità limitata, dovrebbero sotto la propria responsabilità nei confronti della società e dei terzi procedere ad un riesame della stima operata dal perito al fine di verificare la veridicità e la congruità dei valori ivi espressi e, dunque, di evitare una non corretta formazione del capitale sociale.

[79] Su moneta elettronica e servizi di pagamento, E. Cecchinato, *I servizi di pagamento,* in F. Aratari – G. Romano, *Il diritto bancario oggi: aspetti sostanziali e processuali*, Milano, 2023, 365; M. Onza, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Diritto della banca e del mercato finanziario*, 2017, 679; F. Molterni, *Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione,* in F. Maimeri, M. Mancini (a cura di), Le nuove frontiere dei servizi bancari e di pagamento tra PSD 2, criptovalute e rivoluzione digitale, Quaderni di Ricerca Giuridica della Banca d'Italia, 2019, 185; F. Porta, *Obiettivi e strumenti della PSD2*, in F. Maimeri, M. Mancini (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento tra PSD 2, criptovalute e rivoluzione digitale, Quaderni di Ricerca Giuridica della Banca d'Italia*, 2019; V. Profeta, *I* third party provider*: profili soggettivi ed oggettivi*, in F. Maimeri, M. Mancini (a cura di), Le nuove frontiere dei servizi bancari e di pagamento tra PSD 2, criptovalute e rivoluzione digitale, Quaderni di Ricerca Giuridica della Banca d'Italia, 2019; C. Venanzoni, *I servizi bancari on line,* in F. Aratari – G. Romano, *Il diritto bancario oggi: aspetti sostanziali e processuali*, Milano, 2023, 415;

[80] Sulla moneta elettronica, in generale, P. Cuomo, *La moneta elettronica,* in M. Cian, C. Sandei, *Diritto del Fintech,* Milano, 2020, 195 ss.; O. Troiano, *La moneta elettronica come servizio di pagamento*, in S. Sica, P. Stanzione, V. Zeno Zencovich, *La moneta elettronica*, Milano, 2006, 2006.

tronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'art. 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente»[81].

La moneta elettronica è, dunque, un valore monetario rappresentato da un credito memorizzato elettronicamente o magneticamente, emesso dietro ricevimento di fondi di pari valore, utilizzabile per effettuare pagamenti nei confronti di soggetti diversi da quello emittente. L'emissione di moneta elettronica – che avviene trasformando immediatamente in moneta elettronica i fondi ricevuti dal richiedente (art. 114-*quater* tub) – è oggetto di una attività di riserva a favore di banche e di intermediari finanziari, denominati istituti di moneta elettronica (Imel). Il valore monetario depositato si riduce automaticamente ogni qualvolta il soggetto depositante effettua un pagamento.

Come è stato efficacemente evidenziato, «l'elemento distintivo della moneta elettronica all'interno dei mezzi di pagamento elettronici sta in ciò che una disponibilità monetaria, quantitativamente predeterminata, è registrata all'interno di un supporto elettronico (e-wallet), tipicamente costituito da un microchip inserito all'interno di una smart card in possesso del titolare (c.d. borsellino elettronico), oppure da un file memorizzato nell'hard disk di un personal computer del titolare o, in alternativa, all'interno di una memoria remota (cd. moneta digitale o software money). Una volta memorizzata all'interno di uno di tali supporti, la disponibilità monetaria ivi registrata è suscettibile di trasferimento istantaneo e diretto da parte del titolare, pagatore, ad uno o più terzi, beneficiari dell'operazione di pagamento»[82].

Peraltro, si possono distinguere due tipi fondamentali di moneta elettronica, il primo basato sull'uso di carte prepagate ed il secondo sull'uso di strumenti elettronici o telematici. Nel primo caso, l'utente effettua in anticipo un versamento a favore dell'emittente, cioè deposita un certo valore monetario presso l'emittente; quest'ultimo carica il valore equivalente al deposito sulla carta a microcircuito, che sarà poi utilizzabile per acquistare beni o servizi prodotti dall'emittente stesso o, in linea di principio, anche da altri. Nel caso del secondo tipo

[81] La medesima disposizione ha cura di precisare che non costituisce moneta elettronica: 1) il valore monetario memorizzato sugli strumenti previsti dall'art. 2, comma 2, lettera m), del decreto legislativo 27 gennaio 2010, n. 11; 2) il valore monetario utilizzato per le operazioni di pagamento previste dall'art. 2, comma 2, lettera n), del decreto legislativo 27 gennaio 2010, n. 11.

[82] P. Cuomo, *La moneta elettronica*, cit., 196; O. Troiano, *La moneta elettronica come servizio di pagamento*, cit., 99.

di moneta elettronica, basata su tecnologie telematiche e informatiche, si ha un deposito (registrazione) di un certo valore monetario in una memoria di computer o in una smart card; dopodiché i pagamenti avvengono inviando ordini di trasferimento di fondi per via telematica.

Il valore è, poi, espresso in unità di moneta legale: tuttavia, secondo l'orientamento più diffuso, la moneta elettronica non può essere assimilata direttamente al denaro, ma va ricondotta ai mezzi di pagamento basati sull'interposizione di intermediari finanziari, come è reso manifesto dalla disciplina che qualifica e regola la moneta elettronica come un credito sempre rimborsabile del detentore nei confronti dell'intermediario emittente[83].

Comunque, la moneta elettronica si sostanzia pur sempre in un meccanismo di pagamento sostitutivo del denaro contante (circolante e depositi bancari in conto corrente) che implica il ricorso a strumenti tecnici di tipo elettronico. Così qualificata, in estrema sintesi, la moneta elettronica, appare evidente la differenza con la moneta virtuale: nel primo caso, infatti, il valore memorizzato elettronicamente è, pur sempre, un valore monetario, espresso, cioè, in una unità di conto avente corso legale, mentre la seconda non rappresenta in forma digitale le comuni valute a corso legale (euro, dollaro, ecc.) e, inoltre, non è emessa o garantita da una banca centrale o da un'autorità pubblica e generalmente non è regolamentata[84].

Altrimenti detto, se gli elementi caratterizzanti della valuta virtuale sono costituiti, in positivo, dall'essere una rappresentazione di un valore digitale e, in negativo, dal non essere emessa o garantita da una banca centrale o da un ente pubblico e dal non essere legata ad una valuta avente corso legale, diviene giocoforza distinguerla dalla moneta elettronica, definita dalla stessa legge,

---

[83] P. Cuomo, *La moneta elettronica*, cit., 198 secondo il quale la moneta elettronica si avvicina alla figura dei crediti disponibili basati su rapporti con intermediari aventi ad oggetto la fornitura del servizio di cassa. La disposizione dei fondi, secondo l'A., non avviene attraverso un ordine impartito dal titolare all'intermediario presso il quale il primo detiene i propri fondi e la successiva attuazione dell'ordine da parte del secondo: il trasferimento dei fondi si realizza direttamente in base all'accordo tra pagatore e beneficiario, secondo lo schema della cessione del credito. Tale cessione rispecchia ed attua la destinazione alla circolazione impressa al supporto monetario dell'emittente il quale, con l'atto di creazione della moneta elettronica, si obbliga a corrispondere la quantità di disponibilità monetaria memorizzata all'interno del supporto elettronico non già a colui che ne ha versato la provvista, ma a colui che ne ha acquistato la titolarità dal primo. In questo senso, conclude l'A., è significativo che la legge definisca la moneta elettronica come un credito "emesso per effettuare operazioni di pagamento" (art. 1, coma 1, lett. h-*ter* tub).

[84] V. De Stasio, *Verso un concetto europeo di moneta legale: monete virtuali, monete complementari e regole di adempimento*, cit., 753.

come «valore monetario memorizzato elettronicamente» che rappresenta un credito nei confronti dell'emittente[85].

12. Conclusioni

Le criptovalute hanno assunto – sia pure in ambiti ancora limitati – un significativo rilievo sociale: non è possibile al momento attuale prevedere lo sviluppo futuro, se cioè l'utilizzo delle valute virtuali crescerà ulteriormente diffondendosi su larga scala tra gli operatori economici (con conseguente incremento del loro valore) ovvero se, al contrario, si risolverà in una nuova bolla speculativa, al pari, per citare il primo caso studiato, della bolla dei bulbi dei tulipani olandesi del XVII secolo[86].

---

[85] F. Molterni, *Criptovaluta, valuta digitale, moneta elettronica e modelli di circolazione,* cit., 194, secondo il quale la differenza fra la moneta elettronica e la valuta virtuale sarebbe netta: la moneta elettronica rappresenta un valore monetario ed è tale in ragione del fatto che, per un verso, «documenta» un credito del detentore della moneta elettronica nei confronti dell'emittente, conseguente alla consegna di fondi in favore di quest'ultimo, per altro verso, l'ammontare del credito è pari «al valore nominale» della somma di valuta o moneta reale ricevuta dall'emittente. Tuttavia, secondo l'A., la realtà presenta casi di contaminazioni fra il modello della valuta virtuale e quello della moneta elettronica, laddove vi sia un legame tra la criptovaluta ed una valuta legalmente istituita. Infatti, meno distante dal modello della moneta elettronica è quella valuta digitale o *virtual cryptocurrency* come il *Tether*, i cui creatori hanno sempre assicurato ai clienti di accumulare riserve di un dollaro per ogni Tether creato. In questo modo, il *Tether* converte contanti e denaro bancario in valuta digitale e fissa o vincola il valore della valuta che emette al prezzo delle valute nazionali come il dollaro USA, l'euro e lo yen. In tale dimensione, il «legame» fra la *virtual currency* e la «valuta avente corso legale» è tale da indurre, se non giustificare, nei clienti dell'emittente di *Tether*, e di valute virtuali simili, un affidamento nel loro valore (monetario) comparabile o simile a quello delle monete elettroniche di cui all'art. 1, punto 2, della direttiva 2009/110/CE.

[86] In seguito all'esportazione di bulbi di tulipano dalla Turchia all'Europa nella seconda metà del XVI secolo, in pochi anni, l'Olanda divenne il paese maggiormente coinvolto nella loro coltivazione e diffusione. La selezione di varietà di tulipani rare e la lentezza riproduttiva della specie resero questi fiori un bene di lusso molto desiderato negli ambienti più ricchi della società europea e, di conseguenza, determinarono un crescente aumento del loro valore: l'acquisto di bulbi di tulipani divenne ben presto un investimento sicuro e redditizio condotto con contrattazioni in aste pubbliche o private. All'inizio del XVII secolo il commercio dei bulbi di tulipani divenne una vera e propria "bolla" che beneficiava anche della espansione marittima e commerciale dell'Olanda.
A partire dal 1635, divennero frequenti le transazioni sui bulbi di tulipani, non più appannaggio solo delle classi più ricche, ma rivolte anche ai commercianti delle fasce meno abbienti della società. Tali transazioni consistevano nell'acquisto di "diritti sul bulbo" con un acconto sul prezzo finale, da corrispondere alla fioritura, che avveniva dopo mesi dall'iniziale accordo. Durante questo lungo periodo di tempo, questi accordi si rimodulavano in lunghe catene di negoziazioni tra fioristi e commercianti prive di garanzie sia sui venditori che sugli acquirenti. Queste contrattazioni

Come evidenziato in precedenza, ad oggi, il fondamento dell'utilizzo di una qualsivoglia criptovaluta è meramente pattizio derivando dall'autonomia privata che l'ordinamento riconosce alle parti di un negozio giuridico. Ma se tale autonomia appare facilmente riconoscibile se si guarda all'uso della moneta virtuale in modo, per così dire, «atomistico» o «binario» in quanto essenzialmente rivolto alle parti (e solo a loro) di un determinato rapporto negoziale, più critica è la situazione nei fenomeni, come quello societario, ove, soprattutto con riferimento alle regole che garantiscono la corretta formazione del capitale sociale, vengono in rilievo non tanto e non solo la posizione delle parti che consegnano e che ricevono una determinata valuta virtuale, ma anche e soprattutto la posizione dei terzi che su quel capitale sociale fanno affidamento.

Di tali criticità – e delle difficoltà concettuali di inquadramento sistematico delle criptovalute – costituiscono espressione i provvedimenti giurisdizionali finora conosciuti. Come evidenziato nel corso della trattazione, i problemi, allo stato non risolti, che rendono problematica l'utilizzazione della moneta virtuale (almeno su grande scala) sono rappresentati dall'anonimato che circonda il proprietario e l'utilizzatore della chiave privata e dall'impossibilità di sottoporre quei beni (e, dunque, quei valori) ad esecuzione forzata.

Come sempre quando si tratta di innovazioni sociali fondate su nuove tecnologie, il legislatore, sia nazionale che comunitario, si trova «in ritardo» rispetto alla necessità, oramai avvertita come ineludibile, di una regolamentazione: è, perciò, auspicabile che l'ordinamento giuridico intervenga riappropriandosi della funzione di «governare» i fenomeni sociali ed economici, senza che siano proprio questi ultimi a dettare le regole degli operatori.

La strada sembra, però, inesorabilmente tracciata.

Ducunt fata volentem, nolentem trahunt.

---

consequenziali ebbero come effetto un rialzo dei prezzi ingiustificato rispetto al prodotto commercializzato e alimentarono l'illusione di un facile guadagno. Il 5 febbraio 1637 centinaia di lotti di bulbi furono venduti per una cifra equivalente a circa 5 milioni di euro.

La bolla esplose quando un'asta andò deserta: i prezzi crollarono, le domande di acquisto divennero insufficienti per le tante richieste di vendita. In tale contesto, gli impegni per acquisti a cifre elevatissime danneggiavano gli acquirenti a favore dei contadini. La lobby dei fioristi ottenne di veder modificati i contratti in modo tale che gli acquirenti potessero recedere dal contratto con una penale minima, a danno dei produttori.

Maria Tecla Rodi*

Crypto-asset e mercato finanziario: le "STO" tra regolazione finanziaria e diritto privato

Sommario: 1. Premessa: tra regolazione finanziaria e diritto privato. – 2. Cos'è e come nasce un *crypto-asset*. I concetti chiave. – 3. Quali e quante forme può assumere un *crypto-asset*. Le ICO. – 4. L'emissione di *security token* e le STO.

1. Premessa: tra regolazione finanziaria e diritto privato

In un articolo pubblicato nel febbraio 2021 la professoressa Cherednychenko[1], nell'interrogarsi sulle sfide cruciali che legislatori, corti, autorità di regolazione finanziaria e altri attori, a livello nazionale e unionale, devono affrontare per la tutela degli interessi pubblici e privati in un ambiente finanziario sempre più digitale, rileva come gli sforzi per individuare soluzioni innovative per affrontare le tensioni tra il bene comune e le preferenze individuali in questo nuovo contesto trovino un serio ostacolo nel divario che sussiste, nel discorso politico quanto nel dibattito dottrinale, tra le due aree del diritto che plasmano la dimensione dei mercati finanziari, ossia la regolamentazione finanziaria e il diritto privato.

L'autrice invoca dunque la necessità di riponderare sistematicamente il ruolo del diritto privato nel panorama dei mercati finanziari e più in generale il suo rapporto con la regolamentazione pubblica, pensandoli non come due universi paralleli, ma piuttosto come due facce della stessa moneta, ognuna delle quali ha un ruolo fondamentale da svolgere nella tutela degli interessi pubblici e privati.

In questo senso, sollecita un esame della regolamentazione finanziaria dell'UE attraverso la lente del "diritto privato", nell'assunto che questo esercizio consentirebbe di svelare una complessa interazione tra la dimensione normativa, quella contrattuale e quella dei rimedi di diritto privato che è necessario comprendere meglio per poter regolamentare al meglio i mercati finanziari. Invita, in parallelo,

---

* Le opinioni contenute nel presente scritto sono espresse a titolo esclusivamente personale e non impegnano in alcun modo l'Autorità di appartenenza (Consob).

[1] O.O. Cherednychenko, "*Two Sides of the Same Coin: EU Financial Regulation and Private Law*", in *European Business Organization Law Review*, 2021, vol. 22, pp. 147 ss.

a un esame del diritto privato attraverso la lente "regolatoria" europea, al fine di "innescare" il suo potenziale a contribuire agli obiettivi della regolamentazione finanziaria, realizzando allo stesso tempo la giustizia tra le parti private.

Tenendo a mente questo invito – e dunque la necessità di considerare regolazione finanziaria e diritto privato nella loro indistricabile connessione, in ogni esercizio di analisi giuridica dei fenomeni di mercato – può riscontrarsi come alla data in cui si scrive sono stati aggiunti importanti tasselli regolatori nella direzione della complessiva *digitalizzazione* dell'ambiente finanziario nell'Unione europea.

La proposta della Commissione europea per l'introduzione di un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito – che ha come obiettivo quello di introdurre una sorta di "*sandbox*" per i *crypto-asset* che ricadano nella disciplina esistente applicabile agli strumenti finanziari – è sfociata nel Regolamento (UE) 2022/858[2], applicabile a far data dal 23 marzo 2023 (il regolamento *Pilot regime*) (cfr. *infra*).

Il negoziato interistituzionale sulla proposta della Commissione europea per un regolamento sul mercato dei *crypto-asset*, il cui obiettivo è quello di introdurre un quadro normativo esaustivo per la regolamentazione e la vigilanza di emittenti e prestatori di servizi relativi ai *crypto-asset* che non ricadono nella disciplina degli strumenti finanziari, è sfociato nella pubblicazione del regolamento MiCA nel mese di giugno 2023[3].

I "tasselli" menzionati fanno parte di un disegno unitario (il *Digital Financial Package*), il cui schizzo originario si rinviene in una consultazione della Commissione europea conclusasi nel mese di marzo del 2020 con circa duecento contributi. Alla consultazione ha fatto seguito la pubblicazione del *Report of the High Level Forum on the Capital Markets Union*, che ha riunito 28 esperti (provenienti dall'industria e dal mondo accademico) con l'obiettivo di elaborare raccomandazioni rivolte alla Commissione europea per rilanciare e favorire il processo di realizzazione della *Capital Market Union*. Nella *Recommendation On Crypto/Digital Assets and Tokenisation* il Forum ha invitato la Commissione a intervenire sulla normativa europea, tra l'altro al fine di chiarire quali *crypto-asset* ricadono nell'ambito applicativo della normativa attualmente vigente; e

---

[2] Regolamento (UE) 2022/858 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e che modifica i regolamenti (UE) n. 600/2014 e (UE) n. 909/2014 e la direttiva 2014/65/UE.

[3] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937.

ad adottare un nuovo normativo per *crypto-asset* che non ricadano nell'ambito di applicazione della normativa europea.

Il *Digital Financial Package* è stato presentato come un pacchetto "multi-intervento", composto da quattro proposte, supportate da una "*strategia*". Comprende, oltre alle iniziative legislative citate, anche una proposta di regolamento sulla c.d. *Digital Operational Resilience* (DORA) e la proposta di adozione di una direttiva modificativa delle direttive di settore, al fine di uniformare agli interventi citati il quadro normativo unionale complessivo.

Tra le priorità della strategia *Digital Finance* della Commissione europea risulta quella di assicurare che la cornice regolatoria UE faciliti l'innovazione nell'interesse dei consumatori e dell'efficienza di mercato, intercettando il potenziale delle innovazioni basate sull'uso della tecnologia a registro distribuito, con l'obiettivo dichiarato di consentire un'"abilitazione" del mercato dei *crypto-asset* entro il 2024.

2. Cos'è e come nasce un *crypto-asset*. I concetti chiave

Sia il regolamento *Pilot* che il regolamento MiCA si occupano, dunque, di creare una cornice regolatoria per il fenomeno dei "*crypto-asset*". Ma cosa si intende con *crypto-asset?* Secondo la definizione data dall'articolo 3(1)(2) del regolamento MiCA, un "*crypto-asset*" è la rappresentazione digitale di un valore o di un diritto, che può essere trasferita e archiviata elettronicamente, utilizzando una "*tecnologia a registro distribuito*" o una tecnologia similare.

La definizione di tecnologia a registro distribuito (o "DLT") rilevante ai fini dell'applicazione del MiCA è quella introdotta nel regolamento *Pilot regime*: una tecnologia che consente il funzionamento e l'uso dei "registri distribuiti", ossia archivi di informazioni in cui sono registrate le operazioni, condivisi da una serie di "nodi di rete" e sincronizzati tra essi. I nodi di rete sono dispositivi o applicazioni informatiche che detengono una copia (completa o parziale) delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito e che devono raggiungere un "accordo" per la convalida di ciascuna operazione. Le regole e le procedure per il raggiungimento di questo accordo rappresentano il "meccanismo di consenso".

Nella famiglia di tecnologie DLT compaiono anche le tecnologie "*blockchain*", in cui il *database* si presenta come una serie di fasci di transazioni disposte cronologicamente, i cc.dd. blocchi[4].

[4] Secondo lo *standard* ISO 22739, che detta il vocabolario tecnico di base, la *blockchain* è un "*distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links*".

Token è dunque, da un punto di vista tecnico, la rappresentazione digitale di un insieme di dati, ma la parola viene utilizzata come sinonimo di "*crypto-asset*".

Il *crypto-asset* è il protagonista – e l'esito – di un processo c.d. di "tokenizzazione", ossia di generazione di una "scritturazione digitale".

In via di semplificazione, il concetto di *tokenizzazione* può essere inteso in due accezioni: può essere associata a un bene esistente in natura un'"immagine", dunque una fotografia, digitale (e in questo caso il *crypto-asset* sarà considerato "non nativo"), oppure può essere conferito il rango di "bene" a una registrazione digitale alla quale non corrisponde in natura un bene "sottostante" (e in questo caso si parlerà di *token* "nativo").

"Generare" un *token* su un registro distribuito vuol dire concretamente definire in uno *smart contract* tutte le sue caratteristiche essenziali: uno *smart contract* è, secondo l'attuale definizione data dagli *standard* tecnici ISO, un "programma per computer memorizzato in un sistema a registro distribuito in cui l'esito di qualsiasi esecuzione del programma è registrato sul registro distribuito medesimo". Gli "effetti" da registrare sul registro distribuito costituiranno tipicamente la "transazione", che rappresenta l'esito predefinito dal codice dello *smart contract*[5].

Una tecnologia a registro distribuito, e in particolare la *blockchain*, consente di trasferire i *token* in maniera sicura e su base *peer-to-peer* (ossia, potenzialmente, senza necessità di un'intermediazione tra gli attori di una transazione), garantendo la tracciabilità dei movimenti e l'immutabilità delle registrazioni[6]. La costruzione di un *token*, a sua volta, può essere del tutto personalizzata, ma esistono degli *standard* che mirano a facilitarne la programmazione[7].

---

[5] In questi termini si esprime lo *standard* ISO/TR 23455, ove si sottolinea altresì che l'interpretazione del termine "*smart contract*" si è evoluta dal suo significato originale e che, sfortunatamente, manca attualmente una comprensione condivisa della locuzione. Si sottolinea come tale locuzione non si riferisca necessariamente a un *contratto* in senso giuridico, ma come essa debba essere interpretata nel senso di indicare un'applicazione distribuita che automatizza le transazioni sfruttando la sicurezza dei sistemi DLT. Non dovrebbe invece essere dedotto dall'utilizzo dell'espressione alcun significato legale implicito. Sul dibattito dottrinale in merito alla qualificazione degli *smart contract* cfr. M. Maugeri, *Smart Contracts e disciplina dei contratti*, Bologna, 2021.

[6] Si legge nello *standard* ISO 22739: "*Blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records*".

[7] Si pensi al famoso ERC-20, che introduce uno *standard* per la costruzione di *token* fungibili sulla *blockchain* Ethereum. Una descrizione esemplificativa della funzionalità fornite dall'ERC-20 è fornita dal sito di Ethereum: trasferire *token* da un *account* a un altro; richiedere il saldo corrente di *token* di un *account*; richiedere la quantità totale di *token* disponibile sulla rete; approvare che una quantità di *token* di un *account* possa essere spesa da un *account* di terze parti. Cfr. https://ethereum.org/it/developers/docs/standards/tokens/erc-20/.

3. Quali e quante forme può assumere un *crypto-asset*. Le ICO

In un *warning* emesso il 17 marzo 2022 dalle autorità di vigilanza europee (ESMA, EBA ed EIOPA) – in cui le stesse rilevano il crescente interesse degli investitori verso i *crypto-asset*, "valute virtuali" comprese, e l'emergere di nuove tipologie di *crypto-asset* e di prodotti e servizi correlati[8], manifestando il proprio timore che, nelle more dell'adozione del nuovo quadro regolatorio summenzionato, un numero crescente di consumatori acquisti tali *beni* con l'aspettativa di un rendimento ma senza la consapevolezza degli alti rischi connessi – si legge che il numero di *crypto-asset* emessi a quella data ammonta a circa 17000 (fonte "*coinmarketcap*"). Una cifra significativa in cui confluiscono *crypto-asset* difficilmente riconducibili ad unità quanto alle loro caratteristiche, ma tutti accomunati dall'essere il prodotto di un processo di tokenizzazione.

Nel dibattito pubblico, giuridico e non, i *crypto-asset* sono stati tradizionalmente differenziati, dal momento della loro comparsa sulla scena globale, sulla base delle loro "funzioni", per ragioni di semplicità.

Ciò sebbene sia spesso difficile collocare distintamente ciascuno in una delle categorie individuate.

Si distingue così, in via di prima approssimazione, tra:

- *payment token* (o *token* di pagamento), destinati ad essere utilizzati come un mezzo di scambio (è il caso delle "criptovalute");
- *investment token* (o *token* di investimento), che attribuiscono al titolare diritti di natura partecipativa nell'emittente o diritti di credito nei confronti del medesimo e sono tipicamente acquistati con un'aspettativa di profitto;
- *utility token* (o *token* di utilità), che possono essere utilizzati nella rete dell'emittente per l'acquisto di beni o servizi e che sono tipicamente acquistati senza un'aspettativa di profitto.

Le categorie richiamate si rivelano, a un'osservazione della realtà, non sempre mutualmente esclusive e nella pratica si assiste a loro possibili ibridazioni.

Esiste, inoltre, un'ulteriore *summa divisio* concettuale, che discrimina tra *fungible token* e *non-fungible token*, questi ultimi connotati da caratteristiche di "unicità" e pertanto non assimilabili ad esemplari della stessa specie[9]. Il regolamento MiCA introduce tre categorie di *crypto-asset*, che sono distinte tra loro e assoggettate a requisiti diversi perché percepite come implicanti rischi di natura diversa. Tali categorie non coincidono con i tre macro-contenitori sopra illustrati.

---

[8] Si tratta, ad esempio, di strumenti derivati che hanno come attività sottostante *crypto*-attività e polizze vita collegate a *crypto-asset*.

[9] Sui *non fungible token* si veda F. Annunziata, A. Conso, *NFT – L'arte e il suo doppio*, Milano, 2022.

La prima sottocategoria proposta da MiCA è costituita da *crypto-asset* che mirano a stabilizzare il loro valore facendo riferimento a una sola valuta ufficiale, cui sono "ancorati" (*token* di moneta elettronica o "*e-money token*").

La funzione di tali criptovalute è molto simile alla funzione della moneta elettronica. Come la moneta elettronica, questi *crypto-asset* sono il surrogato elettronico di monete e banconote e possono essere utilizzati per effettuare pagamenti.

Nella seconda sottocategoria di *crypto-asset* ci sono gli "*asset-referenced token*", ossia *crypto-asset* che mirano a mantenere un valore stabile facendo riferimento a altri valori o diritti, o a una combinazione di essi, comprese una o più valute ufficiali. Questa sottocategoria ricomprende tutte le criptovalute ulteriori rispetto a quelle che si qualificano come *token* di moneta elettronica, il cui valore sia ancorato a un bene.

La terza sottocategoria ricomprende tutti i *crypto-asset* che non siano *asset-referenced token* o *token* di moneta elettronica, e include gli "*utility token*", definiti come *crypto-asset* esclusivamente destinati a consentire l'accesso a un bene o a un servizio fornito dall'emittente del *crypto-asset*.

Il regolamento MiCA esclude dal suo ambito di applicazione, tra l'altro, i *crypto-asset* che siano strumenti finanziari ai sensi della direttiva MiFID. Si prevede in proposito che l'ESMA emani degli orientamenti al fine di definire le condizioni e i criteri per la qualificazione dei *crypto-asset* come strumenti finanziari. Essi continueranno a essere disciplinati dal quadro preesistente, perché sulla base del principio *same business-same activity-same rule* l'elemento tecnologico non vale come elemento differenziale.

Per quanto concerne gli NFT, emerge dal testo di MiCA la volontà di non far ricadere nell'alveo applicativo del regolamento *crypto-asset* unici e non fungibili con altri *crypto-asset*, inclusi quelli espressione di arte digitale e oggetti da collezione, il cui valore è attribuibile sulla base delle caratteristiche esclusive di ciascun esemplare, così come i *crypto-asset* che rappresentino servizi o beni materiali unici e non fungibili, come gli immobili. Sono tuttavia salve le ipotesi in cui, nonostante il *nomen* con cui si presentano, i "sedicenti" NFT si prestino ad utilizzi che in concreto li rendano fungibili[10].

[10] Nei considerando del regolamento MiCA vengono delineati dei criteri utili allo scopo di discriminare tra i due fenomeni: le frazioni di un *crypto-asset* unico e non fungibile non devono essere considerate uniche e non fungibili e l'emissione di *crypto-asset* in forma di token non fungibili seriali deve essere considerata un indicatore della loro fungibilità, mentre l'attribuzione di un identificatore univoco a un *crypto-asset* non è sufficiente per classificarlo come univoco o non fungibile. Ulteriore requisito perché il *crypto-asset* possa essere considerato unico e non fungibile è che anche le attività o i diritti da esso rappresentati dovrebbero essere unici e non fungibili.

Alla luce del quadro sopra delineato, emerge chiaramente come sarà necessario un esercizio *finium regundorum* per tracciare una linea di demarcazione, in prima battuta, tra *token* di investimento che si qualificano come strumento finanziario ai sensi della direttiva MiFID (e che pertanto ricadono nella sfera di applicazione della disciplina dell'intermediazione finanziaria classica) e *token* di investimento che non vi ricadono (e che pertanto sono attratti nell'alveo applicativo del regolamento MiCA); quindi, tra *token* fungibili e non fungibili, avendo presente che anche rispetto a tale ultimo profilo, il regolamento MiCA contempla un intervento dell'ESMA in funzione di emanazione di linea guida proprio a questo scopo.

Al dì là della classificazione teorica e normativa dei *crypto-asset*, è opportuno rilevare come la possibilità di "tokenizzare" si sia storicamente tradotta nella possibilità di sfruttare l'offerta di *token* come forma di finanziamento di nuove iniziative imprenditoriali. Alle operazioni di emissione e offerta di "cripto-valute" in senso stretto è stato inizialmente associato il termine "*initial coin offering*" ("ICO"), poi venuto ad identificare qualsiasi offerta di *token*, non necessariamente costituenti una *crypto*-valuta, che possono essere acquistati dietro corrispettivo sia di valuta *fiat* che di "*crypto*-valuta", con l'obiettivo di raccogliere fondi per il finanziamento di un progetto.

Molto frequentemente lo stadio di ideazione dell'iniziativa è di mera progettualità e l'inizio della produzione di beni/prestazione di servizi è programmata dopo la conclusione della raccolta di fondi[11]. Il ricorso ad un'operazione di raccolta tramite un'"*Initial Coin Offering*" (ICO) è sollecitato, rispetto alle alternative più tradizionali, dalla principale suggestione di "disintermediare" le infrastrutture che contraddistinguono oggi il mercato dei capitali. Costituisce un elemento di ulteriore suggestione anche la modalità di regolamento dei flussi finanziari, che è alternativa risetto a quella tradizionale in quanto il pagamento dei *token* generalmente avviene con *crypto*-valute e non con moneta *fiat*.

Figura, tra i tratti caratterizzanti delle ICO, anche la circostanza che l'operazione di raccolta sia promossa e tipicamente effettuata tramite *web*, senza confini di natura territoriale, e sia pubblicato un documento nel quale vengono riportate le principali caratteristiche dell'operazione e dell'oggetto dell'offerta, noto come *white paper*, in luogo del prospetto.

Nel corso degli ultimi anni imprenditori e investitori hanno preso in crescente considerazione le ICO come alternativa alle tradizionali operazioni di raccolta di capitali e occasioni di partecipazione a opportunità di investimento.

---

[11] Si esprime in questi termini il documento "*Le offerte iniziali e gli scambi di cripto-attività. Documento per la Discussione*", pubblicato dalla Consob il 19 marzo 2019 (*cfr. infra*).

Non disconoscendo il potenziale di queste realtà a rappresentare un mezzo nuovo ed efficiente per l'esecuzione di transazioni finanziarie, le autorità di vigilanza hanno tuttavia messo in guardia tutti gli attori del mercato dai rischi insiti nel ricorso alle ICO in virtù dell'assenza di un quadro regolamentare ad esse applicabile. Contemporaneamente, sono partite iniziative regolatorie in singole giurisdizioni, mosse dalla volontà di assicurare che i presidi che puntellano l'operatività dei mercati finanziari tradizionali potessero trovare adeguata applicazione anche in ambiente DLT, con l'obiettivo primario di proteggere investitori e salvaguardare la stabilità finanziaria, iniziative caratterizzate da un certo livello di eterogeneità[12].

Peraltro, nonostante la promessa di disintermediazione ontologicamente sottesa al ricorso alla DLT, si è assistito e si continua ad assistere al proliferare di nuovi servizi collegati ai *crypto-asset* – una vera e propria industria digitale – sviluppati da soggetti che, sostanzialmente, propongono forme di intermediazione sinora inedite.

Rilevano a questo proposito in particolare i servizi volti alla custodia delle chiavi crittografiche (servizi di *custodial wallet*)[13].

La Consob si è interrogata sul problema della disciplina dei *crypto-asset* nel 2019 proponendo un "documento per la discussione", con l'obiettivo di avviare un dibattito a livello nazionale sul tema delle offerte iniziali e degli scambi di cripto-attività, in relazione alla diffusione di operazioni di ICO e della possibilità di investimento in *crypto-asset* da parte dei risparmiatori italiani.

Nel gennaio del 2020 ha quindi pubblicato il suo "rapporto finale", con l'obiettivo di porre le basi di un quadro regolamentare organico e coerente che consentisse l'investimento in *crypto-asset* con piena consapevolezza di rischi e opportunità.

La risposta a livello dell'Unione europea, tuttavia, come si è detto, non si è fatta attendere e ha dunque occupato la scena regolatoria: il futuro regolamento MiCAR detta una disciplina armonizzata che andrà a sostituirsi alle soluzioni nazionali sviluppate sinora.

---

[12] A Malta è stato adottato il "*Virtual Financial Assets Act*" nel 2018. Con la legge 2019-486 del 22 maggio 2019 ("*loi PACTE*") è stato introdotto in Francia un regime facoltativo per le ICO e per la prestazione di servizi aventi ad oggetto *crypto-asset*. In Liechtenstein è in vigore dal 1° gennaio 2020 la legge sui *token* e i prestatori di "servizi TT".

[13] I *wallet* digitali sono applicativi informatici che consentono di conservare le "chiavi private e pubbliche" che identificano ciascun utente nella *blockchain*. Le transazioni sulla *blockchain* sono infatti crittografate; la *blockchain* si basa sul ricorso alla crittografia asimmetrica: viene utilizzata una coppia di chiavi, cosiddette chiave pubblica e chiave privata, legate da una funzione che garantisce che un messaggio criptato con una delle due chiavi possa essere decifrato solo utilizzando l'altra. La chiave pubblica corrisponde all'"indirizzo" del suo titolare.

4. L'emissione di *security token* e le STO

Le STO (*Security Token Offering*) figurano nell'insieme più ampio delle ICO, ma rispetto a esse si è assistito a una crescita negli ultimissimi anni in misura superiore rispetto alle altre forme di ICO. Esse si differenziano principalmente in virtù della diversa natura dell'oggetto dell'offerta: *token* di investimento, che hanno le caratteristiche tipiche di strumenti che ricadrebbero in principio nell'alveo di applicazione della legislazione finanziaria o – nell'ordinamento finanziario italiano – nell'alveo applicativo della disciplina dei prodotti finanziari.

Con *security token* si intende generalmente *securities* emesse in forma digitale tramite *blockchain*, ma la definizione di *security* dipende dall'ordinamento nell'ambito del quale ci si pone l'interrogativo e le risposte non sempre coincidono[14].

Il concetto di *security token* è a sua volta diverso da quello di *tokenised security* sebbene quando si parli di STO i due fenomeni vengano essenzialmente assimilati. Nell'assenza di tassonomia e nomenclatura condivise, il concetto di *security token* può essere inteso come corrispondente a quello di *token* nativo, mentre con *tokenised security* si intende uno strumento non nativo, ossia uno strumento finanziario, emesso ai sensi della disciplina "tradizionale", ma incartato in un "involucro digitale" per sfruttare talune delle caratteristiche della tecnologia: in questo caso lo strumento finanziario pre-esiste (e continua a esistere) nella sua realtà "naturale".

Un "titolo tokenizzato" è infatti il gemello digitale di uno strumento finanziario che esiste al di fuori della *blockchain* e che può essere descritto come "avvolto" nella *blockchain*. Sebbene rappresentare in forma digitale uno strumento finanziario che preesiste potrebbe essere utile, secondo alcuni, per sfruttare il potenziale di efficienza derivante dall'utilizzo della *blockchain* per registrare la titolarità e i trasferimenti, è sempre necessario tenere conto dell'esistenza del titolo sottostante e della disciplina a esso applicabile[15].

---

[14] Negli Stati Uniti, perché possa essere riscontrata una "*security*" devono sussistere congiuntamente a) un investimento in denaro; b) un progetto imprenditoriale; c) un'aspettativa di profitto prevalentemente derivante dagli sforzi del promotore dell'iniziativa o di un terzo, si tratta del c.d. Howey test. Il riscontro positivo di tali requisiti produce come risultato l'assoggettamento del *token* alla normativa applicabile alle *securities*. Un esempio significativo e famoso di applicazione del test è il caso DAO: il 25 luglio 2017, la SEC ha pubblicato il suo *Report of Investigation* sull'offerta di *token* del 2016 da parte di un gruppo noto come "*DAO*". La SEC ha stabilito che i *token* offerti dalla DAO (i "*DAO Tokens*") fossero contratti di investimento ai sensi dell'Howey test e quindi *titoli* ai sensi dello *United States Securities Act* del 1933 e del *Securities Exchange Act* del 1934.
Nell'Unione europea la nozione di "*securities*" (valori mobiliari) è dettata dalla direttiva MiFID II e si basa sui concetti di standardizzazione, trasferibilità e "negoziabilità sul mercato dei capitali".

[15] ASIFMA (Asia Securities Industry and Financial Markets Association), "*Tokenised Securities. A Roadmap for Market Participants and Regulators*", novembre 2019.

Un titolo tokenizzato è stato quindi assimilato ad una "*depositary receipt*" (ricevuta di deposito)[16].

La qualificazione da un punto di vista regolatorio di un titolo tokenizzato può essere complessa perché lo strumento digitale "tratto" dallo strumento sottostante, se non si ricade effettivamente nello schema della ricevuta di deposito, può essere ricaratterizzato sotto forma di un altro strumento finanziario, ivi compreso uno strumento derivato.

Nella proposta di classificazione che si ritiene di condividere, i *security token* non sono – al contrario delle *tokenised security* – una mera rappresentazione digitale del sottostante, ma la diretta espressione digitale del loro contenuto: costituiscono cioè essi stessi attività tipicamente finanziarie e non la loro fotocopia digitale: azioni, obbligazioni, quote di organismi di investimento collettivo che nascono e vivono il loro ciclo di vita esclusivamente su registro distribuito. Nonostante queste differenze, i due termini sono spesso usati, e a torto, in modo intercambiabile. In taluni casi l'espressione *security token* è invalsa a identificare il fenomeno inverso: è il caso della Germania, che oppone al concetto di "obbligazioni digitali" (che sono native in DLT) quello di "*security token*"[17], segno del difetto di un'armonizzazione anche solo nell'utilizzo della nomenclatura, che ancora contraddistingue l'approccio al fenomeno.

Avendo presenti le differenze tra titoli *tokenizzati* e *security token* appena illustrate, ci si può chiedere se sia attualmente consentito il ricorso alle tecnologie di tipo DLT per l'emissione di strumenti finanziari tipici, quali azioni o obbligazioni, in forma di *security token*.

Se i titoli in questione sono destinati a essere negoziati su un "*mercato*", nell'accezione lata del termine, la risposta a questo interrogativo si rintraccia nel regolamento sui depositari centrali, i CSD (c.d. regolamento CSDR[18]). CSDR – che è probabilmente la manifestazione più eclatante, in materia, delle interferenze tra regolazione finanziaria e diritto privato – prevede infatti che se uno strumento

---

[16] Le ricevute di deposito sono certificati rappresentativi di azioni in una società estera negoziati su un mercato locale e consentono agli investitori di detenere azioni di società estere senza la necessità di negoziare direttamente sul mercato estero. L'investitore si interfaccia esclusivamente con un istituto finanziario nel suo paese d'origine – l'emittente delle *depositary reeceipt* – che custodisce, direttamente o indirettamente, una certa quantità di azioni.

[17] Si distingue tra *security token* e *crypto-security*. Sono *crypto-security* esclusivamente i titoli nativi digitali, oggetto di una registrazione in un registro per la circolazione digitale ai sensi della eWpG.

[18] La disciplina richiamata è dettata dal regolamento UE n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli, c.d. CSDR (Central Securities Depository Regulation).

finanziario quale un'azione o un'obbligazione è destinato allo scambio in una sede di negoziazione, il suo regime di forma e circolazione non sia libero, ma condizionato alla necessità di consentire, da parte del CSD, l'attività di "regolamento" (*settlement*): quella cioè di assicurare il trasferimento dei titoli e del corrispettivo in contante oggetto di una transazione, così consentendo il completamento dell'operazione.

A questo fine il citato regolamento prescrive la "rappresentazione in forma scritturale" dello strumento presso un depositario centrale: secondo quanto disposto dall'articolo 3 di CSDR, tra gli altri azioni e obbligazioni – per citare gli strumenti maggiormente rappresentativi della categoria dei valori mobiliari – devono necessariamente ed esclusivamente esistere nelle scritture contabili di un CSD e, a valle, nelle scritture contabili degli intermediari, fino all'ultimo intermediario presso il quale l'investitore ha il proprio *dossier* titoli. Se l'ordinamento interno prevede l'emissione in forma cartolare, i certificati destinati alla negoziazione su una sede di negoziazione devono essere immobilizzati nel *caveau* del depositario centrale e cessano di circolare in quanto tali perché sono trasformati in registrazioni contabili. In quello che in Italia si qualifica come "sistema di gestione accentrata" gli strumenti finanziari si trasferiscono esclusivamente per il tramite degli intermediari in virtù di registrazioni su conti.

Il sistema di *settlement* operato dal depositario centrale deve possedere determinate caratteristiche e in particolare essere "designato" ai sensi della direttiva *settlement finality* (che garantisce l'applicazione di talune tutele, in particolare consentendo che gli ordini di trasferimento possano beneficiare della c.d. definitività)[19].

Ai sensi della stessa direttiva *settlement finality* lo svolgimento dell'attività di *settlement* richiede che i "partecipanti" a un sistema di *settlement* siano banche e imprese di investimento (e solo in via eccezionale, sulla base di considerazioni *ad hoc* in punto di rischio sistemico, altri soggetti).

Anche l'accesso alla sede di negoziazione è oggi consentito, in virtù della disciplina dettata dalla direttiva MiFID, solo a imprese di investimento, enti creditizi e altri soggetti che abbiano un livello sufficiente di capacità di negoziazione, competenza e modalità e risorse organizzative adeguate[20].

Le piattaforme di negoziazione di *token* aspirano invece a offrire un accesso *disintermediato* e diretto agli investitori sia sul fronte della negoziazione che sul fronte del

[19] Direttiva 98/26/CE Del Parlamento europeo e del Consiglio del 19 maggio 1998 concernente il carattere definitivo del regolamento nei sistemi di pagamento e nei sistemi di regolamento titoli.

[20] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE.

settlement, in ciò – come si è detto – confortate dalle caratteristiche della tecnologia: per poter mettere alla prova tutto il potenziale di quest'ultima è pertanto necessario consentire una (almeno temporanea) disapplicazione della disciplina sopra richiamata. Tale disapplicazione sarà possibile in presenza di determinate condizioni "compensative" che permettano di colmare l'eventuale *gap* di tutela. Il ricorso alla DLT porta però con sé forme di rischio inedite: diventa così necessario, in parallelo, prescrivere requisiti aggiuntivi rispetto a quelli tradizionali per chi voglia farne esperienza.

In questa direzione si muove il regolamento *Pilot regime*, che attraverso l'introduzione di nuove infrastrutture dedicate (le "infrastrutture di mercato DLT") e la possibilità di concedere alle medesime infrastrutture esenzioni specifiche dalle previsioni percepite come ostacolo alla DLT, intende favorire lo sviluppo di un mercato secondario di strumenti emessi e trasferiti su registro distribuito, in un contesto di potenziale integrazione tra l'ambiente di *trading* e quello di post-*trading*, e – contemporaneamente – facilitare l'individuazione nel concreto, da parte di tutti i *player*, di tutti i freni normativi che si frappongono all'utilizzo della DLT e che potranno essere successivamente rimossi in uno stadio di intervento differito e definitivo.

In tale quadro, le autorità nazionali saranno responsabili della concessione di deroghe dall'applicazione delle previsioni che possono far da freno al pieno sfruttamento del potenziale della DLT, su iniziativa delle infrastrutture, e l'ESMA avrà un ruolo consultivo e di catalizzazione della convergenza delle prassi di vigilanza.

Il regime *Pilot* sarà applicabile, tuttavia, solo ad alcune tipologie di strumenti, caratterizzati da minore liquidità[21] e fino a soglie massime quantitative.

Ulteriore previsione chiave del regime *Pilot* è quella che interviene sulla definizione di strumento finanziario prevista dalla direttiva MiFID al fine di chiarire che sono strumenti finanziari ai sensi dell'Allegato I alla direttiva anche quelli emessi facendo ricorso alla DLT.

Il regolamento *Pilot regime* riconosce dunque la natura di strumento finanziario di uno strumento emesso su registro distribuito e potenzialmente disinnesca l'applicazione dell'obbligo di rappresentazione in forma di scrittura contabile presso il sistema di gestione accentrata. Agisce, dunque, in negativo, rimuovendo un impedimento. Ma se giriamo la medaglia, come si presenta la faccia "diritto privato", una volta che l'intralcio di regolatorio è stato rimosso?

Sul piano privatistico serve un movimento *positivo* dell'ordinamento. Il diritto nazionale deve essere pronto a supportare l'emissione e la circolazione in forma

[21] Si tratta di azioni; obbligazioni e altri titoli di debito non complessi, nonché ricevute di deposito relative a tali titoli; strumenti del mercato monetario; azioni o quote di organismi di investimento collettivo in valori mobiliari non strutturati.

digitale anche in sede di "primario", a consentire cioè che lo strumento finanziario possa essere generato su un registro distribuito e che possa vivere, nella dimensione del registro distribuito, tutto il suo ciclo di vita[22]. Se necessario, dunque, deve essere modificato per consentire al *Pilot regime* di "attecchire".

Tenendo a mente la destinazione degli strumenti finanziari di cui si discorre – ossia essere negoziati su una sede di negoziazione – la legge di circolazione di tali strumenti dovrebbe, idealmente, poter essere assimilabile, *quoad effectum*, alla legge di circolazione che tipicamente disciplina gli effetti dei trasferimenti sul mercato dei capitali.

Calandosi nella prospettiva nazionale, nel corso dell'ultimo quadriennio la dottrina si è chiesta quale legittima *chance* di emissione in DLT a ordinamento invariato potessero avere questi strumenti (e dunque quali margini di possibilità di fare ricorso alla DLT per consentire l'emissione di attività finanziarie tradizionali e tipiche quali azioni e obbligazioni potessero concretamente darsi in difetto di un intervento *ad hoc* del legislatore), circoscrivendo naturalmente l'analisi a quegli strumenti che non ricadono nell'alveo di applicazione degli obblighi di rappresentazione in forma scritturale[23].

Sono state, in particolare, prese in considerazione alcune potenziali "brecce" nel Codice civile, per verificare la loro concreta propensione a far penetrare il fenomeno. La prima norma considerata è stata quella dell'articolo 2346, comma 1, c.c. nella parte in cui consente, per scelta statutaria, il ricorso a "diverse tecniche di legittimazione e circolazione" per l'emissione di azioni.

È stato sostenuto che la circolazione cartolare potrebbe essere sussunta in quella digitale in *blockchain,* nella misura in cui ne fossero riprodotte le caratteristiche salienti, proprio facendo leva sull'autonomia statutaria attraverso la promozione della DLT quale tecnica di legittimazione e circolazione alternativa[24].

---

[22] In questo senso depone la definizione di strumento finanziario DLT dettata dal Regolamento *Pilot*: strumento finanziario "*emesso, registrato, trasferito e stoccato mediante la tecnologia a registro distribuito*".

[23] È bene sottolineare che, oltre all'obbligo di rappresentazione in forma scritturale di matrice unionale, rilevano anche, a livello nazionale, gli obblighi di rappresentazione scritturale previsti dal Regolamento unico sul post-*trading* della Consob e della Banca d'Italia (cfr. in particolare l'articolo 34), in attuazione della delega conferita dall'articolo 83-*bis*, comma 2, del Testo Unico della Finanza.

[24] Il ricorso ad una DLT *permissioned*, che consenta di evidenziare la sequenza delle vicende circolatorie o costitutive di vincoli e che sia opportunamente configurata per associare univocamente ciascun *token* all'identità di un titolare sarebbe idoneo a soddisfare le condizioni necessarie affinché possano dirsi puntualmente trapiantati in questo nuovo ambiente la nominatività obbligatoria dei titoli azionari ed i meccanismi fondanti l'imputazione e l'esercizio dei diritti sociali, in uno scenario in cui i poteri di controllo e modifica fossero affidati all'organo amministrativo. Così A. Laudonio, *Blockchain and Icos (a Sisyphean Juridical Tale on Financial Markets and Innovation)*, in

È stato inoltre evidenziato come l'assenza, con riferimento agli strumenti obbligazionari, di previsioni equivalenti a quella che in ambito azionario legittimano l'adozione di tecniche di legittimazione e circolazione diverse con riferimento alle obbligazioni, non osterebbe a consentire la scelta di tecniche di legittimazione e circolazione alternative, nella direzione della informatizzazione dei libri sociali e nella riproposizione in chiave DLT degli elementi chiave della circolazione nominativa[25].

Viene, inoltre, in considerazione, secondo altra dottrina, l'articolo 2355, comma 1, che consente e disciplina l'ipotesi di una mancata emissione dei titoli azionari. In questo caso, in cui un "titolo" azionario non è emesso (né in forma cartolare né in forma scritturale), la circolazione dell'azione resta consensuale e gli acquisti sono opponibili all'emittente solo al momento dell'iscrizione nel libro soci. Secondo le prospettazioni di alcuni autori, tale norma potrebbe essere sfruttata considerando l'emissione di "azioni tokenizzate" come l'equivalente di una mancata emissione delle azioni, costruendo in parallelo una tenuta del libro soci con tecnologie basate su registri distribuiti (*ex* art. 2215-bis c.c.)[26].

La soluzione illustrata – ossia una tenuta del libro soci in DLT – sarebbe per altri l'unica possibilità legittima, per una società per azioni, di "rappresentare" le proprie azioni sotto forma di *token*. In questa ipotesi – viene opportunamente sottolineato – i *token* non sarebbero realmente giuridicamente rappresentativi delle azioni della società: dal punto di vista legale, senza uno specifico intervento del legislatore, questo sistema consentirebbe esclusivamente ai *token* di essere uno strumento (nell'accezione di "utensile") il cui trasferimento attiva il meccanismo di aggiornamento del libro soci[27]. Azioni tokenizzate, dunque, e non *security token*.

A. Caligiuri, *Legal Technology Transformation. A Practical Assessment*, *open access*, 2020, pp. 214 e s. Sul tema si veda altresì N. De Luca, *Documentazione crittografica e circolazione della ricchezza*, in M. Cian, C. Sandei, a cura di, *Diritto del Fintech*, Padova 2020, pp. 429 e ss.

[25] Sul punto cfr. A. Laudonio, *op. cit.,* p. 214, nota 9.

[26] Ai sensi dell'art. 2215-bis c.c., i libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni dell'impresa possono essere formati e tenuti con strumenti informatici. La costruzione dovrebbe far sì che "*la circolazione delle azioni tokenizzate, per il tramite della blockchain, possa determinare l'automatico aggiornamento dei libro soci, con effetti anche sull'emittente*". In questo senso N. De Luca, *cit*., p. 432. Contro questa possibile equivalenza azione non emessa-azione tokenizzata si esprime invece A. Laudonio, *cit*.

[27] Così R. Lener, S. L. Furnari, *Company law during the blockchain revolution. The rise of "CorpTech"*, in *Open Review of Management, Banking and Finance*, 2020. 9 e ss.: "*The solution illustrated* [tenuta del libro soci di una S.p.A. in DLT] *seems the only legal possibility for a SPA to distribute to the public crypto-assets representing its shares in the form of equity token. However, what is true is that the equity tokens will not really represent the shares of the company. Legally speaking, without a specific intervention of the legislator, this system will only let equity tokens to be a tool whose alienation would activate the mechanism for the updating of the Shareholder Book".*

Un ulteriore spunto di analisi rispetto ai temi sopra illustrati viene dalla considerazione del dubbio se, in un contesto di titoli non emessi, sia possibile ragionare dell'applicazione della regola dell'acquisto di buona fede – tema che si rivela molto controverso in dottrina[28]. Analogamente controverso in dottrina, a livello unionale, è il tema della rilevanza dell'acquisto di buona fede ai fini del riscontro della sussistenza del requisito della "negoziabilità sul mercato dei capitali", che consente la qualificazione di un "titolo" come valore mobiliare per tutte le finalità dell'ordinamento finanziario[29] (esempio lampante, quest'ultimo,

[28] Rispetto a questo tema, alcuni autori hanno assunto l'applicabilità della regola sugli acquisti a non domino: sarebbe protetto chi in buona fede consegua l'annotazione nel libro soci (cfr. in particolare I. Kutufà, *Azioni non emesse*, Torino, 2013, cfr. in particolare pp. 51 ss.). Secondo quanto prospettato "l'acquirente potrà ritenersi in buona fede se ha acquistato fondando il proprio consenso sulla base della (peraltro unica) documentazione che avrebbe potuto fargli supporre la capacità di disporre dell'alienante: il libro dei soci". Nell'assunto che le risultanze del libro dei soci divengano nella fase (pre)contrattuale accessibili al terzo, sarebbe quindi "possibile comprendere il motivo che rende la sua posizione, al pari di quella assunta dal possessore del titolo, meritevole di tutela reale". Altra dottrina, in risposta, ha rilevato come non basti "l'adozione di una tecnica paracartolare (il fatto documentale, cioè), per dare ingresso ad una disciplina circolatoria diversa da quella di diritto comune". "*Collegando in una relazione di causa a effetto l'asserita equipollenza libro soci – incorporazione e l'attivazione delle regole di tutela degli acquisti*", si corre il rischio di "*attorcigliarsi in una petizione di principio: dovrebbe piuttosto essere la volontà dell'emittente o l'apprezzamento della comunità dei consociati (secondo le diverse teorie sulla fattispecie titolo di credito) a richiamare, grazie all'attitudine della veste documentale (condicio sine qua non, ma non presupposto causale esclusivo), quelle regole. Altrimenti, anche la circolazione della quota di s.r.l. e di ogni altro tipo societario – posta l'indiscutibile equivalenza tra libro soci e registro delle imprese sotto i profili in esame – finirebbe per essere resa una circolazione "cartolare"*" (così M. Cian, Art. 2355. Circolazione delle azioni, in www.notai.bz.it.

[29] Si esprime nel senso dell'irrilevanza della possibilità di un acquisto di buona fede ai fini della qualificazione come valore mobiliare R. Veil, *European Capital Markets Law*, Oxford, 2022 "*the European concept of securities does not require tradability on a regulated market, MTF or OTF… It is sufficient that the instrument can generally be negotiated on a market. Whether acquisition in good faith is possible is irrelevant under MiFID II*". Per contro P. Hacker-C. Thomale, *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, in *European Company and Financial Law Review*, Volume 15 Issue 4, 2018 p. 664, sottolineano come per alcuni autori sia dirimente che l'ordinamento contempli la possibilità di un acquisto di buona fede o che siano previsti meccanismi equivalenti per garantire la tutela *erga omnes* degli investitori ("*While transferability refers to the mere fact of passing on ownership in securities, their negotiability concerns the ease with which ownership can be transferred. It is easy to see that negotiability in fact implies transferability. What is crucial is that they can be traded easily on a capital market. The concept of a capital market, in turn, is not defined in EU securities regulation, but "is broad and is meant to include all contexts where buying and selling interest in securities meet". […] However, scholars are divided on the question whether further criteria have to be met for negotiability to be fulfilled. Some do interpret negotiability in a narrow sense, so as to distinguish it clearly from mere transferability.*

di come la faccia "diritto privato" della moneta possa impattare sull'effigie "regolazione finanziaria").

La breve panoramica che precede testimonia come esigenze di certezza del diritto depongano nel senso – già perseguito in altri ordinamenti – di non procedere *de iure condito* attraverso esercizi interpretativi, quanto piuttosto di introdurre una disciplina positiva dell'emissione e circolazione in forma digitale[30].

Se si considera l'infrastruttura DLT come "tecnologia immediatamente evocativa della logica giuridica alla base della disciplina dei titoli di credito e delle sue evoluzioni, quali la dematerializzazione nel sistema di gestione accentrata degli strumenti finanziari", si può agevolmente cogliere l'invito a non commettere "l'errore di considerare i token e le distributed ledger technology *(DLT) come fenomeni eversivi degli istituti giuridici consolidati"*[31], quanto piuttosto di partire, in Italia, dalla consapevolezza che "il profilo di novità che lo sviluppo di tali tecnologie offre consiste semmai in una inedita forma di rappresentazione e circolazione di posizioni giuridiche soggettive note. In particolare […] il *token altro non è che un veicolo digitale che consente l'incorporazione di determinati diritti, permettendone la circolazione semplificata e garantita tramite l'infrastruttura blockchain*"[32].

Attorno al "veicolo digitale" e dunque alla registrazione su un registro distribuito può essere costruita una disciplina alternativa a quelle cartolari e scritturali: un regime giuridico che dovrebbe essere "(perlomeno) equivalente a quello tipico, in termini di affidabilità, sicurezza e stabilità degli atti giuridici e delle opera-

---

Particularly, they tend to stress that acquisition of securities based on good faith must be possible, or that equivalent security mechanisms need to be in place to protect investors erga omnes, and not only vis-à-vis their contractual party, from insecure links in the chain of ownership". Si veda anche sul punto l'*Advice* dell'ESMA su *Initial Coin Offerings and Crypto-Asset* del 9 gennaio 2019.

[30] In difetto di un intervento espresso del legislatore, dunque, sono "*ancora prematuri i tempi* […] *per la «tokenizzazione»* delle società". Così G. Gitti, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca borsa*, fasc.1, 2020, pp. 13 e ss.. Per una disamina delle iniziative intraprese in Francia e in Germania sia consentito rinviare a M.T. Rodi, *Il finanziamento delle PMI attraverso l'emissione di token digitali: il caso delle STO*, in C. Schena., R. Locatelli, "*Il nuovo ecosistema finanziario per le PMI: le opportunità della digitalizzazione e dello sviluppo sostenibile*", Milano, 2022, pp. 259 ss. Rispetto a quanto descritto in quella sede, si segnala tuttavia che il quadro normativo si sta ulteriormente evolvendo. Per quanto riguarda l'ordinamento francese, è di particolare interesse il *Rapport sur la Réforme des Titres Financiers Numériques du Haut Comité Juridique de la Place Financière de Paris* del 20 maggio 2022 che si preoccupa dell'adeguamento dell'ordinamento interno al Pilot *regime*.

[31] Cfr. G. Gitti, *op. cit.*

[32] Cfr. G. Gitti, *op. cit.* il quale sottolineava come sembrassero "*ancora prematuri i tempi, in difetto di un intervento del legislatore, per la «tokenizzazione»* delle società".

zioni che essa sarebbe dunque chiamata a sancire e documentare" e ad assolvere le "funzioni tipiche" della tecnica cartolare[33].

Oggi come ieri serve dunque individuare, in un sistema nuovo, tecniche di protezione equivalenti a quelle contenute nel Codice civile.

Il nostro ordinamento già conosce, come si è detto, la circolazione tramite scritturazioni contabili. Nel momento in cui si prefigurava, nel 1997, una dematerializzazione totale dei titoli che consentisse "di sostituire all'emissione e alla circolazione del supporto cartaceo una emissione e una circolazione tramite mere scritturazioni contabili", il legislatore delegato del decreto Euro era stato incaricato di procedere "individuando forme di tutela per l'emittente ed il possessore … equivalenti a quelle che assicura loro la disciplina cartolare in tema di titoli di credito", così come a "soddisfare l'esigenza di garantire la correttezza di tutte le operazioni legate alla negoziazione dei titoli stessi".

La Consob si è fatta negli ultimi anni promotrice dell'urgenza di introdurre un nuovo quadro normativo che preveda un regime dedicato per l'emissione e circolazione dei titoli in forma digitale.

Nel suo Libro Verde su "*La competitività dei mercati finanziari italiani a supporto della crescita*" dello scorso marzo, il Tesoro ha segnalato l'esigenza di dotare l'Italia di una cornice legislativa che consenta l'emissione e la circolazione in forma digitale di strumenti finanziari tramite DLT, anche in vista della futura applicazione del regolamento Pilot *regime*, segnalando essere all'esame possibili opzioni di intervento normativo per sperimentare un nuovo regime di emissione e circolazione in forma digitale di strumenti finanziari, prodromico alla definizione, a tendere, della cornice normativa volta a consentire a regime l'emissione e la circolazione in forma digitale di tutti gli strumenti finanziari.

Parafrasando la dottrina che nel 1998, in relazione all'avvento del c.d. "Decreto Euro", si esprimeva in termini di "congedo dal titolo di credito"[34], potrebbe concludersi che l'eventuale commiato dal suo successore – il "titolo scritturale", per come lo abbiamo conosciuto negli ultimi venti anni – potrà essere un commiato senza rimpianti solo a condizione che non siano pretermessi gli obiettivi di

---

[33] Ossia quelle di rendere trasferibile efficacemente e in maniera giuridicamente sicura, gli strumenti in considerazione e comunque di assoggettarli ad atti dispositivi; sopperire "altrettanto (se non più) efficacemente" alla funzione di documentazione della titolarità dello strumento, conferire la legittimazione all'esercizio dei relativi diritti sociali; consentire l'efficace e opponibile creazione e documentazione di vincoli e diritti di garanzia su di essa. In questi termini si esprime P. Carrière, *cit*. *Il fenomeno delle cripto-attività (*crypto-asset*) in una prospettiva societaria*, in *Banca impresa*, pp. 461 e ss. Cfr. in particolare p. 489.

[34] G. Carriero, *La legge sulla dematerializzazione degli strumenti finanziari: tecniche giuridiche ed obiettivi*, in Foro it., 1998, IV, pp. 309 ss.

tutela sopra richiamati e che la nuova disciplina sia – in una logica di "equivalenza funzionale"[35] – "idonea a garantire l'efficienza del mercato, che ne costituisce il più importante momento teleologico"[36]. Solo così il connubio tra regolazione finanziaria e diritto privato potrà rivelarsi vincente e le due facce della moneta essere compiutamente ricondotte ad unità.

Ma come si presenta la faccia "diritto privato" della moneta per i *crypto-asset* diversi dai *security token*? L'analisi richiede una trattazione separata. Merita però, in questa sede, almeno menzionare il progetto *Digital Assets And Private Law* dell'Unidroit, che attraverso l'adozione di un approccio neutrale, che si adatti alle diverse tipologie di *asset*, di tecnologie e di tradizioni giuridiche, mira a fornire orientamenti e sviluppare principi che incarnino le migliori prassi e gli *standard* tecnici internazionali e che possano informare gli interventi legislativi a livello globale per quanto concerne la natura giuridica, il trasferimento e l'utilizzo dei *crypto-asset*[37].

L'esigenza di rendere uniforme l'approccio del diritto privato alla regolazione finanziaria ci riporta dunque, in conclusione, a un interrogativo di carattere generale posto dalla stessa Commissione europea all'inizio del processo che ha portato al *Digital Financial Package*. Nel documento di consultazione del 2019 essa chiedeva al mercato: "*Should harmonisation of national civil laws be considered to provide clarity on the legal validity of token transfers* […]?"[38]. Un quesito ancora cruciale, che troverà probabilmente una risposta solo a valle dell'esperienza applicativa del nuovo quadro regolatorio dei prossimi anni.

---

[35] Il principio di equivalenza funzionale è anche uno dei principi fondanti l'azione dell'UNCITRAL in materia di commercio elettronico, come stabilito nel 1996 con il *Model Law on Electronic Commerce*. Tale principio "consente di definire gli istituti del mondo digitale basandosi sulla funzione che i requisiti formali dei corrispettivi "*analogici*" svolgono negli ordinamenti nazionali, per utilizzarli come parametri fissi nel valutare l'equivalenza tra scritto e informatico" ed è, altresì, alla base del modello di legge sugli *Electronic Transferable Records* (i.e., i titoli di credito dematerializzati) adottato nel 2017. Così G. Finocchiaro, O. Pollicino, "*Electronic Transferable Records: la RoadMap del G7 passa per il Model Law dell'Uncitral*", in https://ntplusdiritto.ilsole24ore.com/, 3 febbraio 2022.

[36] *Op. cit.*

[37] In questo senso il mandato del gruppo di lavoro https://www.unidroit.org/work-in-progress/digital-assets-and-private-law.

[38] Commissione europea, documento "*Public consultation on an EU framework for markets in crypto-assets*" del dicembre 2019.

Niccolò Abriani

Imprese e intelligenza artificiale

Sommario: 1. L'impatto dell'intelligenza artificiale sulle realtà aziendali. – 2 Intelligenza artificiale e macrodati. – 3. Intelligenza artificiale e cibernetica societaria. – 4. L'intelligenza artificiale tra sostenibilità e "infuturarsi" delle imprese. – 5. Dalla *Fintech* alla *Corptech*. – 6. L'intelligenza artificiale come strumento di governo. – 7. L'intelligenza artificiale come oggetto di governo. – 8. *Segue*. Dalla *Corptech* alla *Corporate Digital Responsibility*. – 9. *Corptech* e codici di autodisciplina. – 10. Nuovi profili di responsabilità degli amministratori. – 11. Una postilla: decisioni automatizzate e giustizia predittiva.

1. L'impatto dell'intelligenza artificiale sulle realtà aziendali

Il tema dell'impatto dell'intelligenza artificiale sulle imprese si iscrive all'interno di un quadro generale caratterizzato, da un lato, dai delicati e in larga misura inediti problemi che il sempre più pervasivo e invasivo ricorso ai nuovi strumenti tecnologici pone al Diritto (con la D maiuscola) e, dall'altro, dal crescente impatto dell'intelligenza artificiale sulla Società (con la S maiuscola): dunque, sulla *Gemeinschaft,* non soltanto sulla *Gesellschaft*; o, se vogliamo, sulla *Wider Society*, non solo sulla *Company* o sulla *Corporation*. Questi temi sono stati magistralmente introdotti nella relazione iniziale di questo corso da Mario Libertini, che ha offerto una ineguagliabile sintesi dei diversi impatti che le tecnologie digitali, nel loro insieme, hanno avuto non solo sulla cultura e sulla società, ma anche nell'esperienza giuridica[1].

Nel rinviare a quelle considerazioni, che costituiscono un ideale "piedistallo" di tutti gli interventi successivi, va qui soggiunto che l'intelligenza artificiale, ove correttamente governata, si presenta come nuovo motore della sostenibilità della società, e dunque di una gestione della società-*Gesellschaft* improntata a una visione di lungo periodo nella composizione delle istanze delle diverse parti coinvolte nell'iniziativa imprenditoriale. In questa prospettiva, l'intelligenza artificiale

[1] Per una visione d'insieme v. ora i contributi contenuti in G. Finocchiaro, L. Balestra, M. Timoteo (a cura di), *Major Legal Trends in the Digital Economy*, Il Mulino, Bologna, 2022.

diviene strumento di impulso della sostenibilità dell'attività della *Gesellschaft nella Gemeinschaft,* cioè dell'impresa societaria all'interno della comunità in cui opera, nella logica del "*successo sostenibile*" che il nuovo Codice di *Corporate Governance* entrato in vigore nel 2021 addita quale obiettivo al cui conseguimento sono chiamati gli organi di amministrazione delle società quotate.

Si tratta di due piani tra loro interrelati. Se la nostra società, intesa come *Gemeinschaft,* è oggi in larga misura condizionata dagli algoritmi, questi sistemi risultano in misura ancora più marcata immanenti alle realtà aziendali di ogni grande impresa in forma societaria (*Gesellschaft*), costituendone in alcuni casi il *core business*. Il riferimento è innanzi tutto alle grandi multinazionali dell'IT statunitensi, che si collocano da tempo al vertice delle società più capitalizzate e vengono indicate riassuntivamente con l'acronimo GAFAM (Google, Amazon, Facebook, Apple, Microsoft), nonché ad altre *web-platforms* di rilevanza planetaria (come Ali Baba, Baidu, Tencent e, sia pure su scala minore, la stessa Netflix). Il variegato processo di incorporazione delle nuove tecnologie negli assetti societari coinvolge peraltro una platea sempre più ampia di imprese, imponendo all'interprete il delicato compito di comprendere innanzi tutto la portata sostanziale delle trasformazioni in atto, la vivantiana «natura delle cose».

La trasformazione digitale risulta un passaggio ineludibile per tutte le aziende (ma anche per la pubblica amministrazione e per la stessa giustizia) sia per beneficiare pienamente dell'aumentata efficienza dovuta all'integrazione delle tecnologie nei processi e servizi, sia per acquisire le nuove abilità indispensabili per la missione di guida strategica dell'innovazione e stimolo alla crescita. Il processo di trasformazione digitale costituisce una precondizione per sfruttare appieno e indirizzare funzionalmente alle esigenze delle imprese, la gestione dei macrodati (i *big data*), la cui "distillazione" in metadati da parte della formidabile capacità computazionale dell'intelligenza artificiale gioca un ruolo sempre più cruciale per la previsione delle evoluzioni di mercato e, più in generale, per la simulazione di scenari futuri e dunque per il supporto alle decisioni strategiche. La transizione digitale è altresì rilevante sul fronte della *cybersecurity*, decisiva per garantire la protezione dei dati e degli asset tecnologici e di mercato (oltre alla *privacy* di clienti e dipendenti). Si tratta dunque di un processo destinato a irradiarsi, sia pure con diversi gradi di intensità, all'intero panorama imprenditoriale, ivi incluse le piccole e medie imprese, ove assume una importanza crescente lo sviluppo di metodologie e strumenti tecnologici innovativi e per la gestione dei rischi agli stessi correlati. Uno scenario inedito, nel quale accademia ed esperti della materia sono chiamati ad accompagnare le realtà aziendali nei passaggi chiave della loro trasformazione digitale, a partire dal ricorso consapevole alle piattaforme digitali per facilitare l'accesso ai dati e la messa a disposizione di servizi, all'adozione sostenibile di quelle tecnologie più "dirompenti" che sono

state già oggetto di importanti relazioni (intelligenza artificiale, data science, Internet-of-Things, DLT), sino allo sviluppo di nuovi percorsi educativi sulle tecnologie digitali per aumentare competitività e produttività del proprio personale.

Questi pur sintetici richiami confermano l'importanza dell'approccio interdisciplinare con il quale questo corso ha affrontato il tema dei riflessi giuridici delle nuove tecnologie, allargando l'indagine alla dimensione economica, ma prima ancora tecnologica di un fenomeno che si pone in misura crescente alla base del funzionamento fattuale delle realtà aziendali del nuovo millennio.

2. Intelligenza artificiale e macrodati

Questa pur breve ricognizione agevola la messa a fuoco della portata delle innovazioni tecnologiche nello specifico campo del diritto societario, che campeggia al centro delle considerazioni che si andranno a svolgere in funzione maieutica degli interventi all'interno del gruppo di lavoro che gli organizzatori mi hanno chiamato a coordinare.

Le relazioni che si sono succedute nelle prime due sessioni consentono di cogliere la portata del cambio di paradigma tecnologico costituito dall'intelligenza artificiale e l'esigenza, che tale cambio di paradigma postula, di riconsiderare alcuni assunti generali del nostro sistema giuridico. E permettono di collocare, nel quadro dei trecentosessanta gradi del tema generale, i "dieci gradi" di una trattazione che si concentrerà sui principali problemi che connotano la governance algoritmica delle società. Con l'ulteriore precisazione che non si tratterà il profilo della *liability* (e in particolare il problema della responsabilità da prodotto tecnologico), appuntando piuttosto l'attenzione sul versante della *accountability* e, più precisamente, sul grado di intensità con il quale il ricorso all'intelligenza artificiale è suscettibile di incidere sui doveri degli organi sociali, come *strumento* di governo delle impresa, e dunque *in primis* come tassello degli assetti organizzativi delle stesse, ma altresì come *oggetto* di governo, destinato ad un'opportuna regolamentazione mediante predisposizione di puntuali *policy* dell'intelligenza artificiale.

Prima di procedere all'esame di tali problemi, e dei loro corollari in punto di competenze e responsabilità degli amministratori, permettetemi di ricordare l'importanza, anche (e per alcuni versi, soprattutto) in questo campo, di supplementi di riflessioni e cautele onde prevenire possibili derive alle quali potrebbero condurre le semplicistiche scorciatoie di una diffusa, ma non sempre consapevole, mitizzazione dell'algoritmo (e dell'iper-razionalità garantita dalla macchina). Si tratta di superare un'idea astratta e «oggettiva» della intelligenza artificiale, considerando tale tecnologia nella sua effettiva dimensione funzionale: come ha

rilevato di recente Kate Crawford, «*un'infrastruttura, un'industria, una forma di esercizio del potere*» o, più propriamente, «*un registro di potere*»[2], dietro il quale vi sono creatori, controllori e proprietari con loro interessi e finalità non sempre trasparenti. E in tale prospettiva merita di essere richiamata la quarta delle nuove leggi della robotica proposte, nel solco e ad integrazione di quelle a suo tempo coniate da Asimov, da Frank Pasquale, per la quale «[*i] sistemi robotici e l'AI devono sempre indicare l'identità dei loro creatori, controllori e proprietari*»[3]. Sempre in questa direzione è stato puntualmente sottolineato che è meno importante chiedersi se una intelligenza artificiale sia buona o equa, quanto piuttosto quali forme di potere essa amplifichi, riproduca o abiliti, quali interessi promuova, e «*chi sopporti il maggior rischio di danno*»; e, in ultima istanza, chi ne sia il responsabile, cioè chi sia tenuto a rispondere delle conseguenze[4].

Questo approccio, più congeniale allo studioso di diritto commerciale che ha da sempre al centro della sua riflessione il governo del potere imprenditoriale e i diversi interessi coinvolti nel suo esercizio, consente di mettere meglio a fuoco l'impatto sul sistema imprenditoriale – e dunque, inevitabilmente, anche sul diritto delle imprese – di quel passaggio dalla società digitale alla società algoritmica, che, secondo l'OCSE e la maggior parte degli interpreti, segna l'avvento della «quarta rivoluzione industriale»[5].

Nel contesto ora sommariamente evocato, ma a ben altro livello esaminato durante il corso, si colloca la questione cruciale della *algocrazia* che costituisce uno degli elementi più rilevanti e, al contempo, inquietanti dell'evoluzione in esame, assumendo, per le derive alle quali si è assistito sul fronte concorrenziale,

---

[2] K. Crawford, *The Atlas of AI. Power, Politics and the Planetary Costs of Artificial Intelligence,* Yale University Press, New Haven, 2021 (ed. ita., *Né intelligente, né artificiale, Il lato oscuro dell'IA*, Il Mulino, Bologna, 2021).

[3] F. Pasquale, *New Laws of Robotics, Defending Human Expertise in the Age of AI,* Harvard University Press, Cambridge Mass., 2020 (ed. ita., *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, Luiss, Roma, 2021).

[4] F. Cabitza, *Deus in machina? L'uso umano delle macchine tra dipendenza e responsabilità*, in L. Floridi e F. Cabitza, *Intelligenza artificiale. L'uso delle nuove macchine*, Bompiani, Milano, 2021.

[5] Per tutti, L. Floridi, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Milano, 2017 e R. Brownsword, *Political Disruption, Technological Disruption and the Future of EU Private Law*, in *New Directions in European Private Law*, a cura di M. Tridimas e T. Durovic, London, 2021, 7 ss.; e v. già S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano, 2018. Tra i documenti OCSE, v. *Algorithms and Collusion – Note from the Business and Industry Advisory Committee, OCSE OECD Roundtable on Algorithms and Collusion*, 2017. Va peraltro sottolineato che, se la precedente rivoluzione, determinata dalla meccatronica e della microelettronica tra la fine degli anni Settanta e gli anni Ottanta del secolo scorso, poteva dirsi ancora una rivoluzione «industriale» (la terza, appunto), l'era algoritmica prefigura una dimensione definitivamente postindustriale.

i contorni di una *oligo-algocrazia*. Il potere tecnologico e fattuale sugli strumenti di intelligenza artificiale che viene esercitato dalle *big data company* ormai da tempo trascolora da un mero vantaggio competitivo a un decisivo potere di mercato; un potere che, come ha segnalato Mario Libertini, parrebbe intangibile, almeno secondo gli ordinari meccanismi di mercato. I principali operatori che irradiano il loro *God's Eye* sulla rete, consentendo ai loro algoritmi di profilare enormi quantità di dati (e tra questi, in primo luogo, i già ricordati «GAFAM»), godono di una posizione di predominio che ha indotto appunto a paventare i rischi di una deriva *oligo-algocratica*.

Una linea involutiva che riconsegna inquietante attualità alle preoccupazioni espresse in altri tempi da Norberto Bobbio con riferimento al potere che «che agisce accanto a quello dello Stato, insieme dentro e contro, sotto certi aspetti concorrente sotto altri connivente, che si vale del segreto non proprio per abbatterlo ma neppure per servirlo». La differenza, rispetto al contesto evocato da Bobbio, è che gli attuali contropoteri non operano nell'ombra, costituendo la più evidente – e visibilissima – manifestazione di quella che viene oggi definita «post-democrazia», nella quale le decisioni cruciali per la collettività – in una parola, la politica – non risiede più (o non più soltanto) nelle istituzioni democratiche che continuano bensì ad esistere, ma in una complessa convivenza con poteri extraistituzionali sempre più invadenti (e al contempo, per molti versi, più efficienti), con inevitabili conseguenze in punto di deficit democratico delle relative determinazioni.

Se questo tema è al centro dell'attenzione dei costituzionalisti – in quanto qui a venire in gioco è non solo la *privacy* dei cittadini, ma per così dire il *destiny* delle comunità in cui vivono (come insegna la vicenda *Cambridge Analytica*) – sul versante del diritto dell'impresa è stata sottolineata l'equazione che viene così a delinearsi tra dati necessari quali *input* di un dato servizio o prodotto digitale (ad esempio, i dati personali per un servizio di *social network*), da un lato, e potere di mercato, dall'altro, una equazione che si riflette in un inedito accentramento delle risorse tecnologiche nelle mani di poche grandi imprese e che permette a queste ultime di espandersi in mercati diversi e di «ribaltare» anche questi nuovi mercati a proprio favore secondo strategie c.d. di *tipping*[6]. Il risultato è quello di mercati digitali dalla caratterizzazione fortemente oligopo-

[6] Sui rischi di deriva oligoalgocratica derivanti dal dominio sui big data, si veda, nella dottrina italiana, G. Schneider, *European Intellectual Property and Data Protection in the Digital-algorithmic Economy: A Role Reversal?*, in *Journal of Intellectual Property Law and Practice*, 2018, 13, 3, 229 e ss.; Ead., *Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation Against Facebook*, in *Journal of European Competition Law & Practice,* 2018, 9, 213 e ss.

listica, dove gli strumenti di intelligenza artificiale e l'analisi di grandi quantità di dati innescano dinamiche di mercato foriere di disuguaglianze economiche e sociali, precludendo l'attivazione delle «naturali» tendenze correttive del mercato di schumpeteriana memoria[7].

3. Intelligenza artificiale e cibernetica societaria

È sullo sfondo ora sommariamente richiamato, tanto problematico quanto in continuo mutamento, che viene a collocarsi il tema dell'impatto dell'IA sul diritto societario, in generale, e, più precisamente, dei riflessi giuridici della sempre più pervasiva inclusione dei sistemi di intelligenza artificiale nell'ambito degli assetti organizzativi, amministrativi e contabili della società. Quest'area tematica si declina in una serie di questioni che si intersecano tra loro radialmente: in quale misura possono dirsi adeguati assetti societari che non facciano ricorso anche all'intelligenza artificiale? In quali realtà aziendali il ricorso agli strumenti di intelligenza artificiale può assurgere a vero e proprio dovere giuridico?

Ora, se consideriamo il problema dal «*dark side*» della responsabilità, intesa come *accountability* – ripeto, non della *liability* (di cui altri relatori si occupano in questo corso) – il tema si può considerare da due prospettive distinte.

Sotto un primo versante ci si potrebbe chiedere quali responsabilità possano derivare dal mancato ricorso a strumenti di intelligenza artificiale; e quali corollari potrebbero discendere dall'essersi discostati dalle indicazioni date da questi ultimi; ma anche, all'opposto, dall'averle pedissequamente seguite, senza un adeguato filtro critico. Sotto un secondo versante, la questione è come vada regolato e "governato" l'esercizio che la società fa di questi strumenti, tanto a livello di organi sociali, quanto a livello di management e di realtà aziendale[8].

Questa duplice prospettiva conferma l'ambivalenza concettuale dell'espressione «*governance* della intelligenza artificiale»: siamo cioè di fronte a un genitivo che è al tempo stesso un genitivo *soggettivo* (l'intelligenza artificiale che concorre a governare l'impresa e, magari, un domani la gestirà direttamente) e un genitivo *oggettivo* (l'intelligenza artificiale quale oggetto di governo e di regolamentazione da parte di chi è chiamato a gestire l'impresa e a monitorare tale gestione). Si tratta di due piani tra loro interrelati che dovrebbero idealmente convergere nella funzionalità degli stessi al conseguimento dell'oggetto sociale in coerenza con quel più ampio *corporate purpose* che viene oggi a collocarsi nella prospettiva

---

[7] F. Cabitza, *Deus in machina? L'uso umano delle macchine tra dipendenza e responsabilità*, cit., 81 s.

[8] Per sviluppi di questa impostazione v. N. Abriani e G. Schneider, *Diritto delle imprese e intelligenza artificiale*, Il Mulino, Bologna, 2021.

della "sostenibilità" nel medio e lungo periodo, come indica ora espressamente il Codice di Corporate Governance che concorre a regolare in termini autodisciplinari le società quotate italiane[9].

4. L'intelligenza artificiale tra sostenibilità e "infuturarsi" delle imprese

Se questa prospettiva ci proietta nel futuro, piace evocare un termine che esprime con insuperabile efficacia brachilogica la questione centrale posta dall'intelligenza artificiale: il termine è «*infuturarsi*», un *hapax* assoluto che compare soltanto nel diciassettesimo canto del *Paradiso*, in un verso che, per dirla con Flaiano, «vede oltre il telescopio di Galileo». E, a proposito della capacità predittiva dell'intelligenza artificiale, è appena il caso di ricordare che questo verbo formidabile campeggia al centro del discorso dell'antenato Cacciaguida, in una delle più celebri predizioni della letteratura di tutti i tempi[10]. La sfida che pone l'evoluzione tecnologica è, in estrema sintesi, quella di consentire alle imprese di *infuturarsi* in una doppia accezione.

i) La prima, più fedele al verso dantesco, indica il proiettarsi e il permanere nel futuro, in una versione meno rigorosa e trascendente dell'«*insemprarsi*» che lo stesso Dante utilizza nel decimo canto del Paradiso; una prospettiva che, calata dall'empireo lirico e ricondotta alle strade più sassose dell'incedere imprenditoriale, evoca concetti ben familiari, come la continuità aziendale e, in modo ancora più evidente, la sostenibilità nel lungo termine. E non v'è dubbio che uno degli insegnamenti della recente crisi pandemica sia rappresentato dalla accresciuta consapevolezza dell'esigenza di un'organizzazione imprenditoriale basata su assetti tecnologici avanzati che contribuiscano a fluidificarne i processi gestionali e, più in generale, a strutturare paradigmi efficienti e resilienti nei confronti di nuovi potenziali crisi sistemiche.

ii) Al contempo la prospettiva dell' "infuturarsi" indica una predisposizione verso il futuro, una *forma mentis* che consenta di affrontare e governare con consapevolezza l'innovazione. Solo chi si infutura in modo sostenibile, potrà veramente infuturarsi.

Sotto entrambi i versanti, si tratta di temi che percorrono la storia del pensiero filosofico e scientifico: già Carlo Levi ammoniva che «*il futuro ha un cuore antico*»;

---

[9] N. Abriani, *Il nuovo Codice di* Corporate Governance, in P. Montalenti, M. Notari (a cura di), *La nuova società quotata. Tutela degli stakeholders, sostenibilità e nuova* governance, Atti del convegno di Courmayeur, 9 aprile 2021, Milano, 2022.

[10] «*Tu proverai sì come sa di sale lo pane altrui, e come è duro calle lo scendere e 'l salir per l'altrui scale*».

e speculare rispetto a quel monito è l'incipit della poesia *Le tre parole più strane*, di Wislawa Szymborska: «*Quando pronuncio la parola Futuro, la prima sillaba va già al passato*». La convergenza dei due passi citati induce a rammentare, quando, agli albori del mio percorso universitario, nel corso di diritto romano all'Università di Torino, studiammo il libro di Andrea Di Porto su *Impresa collettiva e schiavo «manager» in Roma antica*, che integrava, arricchendolo di spunti per noi illuminanti, il corso di diritto romano. In effetti, è stato autorevolmente proposto di ricondurre alcuni dei nuovi problemi posti dalla responsabilità nel ricorso all'intelligenza artificiale a chiavi interpretative ricalcate sulle elaborazioni in tema di responsabilità per l'operato degli schiavi in epoca antica[11]. E se sono evidenti a tutti i *caveat* e i distinguo imposti dalla presenza in tal caso di intelligenze naturali generali, con la loro *umanità*, e che precludono trasposizioni anacronistiche, è il caso anche di ricordare che la Cina – che è uno dei più grandi esportatori di intelligenza artificiale – è anche ad oggi il maggior importatore di diritto romano.

La traiettoria storica va dallo schiavo manager alle idee combinatorie di Lullo e soprattutto di Leibniz, al suo *calculemus*, espresso in questi termini nella *Dissertatio de arte combinatoria*: «secondo ciò, quando sorga una controversia, non ci sarà più necessità di discussione tra due filosofi di quella che c'è tra due calcolatori. Sarà sufficiente prendere una penna, sedersi al tavolo e dirsi l'un l'altro: calcoliamo (*calculemus*)!».

Se quelli di Leibniz erano «pensieri ciechi», che si potevano realizzare attraverso meccanismi autodeterminati, senza avere conoscenza dei significati e dei contenuti pensati, come avviene nel caso dei simboli algebrici, in grado di rappresentare qualsiasi numero, su un piano diverso si pone il *cogitare* cartesiano, che conserva nel proprio etimo *cum agitare* (agitare insieme) e non si riduce dunque al mero pensare, configurandosi piuttosto come un agglomerato instabile di elementi diversi: un livello diverso e molto più problematico, essendo la *res cogitans*, nella definizione di Cartesio, «una cosa che dubita, comprende, afferma, nega, vuole, disvuole, immagina anche e percepisce»; e, come tale, ha piena coscienza del suo *agitarsi*»[12].

Il paradigma dell'intelligenza naturale è da sempre rappresentato, almeno per la cultura occidentale, dall'ingegno *multiforme* di un eroe definito da Omero

---

[11] Lo ha fatto magistralmente Ugo Ruffolo in una *lezione d'autore* ospitata online alla Sapienza durante la fase più dura della pandemia: U. Ruffolo, *Intelligenza artificiale e diritto*, https://www.giurisprudenza.uniroma1.it/archivionotizie/lezioni-dautore.

[12] Sul punto si vedano le illuminanti riflessioni di Remo Bodei nel suo ultimo libro, significativamente intitolato *Dominio e sottomissione. Schiavi, animali, macchine, intelligenza artificiale*, Il Mulino, Bologna, 2019.

polytropos e *polymetis*; e sono questi plurimi lati e sfaccettature, che, anche senza ascendere ai vertici di Ulisse, collocano – almeno ad oggi – l'evoluzione della nostra specie ad uno stadio molto più avanzato rispetto all'intelligenza artificiale, nonostante il crescente ricorso da parte di quest'ultima a reti neurali artificiali, composte da elementi fra loro collegati, che lavorano in sincrono sul modello dei neuroni biologici e delle loro sinapsi. E tale profilo appare ancora più rilevante ai fini della gestione di realtà imprenditoriali, dove è fondamentale l'elemento del coordinamento tra azioni diverse.

Naturalmente, da Cartesio ad oggi, molta acqua è passato sotto i ponti della Senna e del Tamigi. Dal passato remoto sopra evocato si giunge così al passato prossimo: da Turing e Wiener sino ad oggi, fra accelerazioni e mutazioni, le «primavere» e gli «inverni» della intelligenza artificiale, con riferimento ai quali alcuni dei nostri massimi giuristi hanno dato da tempo contributi magistrali e di assoluta attualità. E se il pensiero non può che andare innanzi tutto a Stefano Rodotà, va ricordato che all'inizio del secolo scorso un altro grande Maestro del diritto civile, Antonio Cicu, discuteva la sua tesi di laurea nell'Università di Sassari su *Gli automi del diritto:* era il 14 luglio del 1900 e due anni dopo Henri Poincaré pubblicava *La Science et l'Hypothèse*, consegnandoci la celebre frase «*la scienza si basa sui dati, ma un ammasso di dati è scienza come un mucchio di pietre è casa*». Un insegnamento ormai classico, e tra i più richiamati nel corso del Novecento, ma che si attaglia con particolare efficacia alla materia in esame, declinato in una parafrasi di una non meno celebre metafora kantiana: «*gli algoritmi senza i dati sono vuoti, i dati senza gli algoritmi sono ciechi*».

In effetti, sebbene si tenda a porre l'enfasi sulla endiadi «intelligenza artificiale», di indubbia efficacia anche sul piano del marketing (e non a caso venne coniata per acquisire adeguati finanziamenti al progetto di ricerca lanciato dai suoi ideatori), la mera considerazione dello strumento «intelligente» esprime una visione del fenomeno riduttiva e priva di efficacia euristica ai fini di una corretta comprensione dello stesso. L'elemento cruciale che connota l'era algoritmica non è rappresentato dalla macchina, ma dalla quantità e dalla qualità dei dati che questa è in condizione di elaborare: maggiore è la quantità di dati disponibili, maggiore è la capacità dell'algoritmo di generalizzare e di approssimare la funzione; e tanto migliore è la qualità dei dati immessi ed elaborati dalla macchina, tanto più accurati saranno gli *output* che sarà in grado di offrire.

5. Dalla *Fintech* alla *Corptech*

Queste ultime considerazioni ci riportano al tema al centro di questa presentazione: l'utilizzo dei sistemi di intelligenza artificiale come supporto alla gestio-

ne societaria e come *output* dell'attività d'impresa; e in particolare l'utilizzo degli strumenti di intelligenza artificiale per l'esercizio delle funzioni di gestione, indirizzo strategico societario, monitoring valutativo e vigilanza in senso stretto (o «in purezza»), nelle quali si articolano le competenze degli organi amministrativi e di controllo delle società per azioni, secondo la tassonomia funzionale adottata nelle *Disposizioni sul governo societario delle banche* emanate dalla Banca d'Italia, basata come noto sulla tripartizione, di chiara ispirazione «ferro-luzziana», tra funzioni propriamente gestorie-esecutive, di indirizzo e supervisione strategica e di controllo[13].

È questo l'approdo di un percorso sviluppatosi dapprima nei processi di mercato, che da tempo vedono la maggior parte delle scelte di investimento basate sui meccanismi automatizzati propri del *trading* algoritmico, nel più ampio ambito della c.d. *Fintech*, e successivamente irradiatosi all'esercizio delle funzioni di vigilanza da parte delle autorità preposte, che a loro volta sollecitano il ricorso a strumenti di intelligenza artificiale da parte dei soggetti vigilati (c.d. *Regtech* e *Suptech*), fino a penetrare il tessuto delle stesse imprese societarie e i relativi organi di amministrazione e controllo in quella che è stata efficacemente definita come *Corptech* o *Corptech Governance*. Quest'ultima espressione, coniata in quello che è uno dei contributi di riferimento nella materia in esame[14] – e preferibile, in quanto più ampio e comprensiva, rispetto alla formula della *platform governance*, incentrata principalmente sulla *governance* delle piattaforme[15] – si potrebbe declinare, più classicamente, come la «cibernetica societaria» del nuovo millennio. Un sostantivo, quest'ultimo, che esprime in termini riassuntivi la nuova *governance* dell'era algoritmica e che si rivela particolarmente efficace ove si consideri, da un lato, che è proprio la potenza cibernetica che permette ai sistemi tecnologici più avanzati di trascendere la tradizionale funzione di «strumento» destinato a realizzare finalità decise da un soggetto agente umano, per fornire essi stessi indicazioni e finanche assumere decisioni rilevanti per la libertà e la persona umana; e, dall'altro, che l'etimo di *governance* risale al *gubernum* latino, il quale ha a sua volta come radice il *kybernétes* greco.

Al di là della denominazione prescelta, in tale ambito possono ricondursi le diverse possibilità offerte dall'impiego dei sistemi di *machine-learning*, tra cui si

---

[13] P. Ferro-Luzzi, *L'esercizio d'impresa tra amministrazione e controllo*, in *An. giur. econ.*, 2007, 1, 231 ss.

[14] L. Enriques e D. Zetzsche, *Corporate Technologies and the Tech Nirvana Fallacy*, in *Hastings Law Journal*, 72, 2020, 55 ss.

[15] M. Fenwick, J.A. McCahery e E.P.M. Vermeulen, *The End of Corporate Governance (Hello "Platform Governance")*, in *European Business Organization Law Review*, 20, 2019, 171 ss.

annovera appunto l'intelligenza artificiale, e di *distributed ledger technology*, di cui *blockchain* e *smart contracts* sono le manifestazioni più note.

6. L'intelligenza artificiale come strumento di governo

L'importanza del fenomeno, testimoniata anche da un recente studio ad esso dedicato dalla Commissione europea[16], si può apprezzare da un duplice angolo prospettico. Si tratta, da un lato, di esaminare le opportunità della intelligenza artificiale come «strumento» di governo dell'impresa, a supporto delle decisioni degli amministratori; dall'altro, di considerare i rischi che il ricorso a tali tecnologie può determinare, facendone dunque «oggetto» di una puntuale regolamentazione volta a governarli e, per quanto possibile, mitigarli.

La prima area tematica – l'intelligenza artificiale come *strumento* di governo – è quella più ampiamente trattata dai (pur pionieristici) studi in materia che, da questa prospettiva, hanno già offerto importanti contributi all'esame della interazione tra *corporate governance* e intelligenza artificiale, in relazione, come si è anticipato, all'utilizzo di quest'ultima a supporto delle funzioni amministrative: e ciò tanto nella declinazione propriamente gestoria, affidata ai consiglieri esecutivi, quanto in quella di indirizzo strategico e *monitoring* valutativo, che è propria dell'organo collegiale.

A questo riguardo assume un rilievo centrale il già evocato problema della inclusione degli strumenti dell'intelligenza artificiale nell'ambito degli assetti organizzativi, amministrativi e contabili della società. Un tema che si articola, a sua volta, in una serie di questioni che si intersecano tra loro radialmente: in quale misura possono dirsi adeguati assetti societari che non facciano ricorso anche all'intelligenza artificiale? Come vanno ridefinite le categorie dell'informazione adeguata al fine dell'assunzione di decisioni consapevoli (e quella, speculare, del difetto di istruttoria) nella *governance* algoritmica? E ancora, sotto altro versante, quali conoscenze tecniche sono – e saranno sempre più in futuro – richieste ai componenti dell'organo amministrativo ai fini di un utilizzo consapevole degli algoritmi o, quanto meno, di un adeguato monitoraggio su tale utilizzo da parte del *management*?

Quest'ultimo quesito sospinge l'analisi verso il possibile ricorso all'intelligenza artificiale nella stessa attività di autovalutazione del consiglio di amministrazione in ordine alla propria composizione e al fine di selezionare i migliori

[16] Commissione europea, *Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance,* giugno 2021, reperibile all'indirizzo https://op.europa.eu/en/publication-detail/-/publication/13e6a212-6181-11ec-9c6c-01aa75ed71a1/language-en.

candidati alla carica di amministratore: tema, quest'ultimo che assume particolare delicatezza in presenza di clausole statutarie che prevedano la predisposizione di una lista del consiglio di amministrazione, ma anche, più in generale, nelle più frequenti ipotesi in cui quest'ultimo sia chiamato a procedere alla cooptazione di nuovi componenti in sostituzione di consiglieri cessati dalla carica in corso di mandato[17].

Un ulteriore campo nel quale le tecnologie algoritmiche potrebbero essere utilmente impiegate dall'organo amministrativo – nell'ambito della funzione di valutazione e intervento «proattivo» sugli assetti statutari in funzione degli obiettivi di una più efficiente *governance* societaria, che il nuovo Codice di *Corporate Governance* assegna al consiglio – potrebbe ravvisarsi nel rafforzamento del dialogo e dell'interlocuzione biunivoca con gli azionisti o ancora nella stima dell'impatto che eventuali modifiche dei diritti amministrativi e patrimoniali delle azioni e degli altri strumenti finanziari sono destinate a produrre sugli assetti proprietari e, più in generale, degli effetti di mercato e strategici, conseguenti[18].

7. L'intelligenza artificiale come oggetto di governo

Il secondo angolo prospettico della *Corptech* considera l'intelligenza artificiale come *oggetto* di governo, muovendo da un'attenta valutazione dei peculiari rischi connessi al ricorso ai nuovi strumenti tecnologici, che richiedono un loro adeguato monitoraggio, sollecitandone una puntuale regolamentazione: un governo e una regolamentazione dei rischi tecnologici che compete all'organo amministrativo, entro margini di discrezionalità tecnica e in considerazione del rapporto costi/benefici degli sviluppi connessi all'utilizzo di sistemi di intelligenza artificiale.

Nel nuovo scenario che viene così a delinearsi le imprese sono chiamate ad affrontare la sfida della digitalizzazione e, ancora più in vertice, quella che viene definita come *Corporate Digital Responsibility*, intesa appunto come responsabilità derivante dalla gestione dei rischi connessi alla prima. In questa prospettiva si tratta non soltanto di operare un efficiente *risk management,* ma di valutare con

---

[17] E v. per alcuni primi spunti N. Abriani, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *NDS*, 2020, 261 ss.

[18] N. Abriani, *Il nuovo Codice di* Corporate Governance, cit. Per sviluppi di questa impostazione v. C. Picciau, *The (Un)Predictable Impact of Technology on Corporate Governance*, in *Hastings Business Law Journal*, 17, 2021, 1, 114 ss.; M.L. Montagnani, *Il ruolo dell'intelligenza artificiale nel funzionamento del consiglio di amministrazione delle società per azioni*, Egea, Milano, 2021.

attenzione in quali ambiti e a quali condizioni la *Corptech* sia suscettibile di (o sia addirittura destinata a) valorizzare la *governance* societaria; e in quale misura, a quali livelli e con quali presidi tale evoluzione possa tradursi operativamente, non solo nella dimensione propriamente esecutiva del *management* (dove è già in larga misura presente), ma anche come strumento per rendere più incisiva la funzione di *monitoring* e *advisory* del *board*, da un lato, e per rafforzare il dialogo (e, in generale, i rapporti) tra la società e i propri azionisti, consentendo una più efficace interlocuzione con questi ultimi e i principali *stakeholders*, fino ad arrivare, nelle ipotesi più rivoluzionarie, alle sperimentazioni delle *decentralised autonomous organisations (DAOs),* realtà associative dove l'architettura tecnologica costituita dalla *blockchain* struttura, principalmente mediante *smart contracts*, le relazioni tra i partecipanti all'organizzazione stessa, senza uno statuto o un accordo fondativo.

8. Segue. Dalla *Corptech* alla *Corporate Digital Responsibility*

Nella logica di una efficiente *Corporate Digital Responsibility* si potrebbero porre le premesse per un recepimento all'interno delle *policy* delle società delle istanze contenute negli *Orientamenti per un'intelligenza artificiale affidabile*, di per sé privi di immediata valenza giuridica e, in termini più analitici, dei principi ora espressi dalla proposta di regolamento sulla intelligenza artificiale, di cui altri relatori si sono occupati in questo corso. Nella prospettiva della sostenibilità andrebbe innanzi tutto verificato se gli strumenti in concreto utilizzati dalla società presentino i requisiti, in primo luogo di trasparenza, previsti dalla proposta di regolamento per i sistemi di intelligenza artificiale cc.dd. ad alto rischio, indipendentemente dalla effettiva riconducibilità a tale categoria degli strumenti usati in ambito societario a supporto di decisioni strategiche od operative e, tanto meno, dell'attività di *monitoring* valutativo del consiglio. In altra sede si sono sottolineate le difficoltà che il testo della proposta di regolamento pone all'interprete nel sussumere gli strumenti di intelligenza artificiale utilizzati nell'esercizio delle funzioni degli organi di amministrazione e controllo all'interno della categoria dei sistemi ad alto rischio[19]. In effetti, la lettura degli elenchi contenuti negli allegati alla proposta segnala riferimenti agli strumenti di intelligenza artificiale finalizzati a determinare l'accesso a servizi privati essenziali come il credito e dunque utilizzati «per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito»; al di fuori di questa specifica ipotesi, che riguarda le sole

[19] N. Abriani e G. Schneider, *Diritto delle imprese e intelligenza artificiale*, cit., spec. 140 ss. e 191 ss.

imprese attive nel settore creditizio, gli strumenti di intelligenza artificiale usati in ambito societario non sembrerebbero ricadere nell'ambito regolatorio dei sistemi considerati ad alto rischio.

Ma, al di là della sua formulazione finale, la proposta di Regolamento è suscettibile di assumere una duplice valenza, al contempo diretta e indiretta, nel campo in esame: *i*) diretta, in quanto imporrà di verificare la piena *compliance* alle nuove previsioni degli strumenti utilizzati nella realtà aziendale (ove questi siano riconducibili per il loro specifico oggetto alla tassonomia di cui agli allegati); *ii*) indiretta, in quanto potrebbe (*recte*, dovrebbe) indurre le società a informare il ricorso agli strumenti decisori latamente qualificabili di *Corptech* (e, in particolare, quelli in funzione di *roboadvisory*) alle regole precauzionali e ai principi etici che ispirano la proposta di disciplina eurounitaria. Si verrebbero così a integrare le politiche ESG con l'ulteriore e coessenziale tassello della *Corporate Digital Responsibility*, intesa come un insieme di pratiche e comportamenti che aiutano organizzazioni complesse, quali sono le grandi imprese societarie, a usare i dati e la tecnologia in modo responsabile, anche a livello sociale ed ambientale, oltre che economico e propriamente tecnologico.

Essenziale a questi fini è la conservazione di un approccio antropocentrico alla gestione societaria le cui redini devono essere saldamente ancorate a quello che l'art. 14 della proposta di regolamento europeo sull'intelligenza artificiale definisce requisito della «supervisione umana» (principio già imposto, per il trattamento dei dati personali, dall'art. 22 del GDPR). L'approccio antropocentrico è del resto elemento cardine di applicazioni di intelligenza artificiale che possano definirsi propriamente «etiche» ai sensi degli *Orientamenti* sopra richiamati, nonché scudo essenziale per scongiurare derive automatizzate del governo societario che finirebbero per tramutare i caratteri fondamentali dell'impresa così come fino ad oggi concepita.

A questo riguardo meritano di essere richiamate due recenti iniziative del *Bundesministerium der Justiz* tedesco e del Governo francese, entrambe in materia proprio di *Corporate Digital Responsibility*[20], cui ha fatto seguito nell'estate di quest'anno la già ricordata iniziativa della Commissione europea[21]. L'obiettivo sotteso a queste iniziative è promuovere uno sviluppo responsabile del processo di trasformazione digitale riguardante le imprese, procedendo a una mappatura dei nuovi obblighi e delle aree di responsabilità d'impresa derivanti dai processi di

---

[20] Bundesministerium für Justiz und Verbraucherschutz, *Corporate Digital Responsibility Initiative: Shaping the Digitalization Process Responsibly: A Joint Platform*; Id., *Szenarientechnik der CDR Initiative*, 2 aprile 2019; France Stratégie, *Corporate Digital Responsibility – 1. Data Key Isuues Synthesis*.

[21] E v. *supra* alla nt. 16.

digitalizzazione, nonché di individuare le imprese adempienti. La premessa dalla quale muovono è il riconoscimento della sussistenza di una lacuna rispetto al coordinamento tra i requisiti regolatori in materia di strumenti tecnologici digitali e responsabilità sociale d'impresa. In questa prospettiva, la sensibilizzazione sui rischi tecnologici nel contesto societario è considerata una precondizione essenziale per creare una transizione digitale etica e corretta (*fair*). L'obiettivo ultimo è quello di promuovere un processo di digitalizzazione responsabile delle imprese mediante la condivisione di *best practices* e di strategie di *problem solving,* alla luce della nuova rilevanza di questa nuova area di responsabilità «sociale» o, più correttamente, «tecnologica» delle imprese.

Sempre in questa prospettiva non è casuale che nel regolamento istitutivo del dispositivo per la ripresa e la resilienza si ponga in risalto la necessaria convergenza tra transizione verde e trasformazione digitale, così come nel piano nazionale di resilienza presentato dal governo italiano[22]; ed è parimenti significativo che anche un recente studio Assonime sui doveri degli amministratori indichi nella digitalizzazione delle imprese un *driver* fondamentale di evoluzione verso la sostenibilità[23].

9. *Corptech* e codici di autodisciplina

Evidenti sono le implicazioni di quanto sin qui osservato sulla *corporate governance*, in generale, e sulla responsabilità degli amministratori, in particolare.

Sul primo versante va peraltro stigmatizzato che le opportunità e i rischi connessi all'utilizzo della intelligenza artificiale non trovano ancor oggi riscontro in alcuna delle disposizioni contenute nei codici di autodisciplina delle società quotate, a cominciare dal nuovo Codice di *Corporate Governance* italiano entrato in vigore nel 2021.

Questa perdurante disattenzione al fenomeno, per molti versi sorprendente ove si consideri la posizione di avanguardia storicamente assunta dall'autodisciplina in questo settore – che registra due sole eccezioni su scala europea nel *Código de buen gobierno de las societades cotizadas* spagnolo, recentemente riformato nel 2020, e soprattutto nel Codice di C*orporate Governance* olandese, che pure risale al 2016 – sembra tradire una preoccupazione, comune ai redattori dei codici di *corporate governance*, di mantenersi fedele all'ispirazione che ha tradizionalmente indirizzato l'intervento dell'autodisciplina in questo settore;

[22] Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, 18 febbraio 2021, OJ L. 57/17.

[23] ASSONIME, *Doveri degli amministratori e sostenibilità,* Rapporto del 18 marzo 2021.

e, in particolare, di preservare l'effettiva dialettica tra amministratori, rispetto alla quale i tradizionali rischi di *bias* autoritari nei confronti dei *top manager* potrebbero essere rafforzati (e, per alcuni versi, esorcizzati) dalla sudditanza alla indicazione-predizione algoritmica. Una impostazione che si potrebbe definire «romantica», nella sua strenua difesa del libero confronto consiliare in contrapposizione all'«illuminismo iper-razionalista» di chi pretenderebbe di acquisire come punto di riferimento dell'*agere* degli amministratori l'algido *output* dello strumento tecnologico.

Una preoccupazione, quest'ultima, che risulta peraltro più che giustificata ove si consideri che potrebbe essere lo stesso *management* a definire le finalità (lo *script*) del sistema robotico e a selezionare i dati che quest'ultimo è chiamato ad elaborare. Sotto questo versante, gli strumenti in esame possono ottimizzare l'opportunismo del *top management* che li controlla e che potrebbe usarli per agire per il proprio tornaconto e non nell'interesse della società, esorcizzando i conflitti d'interesse dietro un'illusoria oggettività e inevitabilità delle opzioni suggerite dalla macchina, inducendo il consiglio di amministrazione ad accettarle come «oro colato», rendendo i componenti non esecutivi ancora più acritici di quanto già tendono ad essere in considerazione del fatto che non hanno un accesso diretto alle informazioni.

Ma proprio la gravità di questi rischi vale a sottolineare la potenziale incidenza del ricorso a sistemi robotici sulla *corporate governance* e rafforza dunque l'esigenza di affrontare adeguatamente il problema: sin d'ora, in sede di *best practice* e di *policy* interne alle stesse società, e, in un futuro sempre più prossimo, in una declinazione di regole autodisciplinari.

10. Nuovi profili di responsabilità degli amministratori

Le considerazioni sin qui svolte impongono infine di riconsiderare alcuni approcci tradizionali in ordine alla responsabilità degli amministratori. La *Corptech* implica infatti un ripensamento dei generali doveri inerenti ai protocolli istruttori (dovere di agire informati) e organizzativi (doveri di predisporre assetti adeguati) che costituiscono i pilastri della corretta amministrazione ai sensi degli artt. 2381 e 2403 c.c.[24].

Tra le questioni nuove che la giurisprudenza sarà chiamata ad affrontare vi è la domanda, già evocata, se e in quale misura possano dirsi adeguati assetti or-

[24] Ma altresì, per la s.r.l., art. 2475, per le realtà di gruppo, art. 2497, nonché, per tutte le imprese collettive, art. 2086, comma 2, c.c. (su cui *infra* nel testo).

ganizzativi societari che non facciano ricorso all'intelligenza artificiale. Questione che si traduce nell'eventuale configurazione di un vero e proprio dovere giuridico di ricorrere a strumenti di intelligenza artificiale. In altre parole, traslitterando la domanda nel *dark side* della responsabilità: in quali realtà organizzative e sotto quali profili gli amministratori potranno essere condannati a risarcire i danni subiti dalla società e dai suoi creditori per un mancato o inadeguato utilizzo di questi strumenti tecnologici?

Il pensiero corre naturalmente alla nuova formulazione dell'art. 2086 c.c., e alla regola di adeguatezza degli assetti anche in funzione della prevenzione della crisi: quale ruolo può rivestire l'intelligenza artificiale nella elaborazione dei dati che consentono di percepire tempestivamente i segnali di crisi e di prevenire in tal modo derive liquidatorie, conservando la continuità aziendale? E quale ruolo nella definizione dello strumento più adatto per risolvere la crisi stessa, e nella verifica dei risultati dei piani di risanamento? Tema quest'ultimo sottovalutato dalla dottrina, ma centrale sul piano operativo: l'esperienza ci insegna che, quando si omologa un concordato o un accordo di ristrutturazione, è un po' come in quella «festa», passata quale si ritiene ormai di aver «gabbato il santo»; mentre è proprio nella fase esecutiva che il più delle volte i nodi vengono al pettine, sicché è dovere fondamentale degli amministratori (e dei sindaci, lato vigilanza) verificare, pietra miliare per pietra miliare (*milestone by milestone*), l'effettivo rispetto e l'effettiva efficacia del piano di ristrutturazione in fase di realizzazione. E vi è un primo ed evidente collegamento tra questi due piani: uno degli elementi cha andranno doverosamente considerati nella valutazione (e attestazione) della fattibilità del piano di risanamento, non potrà non essere l'adeguatezza degli assetti a monitorarne efficacemente l'attuazione e gli eventuali scostamenti rispetto alle previsioni di piano[25].

Anche da questa prospettiva, il ricorso all'intelligenza artificiale può diventare un vero e proprio dovere giuridico, in relazione al settore e alle dimensioni dell'impresa (secondo le indicazioni opportunamente «relativizzanti» del codice civile, che riferisce il parametro «alla natura e alle dimensioni dell'impresa»), con i già ricordati corollari in punto di competenze richieste ai componenti dell'organo amministrativo (*recte*, all'organo amministrativo nel suo complesso) per poter utilizzare consapevolmente gli algoritmi e, prima ancora, valutare l'utilizzo da parte del management.

Si tratta di questioni tanto delicate, quanto ineludibili, suscettibili di ridefinire – e, per così dire, «riperimetrare» – sia i principi di corretta amministrazione,

[25] E ancora una volta in tale vaglio di adeguatezza potrebbe assumere rilievo il ricorso a strumenti di intelligenza artificiale: N. Abriani, *La* corporate governance *nell'era dell'algoritmo*, cit., 261 ss.

sia la portata della *business judgement rule*; ma, prima ancora, lo stesso *business purpose*, in funzione dell'ampliamento dell'interesse sociale in una prospettiva di sostenibilità di lungo periodo e di inedite e più efficienti modalità di conseguimento degli obiettivi che verso lo stesso convergono.

Nei grandi studi legali sempre più diffuso è il ricorso a sistemi c.d. di *Legaltech*, in particolare per valutazioni prognostiche delle prospettive di successo di *class action*, tra le quali fanno spicco, al di là dell'Atlantico, azioni sociali di responsabilità promosse secondo il meccanismo della *derivative suit*, sovente accompagnato da patti di quota lite. Lo strumento di *Legaltech* viene in queste ipotesi attivato inserendo una serie di dati noti (tra i quali l'evento dannoso ormai verificatosi), per risalire a ritroso ai fatti che l'abbiano cagionato, sulla base di una serie finita di precedenti giudiziali e di una serie potenzialmente assai ampia di concatenazioni di eventi analoghi. Com'è stato osservato, lo strumento di *Corptech* utilizzato dagli amministratori a supporto delle loro decisioni gestorie si pone su un piano diverso e obiettivamente più problematico: in questo caso, infatti, lo strumento utilizza i dati a disposizione (l'esperienza e la giurisprudenza passate, *in primis*) «per articolare scenari sulla base di tutti i fatti già noti e di quelli futuri ma ragionevolmente (secondo l'algoritmo) prevedibili». Il vantaggio del prodotto di *Legaltech* su quello di *Corptech* è evidente: «il primo potrà infatti ignorare i fatti che non si saranno verificati o che, pur verificatisi, per qualunque contingente insieme di circostanze, non avranno inciso sul risultato finale. Il secondo, al contrario, potrà selezionare molto meno e, al contempo, potrebbe non considerare anche fatti che, *ex post*, e per quanto imprevedibilmente anche per una macchina dalla "intelligenza" superiore a quella di un essere umano, si saranno disvelati eziologicamente rilevanti»[26].

Ora, il vantaggio del prodotto di *Legaltech* è, a ben vedere, lo stesso vantaggio che avrà il giudice chiamato a decidere sulla responsabilità degli amministratori, magari avvalendosi a sua volta di uno strumento di intelligenza artificiale: una macchina in funzione di perito del giudice (ma forse qualcosa di più, avvicinandosi al parere del Pubblico Ministero nei giudizi innanzi alla Suprema Corte) che non soltanto si gioverebbe di dati ulteriori (appunto, del senno di poi) ma potrebbe avere un diverso script e capacità computazionale più avanzata (il che

---

[26] L. Enriques, *Responsabilità degli amministratori e ruolo degli algoritmi: brevi annotazioni sul senno di poi 4.0*, in *Intelligenza artificiale – Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Giuffrè, Milano, 2020, 295 ss., ove si soggiunge che il prodotto *CorpTech* richiede di essere tarato, nel senso di poter evidenziare solo un sottoinsieme di scenari rilevanti, scartando quelli meno probabili, alla luce dei limiti che gli umani che siedono nel consiglio d'amministrazione presentano sul piano sia della capacità di elaborare informazioni, sia del tempo da dedicare a ogni decisione.

non stupirebbe, data la rapidità di evoluzione di questo settore) rispetto a quella utilizzata anni addietro dall'organo amministrativo, al momento della decisioni rivelatasi *ex post* dannosa.

In questo quadro, quali margini restano alla regola di insindacabilità del merito delle decisioni imprenditoriali? Può dirsi inescusabile l'errore di gestione operato dagli amministratori che abbiano disatteso le indicazioni del sistema di intelligenza artificiale? Ma non rischiamo così di appiattire in una sorta di logica conformista la gestione, una gestione che invece deve essere attiva, coraggiosa, innovativa, e che è tutelata dalla *business judgment rule* proprio in tale prospettiva? Per questa ragione occorre valutare con estrema prudenza l'imposizione di oneri di motivazione che, quand'anche fossero configurabili, non andrebbero declinati diversamente a seconda che si segua o si disattenda l'indicazione algoritmica. In questo quadro andrebbe riconsiderata la proposta – a suo tempo avanzata in termini dubitativi[27] – di richiedere una motivazione «forte», in caso di scostamento dalle indicazioni dell'intelligenza artificiale[28], e una motivazione «debole», quando invece si seguissero tali indicazioni[29].

Sono questioni che rimetto alla riflessione del gruppo di lavoro, in termini inevitabilmente interlocutori, limitandomi a sottolineare l'intreccio quasi osmotico che presentano rispetto ai temi, a voi più familiari, della giustizia predittiva. L'unica certezza che mi sentirei di consegnare, tanto con riguardo al decidere degli organi sociali quanto allo *ius dicere* dell'autorità giudiziaria, è che gli *output* della macchina non possono mai essere oggetto di un pedissequo recepimento, per le ragioni che altri, e ad altro livello, hanno in questa sede ricordato, nella consapevolezza dei delicati problemi di selezione dei dati; e, prima ancora, della circostanza che «*dato*» è un participio passato che, in quanto tale, porta con sé, inevitabilmente, le incrostazioni di pregiudizi potenzialmente discriminatori o comunque suscettibili di dissuadere da quelle sperimentazioni coraggiose che costituiscono la cifra caratterizzante l'innovazione imprenditoriale, consentendo elementi di virtuosa discontinuità – o, più nettamente, di *disruption* – rispetto al passato.

Per quanto l'evoluzione tecnologica possa rendere i nuovi strumenti sempre più idonei a contribuire a un'efficace gestione delle imprese (e della giustizia),

---

[27] N. Abriani, *La* corporate governance *nell'era dell'algoritmo*, loc. ult. cit.

[28] Una motivazione avvicinabile a quella richiesta dall'art. 2391 c.c. per operazioni in cui sono interessati gli amministratori o parti correlate, dove bisogna dimostrare *la convenienza* per la società.

[29] Come quella richiesta per le operazioni indirizzate dalla holding nell'ambito della direzione e coordinamento, ove è sufficiente dimostrare *l'interesse* della società in una logica di gruppo, ai sensi dell'art. 2497-*ter* c.c.

va tenuto presente che gli algoritmi sono strumenti comunque vincolati a dei *patterns* che, quand'anche "adattivi" e auto-generati, restano soggetti a un determinismo intrinseco derivante dai criteri sulla base dei quali la macchina si è formata o che la stessa ha elaborato a fini predittivi. Proprio in quanto strumento *di natura digitale*, l'intelligenza artificiale per definizione non può non funzionare se non sulla base di bit e calcoli matematici deterministici; e questi caratteri strutturali la rendono strutturalmente inidonea a replicare la complessità del ragionamento umano, imponendo cautele e supplementi di attenzione che costituiscono il doveroso comun denominatore, pur con i necessari distinguo, di ogni riflessione in tema tanto di cibernetica societaria, quanto di giustizia predittiva, nella consapevolezza che "*la ragione nel diritto (…) si connette al probabile, all'opinabile, al plausibile*", da ciò discendendo la necessità di preservare un'area di "*coscienza non automatizzata in grado di fronteggiare e governare l'automatismo delle macchine*"[30].

[30] G. Zaccaria, *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. dir. civ.*, 2020, 277 ss..

Giorgio Resta

Le decisioni algoritmiche e le frontiere dell'uguaglianza

1. Governare l'innovazione tecnologica: l'incrocio tra *big data* e *machine learning*

Queste pagine intendono svolgere alcune riflessioni, dal punto di vista del giurista, sui problemi posti dal ricorso agli algoritmi quali strumenti di decisione sia in ambito pubblico sia in ambito privato[1].

È bene chiarire sin da ora che, per apprezzare correttamente la reale natura delle questioni coinvolte, è necessario concentrarsi non soltanto sul profilo dell'automazione nelle decisioni (algoritmi e *machine learning*), ma anche su quello della disponibilità di una massa enorme di dati, sulla quale si appuntano le tecniche di *data analytics* e che quindi rappresenta il presupposto essenziale per il funzionamento dei moderni algoritmi di apprendimento automatico[2]. *Big data* e *machine learning,* in altri termini, sono i fattori fondamentali alla base delle due cruciali questioni regolatorie con le quali la società è oggi chiamata a confrontarsi:

a) come disciplinare la raccolta e l'uso dei dati fruibili per i trattamenti algoritmici (questione "a monte");

---

[1] Sulla nozione di algoritmo, quale descrizione formalizzata e astratta di una procedura computazionale, e le sue implicazioni giuridiche v. W. Hoffmann-Riem, *Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, Archiv des* öffent. *Rechts,* 142 (2017), 2 ss.

[2] Sul punto D. Pedreschi – F. Giannotti et al., *Open the Black Box. Data-driven Explanation of Black Box Decision Systems,* in *ArXiv,* 1 (2018), 1-2; S. Barocas – A.D. Selbst, *Big Data's Disparate Impact,* 104 *California L. Rev.* 671 (2016).

b) come regolare il processo decisionale in quanto tale, sia nel suo *iter* procedimentale sia nei suoi effetti sociali, in modo da assicurare un equilibrato bilanciamento degli interessi collettivi coinvolti (questione "a valle").

Su entrambi gli aspetti la discussione è accesa e non mancano esempi di interventi normativi, decisioni giurisprudenziali o prassi operative, dei quali si darà conto nelle pagine che seguono. La notevole attenzione rivolta alle suddette questioni – in ambito accademico, da parte di istituzioni ed enti di ricerca[3], nonché talora anche in sede di azione politica, come nell'esempio del *Koalitionsvertrag* tedesco tra CDU, CSU e SPD del 2018 – riflette una chiara consapevolezza della profonda ambiguità di tutti i grandi processi di innovazione tecnologica, capaci di imprimere una netta discontinuità alle dinamiche evolutive della società. Da un lato essi possono avere una valenza fortemente emancipatoria, redistribuendo il potere sociale e creando opportunità di crescita, progresso e miglioramento della condizione umana. Dall'altro, se non sono democraticamente governati, rischiano di consolidare le posizioni di privilegio, le disuguaglianze e le asimmetrie di potere esistenti in una data comunità organizzata[4].

È stato così per le innovazioni collegate alla prima rivoluzione industriale – e le lucide pagine di Karl Marx e Karl Polanyi stanno tuttora a ricordarcelo – ed è così per quelle della quarta rivoluzione[5]. Far pendere il piatto della bilancia verso l'uno o verso l'altro polo è il frutto di scelte sociali, rispetto alle quali la mediazione giuridica svolge un ruolo centrale. Ciò è ancor più vero in relazione alle innovazioni legate al mondo digitale, non foss'altro perché qui viene meno il primo e più elementare strumento di controllo e tutela dei beni, rappresentato dal possesso materiale. Rispetto ai beni intangibili, come l'informazione, qualsiasi meccanismo di allocazione esclusiva presuppone necessariamente l'intervento

---

[3] Mi limito a ricordare i seguenti rapporti e documenti: House of Lords, Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?,* London, 2018; AI Now *Report 2018;* Council of Europe, *Discrimination, artificial intelligence, and algorithmic decision-making,* a cura di F.Z. Borgesius, Strasbourg, 2018; Art. 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* last revised February 2018; Council of Europe, *Draft Guidelines on Artificial Intelligence,* 2018; Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability,* Washington, 2014; Executive Office of the President of USA, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights,* 2016.

[4] In generale, ed altresì con riferimento alle tecniche di intelligenza artificiale, v. R. Baldwin, *The Globotics Upheaval. Globalization, Robotics, and the Future of Work,* Oxford, 2019; v. altresì S. Rodotà, *Tecnologie e diritti,* Bologna, 1997.

[5] V. ancora R. Baldwin, *The Globotics Upheaval. Globalization, Robotics, and the Future of Work, passim*.

del diritto, che, come nel caso dei diritti di proprietà intellettuale, può creare situazioni di scarsità artificiale al fine di stimolare l'accumulazione di conoscenza e la produzione di innovazione. Misurare i caratteri e i limiti dell'intervento giuridico è allora essenziale, perché l'adozione di modelli di governo non equilibrati e troppo sbilanciati sul polo della protezione rischia – a tacer d'altro – di allargare in maniera sproporzionata le sfere di proprietà, comprimendo artificialmente le sfere di libertà (civili, politiche ed economiche), con l'effetto di precludere il conseguimento di molte delle opportunità aperte dalle nuove tecnologie, specie in termini di condivisione delle conoscenze e accesso al patrimonio comune immateriale.

Di conseguenza, questo contributo dovrà prendere in considerazione non soltanto il problema della trasparenza e non discriminatorietà degli algoritmi (par. 3), ma, prima ancora, la questione del regime di appartenenza delle informazioni processate in forma automatica e usate per fini di decisione (par. 2).

2. Il controllo sui dati nell'economia digitale

Quando si discorre di *big data analytics* si fa riferimento a due principali categorie di dati: *a*) i dati personali, ossia riferibili a un determinato individuo, identificato o identificabile; *b*) i dati non personali, ossia non riferibili a un determinato soggetto, per propria natura o perché sottoposti a un processo di anonimizzazione.

La gran parte dei processi decisionali automatizzati non sarebbe oggi pensabile prescindendo dall'accesso sistematico a entrambe le categorie di informazioni, sovente rese disponibili non direttamente dai *data subjects* o comunque dai *data sources,* bensì dagli intermediari professionali, i *data brokers,* i quali operano in un mercato ormai floridissimo, anche se poco conosciuto nei suoi dettagli organizzativi e regolamentato in maniera ancora frammentaria e lacunosa[6]. Quanto al rilievo di ciascuna tipologia di dati, si pensi, dal primo punto di vista, alle informazioni relative alla storia creditizia, alle propensioni di acquisto di un consumatore, oppure alle informazioni relative alla salute o alle preferenze politiche di un lavoratore: tutti dati utili ai fini della costruzione di un profilo individuale, e dunque spesso per fini di decisioni algoritmiche; e, dall'altro, alle informazioni prodotte dai macchinari intelligenti, come gli autoveicoli di ultima generazione (informazioni relative allo stato funzionale del veicolo, chilometri percorsi, anomalie rilevate, strade percorse, etc.), gli elettrodomestici intercon-

[6] In proposito v. l'indagine conoscitiva della Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability,* Washington, 2014.

nessi, oppure le informazioni prodotte dal settore pubblico (informazioni catastali, cartografiche, meteorologiche, etc.).

Diversi sono, ovviamente, i problemi sottesi all'utilizzo dell'una e dell'altra tipologia di informazioni, le quali mettono in gioco in maniera diversa la sfera della soggettività individuale. Differenti, di conseguenza, dovrebbero essere i regimi giuridici applicabili, sia pure nella consapevolezza dell'estrema fluidità dei confini e della presenza di continue sovrapposizioni tra le due categorie di dati.

La tendenza degli ordinamenti giuridici occidentali è quella di assoggettare a garanzie e salvaguardie soprattutto il segmento delle informazioni personali, anche se ciò avviene secondo forme e con modalità molto diverse. Gli ordinamenti europei hanno da più di vent'anni optato per un sistema incisivo di controllo sulla circolazione dei dati personali, ispirato alla logica dei diritti fondamentali e capace di assumere una incidenza significativa sul piano della circolazione globale dei modelli regolatori[7].

Nel prossimo paragrafo ci si interrogherà sui limiti posti alla raccolta e ulteriore trattamento dei dati personali per fini di profilazione e decisione algoritmica (par. 2.1.).

Nel paragrafo successivo si indagherà, invece, sul livello di tutela ascritto ai dati non personali, chiarendo in particolare se di essi possa predicarsi un regime d'appartenenza in forma esclusiva (par. 2.2.).

2.1. I dati personali

Il regime applicabile ai dati personali è ormai compiutamente delineato dal Regolamento UE n. 2016/679 (di seguito GDPR), al quale si aggiungerà a breve il Regolamento *e-privacy*, ancora in fase di negoziazione. Esso offre una risposta a molte delle questioni oggi sul tavolo, anche se permangono alcuni elementi d'ambiguità che potranno essere sciolti solo dalla prassi applicativa.

Quanto al profilo della raccolta dei dati, il diritto europeo muove, in termini generali, da una prospettiva opposta rispetto a quello americano. Mentre negli USA può ritenersi vigente un regime di libertà di trattamento dei dati personali, salve le specifiche ipotesi di divieto fissate a livello di leggi speciali[8], nel conte-

---

[7] G. Greenleaf, *The influence of European data privacy standards outside Europe: implications for globalization of Convention 108, Int'l Data Privacy Law,* 2 (2012), 68.

[8] In generale, v. P.M. Schwartz – K.N. Peifer, *Transatlantic Data Privacy Law,* 106 *Georgetown Law Journal* 115 (2017). Tra le molte conseguenze di questa diversità di approccio, può annoverarsi anche il ricorso a maglie larghe negli USA del *political microtargeting,* su cui v. C. Bennett, *Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?*, 6 International Data Privacy Law, no. 4 (2016).

sto europeo i dati personali non possono essere trattati se non in presenza di una specifica base autorizzativa rientrante tra quelle previste dall'art. 6 GDPR per i dati personali "comuni" e dall'art. 9 per le categorie particolari di dati (quelli che nella disciplina previgente si definivano "dati sensibili"). Tra le suddette cause di giustificazione rientra anche il consenso dell'interessato, che benché nell'economia degli artt. 6 e 9 svolga complessivamente un ruolo marginale, gode sempre di preponderante attenzione sia nella prassi applicativa sia nelle analisi scientifiche.

Il riferimento al consenso permette di sciogliere subito un equivoco che aleggia spesso nella letteratura in materia. Deve ribadirsi che la previsione circa la necessità del consenso non giustifica la conclusione che ciascun individuo debba ritenersi titolare di un diritto dominicale liberamente alienabile sui propri dati personali[9].

La finalità del GDPR non è quella di allocare titoli esclusivi alienabili e quindi porre le premesse per un efficiente mercato delle informazioni, bensì di bilanciare l'esigenza della circolazione intracomunitaria dei dati con il rispetto dei diritti fondamentali coinvolti (dignità, riservatezza, identità ed altre libertà civili: si noti che l'art. 8 della Carta dei Diritti UE configura il diritto alla protezione dei dati come autonomo diritto fondamentale della persona umana). Ciò si ricava dalle specifiche scelte normative compiute nel GDPR[10]: *a*) il consenso non è considerato sempre un requisito essenziale per il trattamento, anzi in molti casi esso non è necessario (per l'esecuzione di un contratto di cui è parte l'interessato, per il perseguimento del legittimo interesse di cui il titolare del trattamento è portatore, per compiti di interesse pubblico, etc.), sicché non può ritenersi vigente alcuna forma di tutela assoluta dei dati; *b*) requisito espresso di validità è la "libertà" della sua manifestazione (art. 4, n. 11, GDPR), e di questa può dubitarsi in presenza di particolari condizioni di disparità di potere sostanziale, come è il caso per molti rapporti *online* che riflettono condizioni di offerta oligopolistiche e si avvalgono della contrattazione standardizzata; *c*) anche qualora il consenso sia validamente inserito in un accordo contrattuale, rendendo la cessione delle informazioni personali un elemento del sinallagma (come presupposto dalla Proposta di direttiva

[9] C. Berger, *Property Rights to Personal Data? An Exploration of Commercial Data Law,* in *Zeitschrift* für *geistiges Eigentum,* 9, 2017, p. 340; S. Gutwirth – G. González Fuster, *L'éternel retour de la propriété des données: de l'insistance d'un mot d'ordre,* in Degrave-de Terwangne-Dusollier-Queck (a cura di), *Law, norms and freedoms in cyberspace – Liber amicorum* Yves *Poullet*, Bruxelles 2018, 117.

[10] Si veda in questo senso J. Drexl, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy,* in A. De Franceschi et al., *Digital Revolution: New Challenges for Law,* forthcoming, Beck, 2019 (on file with the author).

sulla fornitura di contenuti digitali)[11], esso è sempre revocabile (art. 7, c. 3, GDPR), a testimonianza dell'assenza di quei caratteri di stabilità delle posizioni negoziali, propri delle relazioni di mercato; *d)* infine esso non è di ostacolo all'esercizio del diritto alla portabilità (art. 20 GDPR), il quale testimonia l'esigenza di mantenere nelle mani della persona il potere di controllo sull'utilizzazione dei propri dati[12].

Una volta accertata la sussistenza dell'idonea base giuridica, il diritto europeo assoggetta il trattamento a importanti condizioni sostanziali e procedurali, le quali assumono un rilievo cruciale quando si sia in presenza di un'attività di "profilazione" dell'interessato[13]. Questa è definita dal GDPR come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"[14]. Si deve notare che un trattamento anche parzialmente automatizzato non esclude la sussistenza di un'attività di profilazione, contrariamente a quanto previsto dall'art. 22 GDPR in relazione alle decisioni interamente automatizzate, che soggiacciono al regime di divieto solo in quanto l'intervento umano sia del tutto escluso[15].

Quanto ai principi che disciplinano il trattamento, questo deve anzitutto essere condotto in maniera "trasparente". Ciò implica uno specifico onere informativo nei confronti dell'interessato (sia che i dati siano forniti da costui in maniera volontaria, sia che essi siano compulsati da altra fonte), precisato nei suoi lineamenti dagli artt. 12-14 GDPR. Si deve notare che, a tal riguardo, è espressamente previsto l'obbligo di comunicare informazioni circa "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par. 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato" (art. 13, lett. f, GDPR)[16].

---

[11] V. G. Resta – V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.,* 2018, 411 ss.

[12] V. R. Janal, *Data Portability – A Tale of Two Concepts,* in *JIPITEC,* 8, 2017, 59.

[13] Cfr. Art. 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* last revised February 2018, 6 e ss.

[14] In generale v. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* in Id., a cura di, *Intelligenza artificiale, protezione dei dati personali e regolazione,* Torino, 2018, 30 ss.

[15] *Ibid.,* 7.

[16] In tema M. Temme, *Algorithms and Transparency in View of The General Data Protection Regulation,* 3 *Eur. Data Prot. L. Rev.* 473 (2017), 482.

Si deve poi osservare il parametro della "correttezza", sicché anche un trattamento formalmente lecito potrebbe rivelarsi scorretto se ad esempio i dati sono impiegati in maniera tale da produrre effetti discriminatori, per precludere l'accesso a beni e servizi fondamentali, etc.

Inoltre, i dati in oggetto devono essere esatti ed accurati e in ogni caso devono rispettare la regola aurea della "minimizzazione": non è possibile, cioè, ricorrere a una massa sovrabbondante di dati, a meno che ciò non sia strettamente necessario rispetto alle finalità sottese al trattamento, né è ammissibile conservare tali dati per un lasso temporale sproporzionato (art. 5, n. 1, lett. e). Ciò si sposa, peraltro, con la regola per cui gli strumenti automatizzati di trattamento dei dati devono essere progettati sin da principio e devono operare in via predefinita in modo da ridurre al massimo la quantità di dati personali trattati e l'incidenza di tali operazioni sulla sfera della persona (*privacy by design* e *privacy by default*).

Infine, deve essere osservato il principio della finalità, sicché il trattamento validamente iniziato in relazione a un determinato scopo, come indicato nell'informativa resa al soggetto, non giustifica in linea di massima l'impiego dei dati per il conseguimento di scopi distinti, fatte salve le condizioni di compatibilità previste nell'art. 6, c. 4 GDPR. Un'applicazione importante di tale logica si rinviene nei limiti posti all'interconnessione degli archivi della p.a., la quale è subordinata a una specifica previsione di legge, ai sensi dell'art. 6, c. 1, lett. e) e art. 6, c. 3 GDPR[17].

Fra gli altri strumenti atti ad operare in chiave preventiva, qualora il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche, v'è la "valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali" (art. 35). Il titolare è tenuto ad adottare un siffatto documento qualora si intenda porre in essere "una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche".

Queste ed altre regole, che non è possibile qui analizzare nel dettaglio, delineano un meccanismo di controllo capillare, che restringe *ex ante* la quantità e la tipologia dei dati personali utilizzabili – entrando di fatto in conflitto con un altro segmento importante della legislazione comunitaria che, soprattutto in materia finanziaria e bancaria, incentiva il ricorso a forme di invasive di profilazione dei

[17] V. S. D'Ancona, *Trattamento e scambio di dati e documenti tra pubbliche amministrazioni, utilizzo delle nuove tecnologie e tutela della riservatezza tra diritto nazionale e diritto europeo, Riv. it. Dir. pubb. Com.,* 2018, 587 ss.

clienti al fine di valutarne la solvibilità e il merito di credito[18] – assicurando al contempo che questi abbiano un elevato grado di 'qualità', nel senso di accuratezza, esattezza e granularità[19]. A tal riguardo si prevede che i dati debbano essere esatti e se necessario aggiornati, non possano essere conservati per un periodo eccessivo di tempo, e in ogni caso sono suscettibili di accesso, controllo, rettifica, integrazione e persino cancellazione su istanza del soggetto interessato (artt. 13-21 GDPR).

Ciò significa, in estrema sintesi, che l'infrastruttura regolatoria si caratterizza per una serie di filtri atti a elevare la qualità dell'ecosistema informativo, selezionando *ex ante* tipologia, volume e caratteri delle informazioni utilizzabili per fini di profilazione, analisi a scopo predittivo e decisioni algoritmiche. Ciò rappresenta una circostanza non trascurabile, perché come è ben noto, gli algoritmi funzionano secondo la logica *garbage in – garbage out*, per cui dati incongrui, inesatti o non aggiornati non possono che produrre risultati decisionali inaffidabili[20]. D'altra parte, non si deve dimenticare che *non tutti* i dati immessi nel processo automatizzato sono dati personali in senso stretto.

2.2. I dati non personali

Le informazioni rilevanti per gli algoritmi di apprendimento automatico, come si è appena ricordato, non sono soltanto quelle atte ad identificare un individuo determinato. Tutte le informazioni prodotte da macchine, o i flussi inerenti le comunicazioni elettroniche, ad esempio, costituiscono, una porzione importante dell'universo *big data,* ma non rientrano necessariamente nel novero dei "dati personali", o perché strutturalmente non riferibili a una persona determinata, o perché oggetto di un processo di anonimizzazione (che preclude l'applicabilità della disciplina in materia di protezione dei dati personali)[21].

---

[18] V. ad es. il Considerando 27 e l'art. 8 della Direttiva 2008/48/CE, relativa ai contratti di credito ai consumatori, ove si prevede che "Member States shall ensure that, before the conclusion of the credit agreement, the *creditor assesses the consumer's creditworthiness on the basis of sufficient information*, where appropriate obtained from the consumer and, where necessary, *on the basis of a consultation of the relevant database*. Member States whose legislation requires creditors to assess the creditworthiness of consumers on the basis of a consultation of the relevant database may retain this requirement"; nonché il Consumer Financial Services Action Plan della Commissione del 2017. In tema v. l'indagine di V. Zeno-Zencovich, *'Smart Contracts', 'Granular Legal Norms', and Non-Discrimination,* di prossima pubblicazione.

[19] Per un panorama più dettagliato v. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* cit.

[20] M. Temme, *Algorithms and Transparency in View of The General Data Protection Regulation,* 3 *Eur. Data Prot. L. Rev.* 473 (2017), 478.

[21] Per un'analisi dettagliata v. C. Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy,* S. Lohsse – R. Schulze – D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools,* Oxford – Baden-Baden, 2017, 327 ss.

Il regime giuridico dei "dati non personali" – come definiti, in negativo, dal recente Regolamento 2018/1807/UE sulla libera circolazione dei dati non personali nell'Unione Europea[22] – è molto meno chiaro e univoco di quello relativo a dati personali[23]. In particolare, è quanto mai accesa la discussione se il dato, in quanto tale, possa costituire il termine di riferimento di una pretesa di natura proprietaria[24]. In questo senso, in particolare, sembrava essere orientata la Commissione con la Comunicazione al Parlamento Europeo e al Consiglio del 2017 su "Building a European Data Economy", nella quale si evocava l'introduzione di un nuovo "diritto del produttore di dati"[25].

Che si ponga la questione in questi termini non sorprende più di tanto, poiché accade di continuo che, di fronte all'emersione di nuovi beni patrimonialmente rilevanti, il primo schema al quale ci si rivolge per operare un inquadramento della realtà è quello del diritto di proprietà. È stato così per l'immagine, per l'etere, per l'energia, ed è così oggi per i dati non personali. Tuttavia, applicato all'informazione, lo schema proprietario si rivela fuorviante e non è in grado di apprestare soluzioni operazionali affidabili[26].

Difatti, essendo l'informazione un bene tipicamente non rivale nel consumo e suscettibile di produrre conoscenza incrementale, introdurre barriere artificiali alla sua circolazione tramite il riconoscimento di un diritto di esclusiva significa operare una forma di etero-regolazione, la quale può giustificarsi soltanto al fine di rimediare a un fallimento del mercato. Nelle ipotesi sottese ai diritti di proprietà intellettuale tradizionali, questo è rappresentato dal livello subottimale di produzione del bene*:* in assenza di un monopolio legale di sfruttamento, l'autore di una creazione estetica o utile non riuscirebbe a far propri gli utili derivanti dallo sfruttamento del bene (l'informazione è bene non escludibile, oltre che non rivale non consumo), sicché non avrebbe un incentivo sufficiente a investire e creare, con danno per l'intera collettività. Per contro, nel caso dei dati grezzi, privi cioè di un'immediata utilità estetica o industriale (quale quella sottesa al riconoscimento del diritto d'autore o del diritto di brevetto), non è la promessa

---

[22] Art. 3, Regolamento 2018/1807/UE.

[23] J. Drexl, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy,* cit.

[24] D. Zimmer, *Property Rights Regarding Data?,* in S. Lohsse – R. Schulze – D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, cit., 101 ss.; M. Becker, *Rights in Data – Industry 4.0 and the IP Rights of the Future,* in *Zeitschrift* für *geistiges Eigentum,* 9, 2017, p. 253.

[25] COM (2017) 9 final, p. 13.

[26] Sulla linea qui sostenuta v. J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access, JIPITEC,* 8 (2017), 257.

di un profitto monopolistico a costituire la molla principale per innescare il processo creativo ed innovativo, bensì lo sono fattori diversi come la concorrenza e il miglioramento dell'assetto tecnologico[27]. Non a caso, nella realtà attuale, che pur è connotata dall'assenza di diritti di privativa, le informazioni "grezze" vengono nondimeno prodotte in maniera intensiva e in diversi casi rappresentano la principale voce del capitale d'impresa.

In altri termini, le istituzioni giuridiche esistenti, e in primo luogo gli istituti del segreto industriale e della concorrenza sleale[28], unitamente al controllo di fatto sulle informazioni rilevanti[29], offrono strumenti di salvaguardia sufficienti per proteggere il parco informativo di un'impresa, senza che sia necessario ricorrere a misure controproducenti come quelle del riconoscimento di nuovi diritti di esclusiva[30]. Controproducenti, queste ultime, non soltanto perché rischiano di frenare il processo di sviluppo e innovazione, creando continui conflitti circa la titolarità della risorsa (si pensi alle informazioni circa le buche stradali rilevate dai sensori delle autovetture o da altri meccanismi di rilevazione) e elevando a sistema il potere di veto dei singoli detentori di segmenti di informazioni utili soprattutto in forma aggregata per fini di apprendimento automatico (problema degli *anti-commons*)[31]; ma anche perché tali pretesi diritti di esclusiva non potrebbero non riflettersi negativamente sulla libera circolazione dei dati, e dunque sulle garanzie della libertà d'informazione, particolarmente rilevanti oggi per il funzionamento dei processi democratici in un ambiente digitale.

In conclusione, qualsiasi tentativo di introdurre nuove forme di esclusiva concernenti dati non personali deve essere rigettato in quanto non giustificabile sul piano funzionale – come in parte si è rivelata essere la scelta di introdurre un diritto *sui generis* sulle banche di dati non creative – e foriero di conseguenze nocive sul piano dell'innovazione tecnologica e della trasparenza dei processi democratici.

---

[27] Per un panorama sulla prassi v. C. Wendehorst, *Besitz und Eigentum im Internet der Dinge,* in H. Micklitz – L.A. Reisch et al., a cura di, *Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt,* Baden-Baden, 2017, 367.

[28] T. Aplin, *Trading data in the digital economy: trade secrets perspective,* in S. Lohsse – R. Schulze – D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, cit., 59 ss.

[29] F. Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme,* in S. Lohsse – R. Schulze – D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, cit., 159 ss., 167.

[30] J. Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access,* cit., 260-261.

[31] Nel senso di M. Heller, *The Gridlock Economy. How Too Much Ownership Wrecks Markets, Stops Innovation, and Costs Lives,* New York, 2008.

3. Le decisioni algoritmiche e le prospettive dell'uguaglianza

Il ricorso a trattamenti algoritmici per finalità di previsione e/o di decisione è ormai all'ordine del giorno tanto nel settore pubblico quanto nel settore privato[32].

Si pensi, dal primo punto di vista, all'uso da parte della p.a. di strumenti algoritmici per decidere questioni seriali o fondate su parametri predeterminati (come l'assegnazione degli insegnanti alle sedi scolastiche vacanti)[33]; per operare valutazioni *data-driven* delle prestazioni dei dipendenti (come in un noto caso USA concernente la valutazione degli insegnanti)[34]; per orientare la prestazione dei servizi sociali (in Pennsylvania – ricorda un articolo apparso su Nature lo scorso anno – è stato messo in atto un sistema di profilazione e *scoring,* individuale, l'*Allegheny Family Screening Tool*, finalizzato ad individuare i bambini a rischio di esclusione sociale e maltrattamento e progettare gli interventi di tutela)[35]; per gestire i flussi migratori e effettuare uno *screening* preventivo dei *files* dei richiedenti asilo, visto di ingresso e soggiorno, etc.[36]; per orientare le azioni di contrasto al terrorismo, sfruttando le potenzialità delle analisi predittive ma non di rado ponendo le premesse per un immenso e capillare sistema di sorveglianza occulta degli individui (è quanto è emerso con le rivelazioni di Edward Snowden)[37]; per indirizzare le operazioni di polizia e prevenire la commissione dei reati (come nel caso dell'applicativo PredPol)[38]; per assumere decisioni concernenti l'amministrazione della giustizia penale (emblematico è l'esempio di COMPAS, il software utilizzato in diverse giurisdizioni USA al fine di calcolare il rischio di recidiva e la pericolosità sociale di un soggetto sottoposto a procedimento penale, e quindi misurare l'entità e la tipologia della sanzione irrogabile o modellare il meccanismo di esecuzione delle pene)[39].

Si pensi, dal secondo punto di vista, al trattamento algoritmico nell'ambito dei rapporti di lavoro (algoritmi computerizzati vengono di frequente utilizzati al fine di sollecitare selettivamente le domande d'impiego, per compiere le scelte in materia di assunzione, o per operare la valutazione delle prestazioni dei di-

---

[32] S.C. Olhede – P.J. Wolfe, *The growing ubiquity of algorithms in society: implications, impacts, and innovations, Phil. Trans. R. Soc. A* 376:20170364.

[33] V. TAR Lazio, 10-9-2018, n. 9227; TAR Lazio, 22-3-2017, n. 3769.

[34] *Houston Fed. Of Teachers v. Houston Ind. School District,* 251 F. Supp. 3d 1168 (2017).

[35] R. Courtland, *The Bias Detectives, Nature,* 558 (2018), 357.

[36] Per molti esempi v. M. HU, *Algorithmic Jim Crow,* 86 *Fordham L. Rev.* 633 (2017).

[37] M. Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, in 42 *Pepp. L. Rev.* 773 (2015).

[38] Per un'attenta analisi giuridica del problema del *predictive policing* v. T. Rademacher, *Predictive policing im deutschen Polizeirecht, Archiv des* öffent. *Rechts,* 142 (2017), 366 ss.

[39] R. Courtland, *The Bias Detectives,* cit., 358-359.

pendenti)[40]; alla vendita di beni e servizi (è da ciò che dipende l'applicazione di prezzi, e spesso anche condizioni d'offerta, differenziati nei rapporti *on line*)[41]; al mercato del credito (si pensi ai meccanismi di *credit scoring* al fine di valutare l'affidabilità finanziaria nel quadro delle procedure di finanziamento a singoli individui e ad imprese)[42]; alla comunicazione (dal *microtargeting* nella comunicazione politica, all'ordinamento delle notizie rese fruibili agli utenti da un *social network* quale *Facebook*)[43]; nonché ovviamente ai mercati finanziari (basti un rinvio al Regolamento 2017/589/UE in materia di *trading* algoritmico).

Il processo decisionale algoritmico, mette conto precisare, può essere interamente automatizzato, come nel caso dei filtri anti-*spam* che in maniera del tutto autonoma selezionano il tipo di messaggi da indirizzare nella casella della posta indesiderata, oppure può trattarsi di una delega soltanto parziale alla macchina, come nell'ipotesi in cui alla valutazione computerizzata dell'affidabilità finanziaria di un cliente faccia seguito una decisione umana definitiva circa la concessione di una linea di credito.

Come si può agevolmente intuire, l'automazione del processo decisionale permette, se ben congegnata, di conseguire notevoli vantaggi in termini di uniformità, affidabilità e controllabilità della decisione stessa. Essa appare dunque astrattamente in linea, non soltanto con le istanze di calcolabilità delle relazioni di mercato, ma anche con i valori di neutralità ed efficacia dell'azione amministrativa di cui all'art. 97 Cost.[44].

---

[40] P. Kim, *Data-driven Discrimination at Work,* 58 *William & Mary L. Rev.* 857 (2017); D.J. Dalenberg, *Preventing discrimination in the automated targeting of job advertisements,* 34 *Computer Law & Security Rev.* 615 (2108)*;* e B. Dzida – N. Groh, *Diskriminierung nach dem AGG beim Ansatz von Algorithmen im Bewerbungsverfabren, NJW,* 2018, 1917.

[41] Sul tema dei prezzi differenziati v. ad es. T. Tillmann – V. Vogt, *Personalisierte Preise im Big-Data-Zeitalter,* in *Verbraucher und Recht,* 2018, 447; sulla segmentazione degli utenti nel servizio Airbnb, v. C. Lutz – G. Newlands, *Consumer Segmentation Within the Sharing Economy: The Case of Airbnb,* 88 *Journ. Business Research* 187 (2018).

[42] D. Keats Citron – F. Pasquale, *The Scored Society: Due Process for Automated Predictions,* 89 *Washington Law Review* 1 (2014).

[43] In generale v. M. Ebers, *Beeinflussung und Manipolation von Kunden durch Behavioral Microtargeting. Verhaltenssteuerung durch Algorithmen aus der Sicht des Zivilrechts,* in *Multimedia und Recht,* 2018, 423; G. Boccia Artieri – A. Marinelli, *Introduzione: piattaforme, algoritmi, formati. Come sta evolvendo l'informazione online, Problemi dell'informazione,* 2018, 349 ss.

[44] In particolare, come si è autorevolmente notato, "i vantaggi di un'automazione dei processi decisionali amministrativi sono evidenti con riferimento a procedure seriali o standardizzate, caratterizzate da un alto tasso di vincolatezza o fondate su presunzioni, probabilisticamente significative di un certo fatto. Si pensi alle procedure di trasferimento contestuale o di prima assegnazione di sede agli insegnanti; e si pensi alla erogazione di contributi assistenziali agli aventi diritto sulla base

Per altro verso, però, la logica stessa delle tecniche di *big data analytics* porta con sé alcuni rischi, che devono essere attentamente considerati. Poiché la ricostruzione di tendenze predittivamente rilevanti avviene a partire dalle occorrenze empiriche esistenti, dalle quali le macchine ricavano *trend* utili ad orientare la valutazione di situazioni future, l'intero sistema ha la propensione a "codificare" il passato, ingabbiando soluzioni e predizioni all'interno delle griglie fornite dai trascorsi storici e dal set di valori che ha guidato la programmazione del sistema[45]. Ciò significa, in altri termini, che un determinato "stato del mondo" tende a essere cristallizzato nel processo prognostico, influenzandone i risultati ed orientando più o meno incisivamente le decisioni prese a valle della valutazione automatizzata.

Se questo può non apparire particolarmente problematico quando si prendano in esame accadimenti naturali, come l'andamento delle perturbazioni per fini di previsioni meteorologiche, ben diversa è la situazione qualora le tecniche predittive si appuntino su stati dell'uomo e su processi sociali[46]. Qui, infatti, uno dei pericoli più evidenti è che le condizioni di disparità sociale esistenti in un dato momento storico si riflettano sul giudizio prognostico tramite la costruzione di profili individuali o più spesso di gruppo, composti per inferenza da fattori come la propensione al consumo, la capacità di spesa, il luogo di residenza, i trascorsi familiari, il grado di istruzione, la storia giudiziaria, etc.[47] Se non adeguatamente monitorate e rese neutre rispetto ai rischi di *bias* già insiti nella selezione dei dati rilevanti, le decisioni algoritmiche che si basano su tali fattori sono atte a produrre effetti discriminatori e aggravare il peso delle disuguaglianze, invece che contribuire a ridurle, come pure la tecnologia potrebbe fare. Peraltro, come è ben noto, è lo stesso corretto funzionamento del processo deliberativo democratico a

---

di parametri predeterminati. Ma si pensi anche, quanto alle decisioni sfavorevoli, agli accertamenti fiscali fondati su base presuntiva i cui dati siano "messi insieme" da una macchina o alle sanzioni amministrative (per esempio per eccesso di velocità) elaborate in via automatizzata sia quanto alla rilevazione dell'infrazione sia per la determinazione della correlativa sanzione e la "formazione" stessa del provvedimento" (F. Patroni Griffi, La decisione robotica e il giudice amministrativo, accessibile all'indirizzo https://www.giustizia-amministrativa.it/documents/20142/147941/Patroni%20Griffi%20%20La%20decisione%20robotica%20e%20il%20giudice%20amministrativo%20-%2028%20agosto%202018.pdf/24218a2e-47b7-1c0a-b2eec1b670347f95/Patroni+Griffi+-+La+decisione+robotica+e+il+giudice+amministrativo+-+28+agosto+2018.pdf)

[45] Per una spiegazione puntuale e accessibile dei modelli matematici e statistici sottesi alle decisioni algoritmiche C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* London, 2017.

[46] D. Keats Citron – F. Pasquale, *The Scored Society: Due Process for Automated Predictions,* cit., 4 ss.

[47] S. Barocas – A.D. Selbst, *Big Data's Disparate Impact,* cit., 677 ss.

essere minacciato da una incontrollata proliferazione di ciò che Cathy O'Neil ha definito le "weapons of math destruction": la sollecitazione personalizzata resa possibile dalle moderne tecnologie della comunicazione tende a segmentare artificialmente (e condizionare la formazione) delle preferenze politiche, con tutti quegli effetti distorsivi sul piano dell'esercizio dei diritti democratici che da ultimo il caso *Cambridge Analytica* ha compiutamente illustrato[48]. È ovvio, poi, che qualora ci si muova in un contesto non democratico, le possibilità di accesso, aggregazione dei dati e profilazione, offerte dalle moderne tecnologie, sono tali da assicurare un controllo capillare sui comportamenti individuali, capace di reprimere qualsiasi forma di dissenso e segmentare i cittadini e le imprese in liste "rosse" e "nere" che evocano i peggiori incubi orwelliani. Che non si tratti di distopia, ma di preoccupante realtà, è dimostrato dal "social credit system" posto in atto dal governo cinese a partire dal 2014, con l'obiettivo di rafforzare la fiducia nelle istituzioni e nei mercati, e consistente nell'attribuzione di un punteggio individuale (e correlative penalizzazioni) in funzione del grado di aderenza a regole e norme sociali mostrato dai singoli nel corso della vita quotidiana[49].

Ma torniamo al tema iniziale dell'effetto discriminatorio, ricorrendo a due esempi in grado di chiarire meglio i termini del problema.

Il più noto è senza dubbio quello relativo all'uso di un algoritmo computerizzato, noto con l'acronimo COMPAS (C*orrectional Offender Management Profiling for Alternative Sanctions*), atto a quantificare il rischio di recidiva di soggetti sottoposti a procedimento penale. Prodotto da una società commerciale, esso è stato impiegato in molteplici giurisdizioni statunitensi per calcolare la probabilità di commissione di altri reati nell'arco dei due anni successivi, e quindi per decidere sia in merito al tipo e al quantum di pena da irrogare, sia alle modalità di esecuzione della medesima[50]. Diversi studi hanno sottoposto ad analisi il funzionamento del suddetto algoritmo, dimostrando la presenza di un pregiudizio sistematico a detrimento delle persone di colore. In particolare, un

---

[48] Cfr. F.J.Z. Borgesius et al, *Online Political Microtargeting: Promises and Threats for Democracy,* 14 *Utrecht L. Rev.* 82 (2018); B. Bodó – N. Helberger – C. de Vreese, *Political micro-targeting: a Manchurian candidate or just a dark horse?*, *Internet Policy Review*, *6* (2017). DOI: 10.14763/2017.4.776; W. Hoffmann-Riem, *Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht,* cit., 14-15.

[49] M. HU, *Small Data Surveillance v. Big Data Cybersurveillance*, in 42 *Pepp. L. Rev.* 773 (2015); e Y.J. Chen et al., *'Rule of Trust': The Power and Perils of China's Social Credit Megaproject,* 32 *Columbia J. Asian Law* 1 (2018).

[50] Di qui la controversia decisa dalla Supreme Court del Wisconsin nel caso *State v. Loomis,* 881 N.W.2d 749 (2016), nella quale è stata rigettata la richiesta di ritenere l'irrogazione di una pena basata sulle risultanze dell'applicativo COMPAS come confliggente con le garanzie del *due process*.

rapporto realizzato da Propublica dimostra che tra coloro i quali sono stati classificati ad alto rischio di azioni criminogene, che non hanno però nei due anni successivi compiuto atti illeciti, i bianchi sono in percentuale del 23,5%, mentre gli Afro-americani del 44,9%[51]. Per contro, in quelli classificati a basso rischio, che invece si sono resi effettivamente responsabili di atti criminali, i bianchi sono 47,7%, mentre gli afro-americani sono il 28%. È interessante capire a quali fattori sia imputabile un siffatto 'bias' discriminatorio. Un dato che emerge da diverse ricerche è che i punteggi elaborati da COMPAS sono la risultante delle risposte a 137 questioni, offerte direttamente dagli indagati o desunte da altri dati pubblici. L'origine etnica non potrebbe per legge rientrare tra le domande, ma rileva indirettamente, atteso che vengono presi in esame fattori spesso statisticamente correlati all'appartenenza "razziale", come il luogo di residenza, i precedenti penali (personali o familiari), il consumo di stupefacenti, il livello di istruzione, etc.

Il secondo esempio attiene ai rapporti di mercato. Esso concerne il *software* utilizzato da Amazon per individuare le città e i circondari dove offrire il servizio di consegna in un giorno. Un'indagine compiuta da Bloomberg nel 2016 ha fatto venire alla luce una chiara stratificazione per fasce di reddito e in genere capitale sociale[52]. Mentre tutte le principali città statunitensi risultano coperte, al loro interno vi sono "buchi" di copertura del servizio legati in maniera nient'affatto casuale con le aree più povere e degradate del territorio, come il Bronx a New York e Roxbury a Boston. Questo banalissimo esempio mostra come orientare i comportamenti futuri esclusivamente in base alle condizioni esistenti rischi di cristallizzare le disparità del presente, spingendo i più svantaggiati sempre più in basso nella piramide sociale.

Come già indicano questi semplici esempi, alla radice dell'effetto discriminatorio dell'algoritmo possono celarsi diversi fattori, dei quali il programmatore non sempre ha piena consapevolezza[53].

Innanzitutto, la scelta delle variabili o delle categorie in base alle quali è costruita la decisione algoritmica può tradursi in forme di discriminazione indiretta. Ad esempio, se nella programmazione di un algoritmo utilizzato per decisioni relative all'assunzione di personale si concretizza la nozione di 'buon' dipenden-

---

[51] J. Angwin – J. Larson – S. Mattu – L. Kirchner, *Machine Bias, ProPublica,* 23-5-2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[52] D. Ingold – S. Soper, *Amazon Doesn't Consider the Race of Its Customers. Should it?,* https://www.bloomberg.com/graphics/2016-amazon-same-day/.

[53] Quanto segue sintetizza l'analisi compiuta da Council of Europe, *Discrimination, artificial intelligence, and algorithmic decision-making,* a cura di F.Z. Borgesius, cit., 10-14; e da S. Barocas – A.D. Selbst, *Big Data's Disparate Impact,* cit..

te avendo riguardo – tra gli altri – al criterio della puntualità nel recarsi sul luogo di lavoro, ciò può finire per penalizzare sistematicamente tutti coloro che vivono in periferia ed impiegano di conseguenza maggior tempo per raggiungere ogni giorno la sede dell'impresa. E poiché in determinati contesti vivere in periferia si correla in misura prevalente con origini etniche, condizioni sociali e di reddito più disagiate, un siffatto criterio formalmente "neutro" potrebbe finire per riprodursi a danno di categorie già svantaggiate.

In secondo luogo, può risultare fallace il set di dati sui quali si esercitano i processi di auto-apprendimento delle macchine. In particolare, tali dati potrebbero essere relativi a un campione troppo ristretto o parziale, o riflettere essi stessi una situazione discriminatoria. Se, ad esempio, si calcolasse l'attitudine a delinquere esclusivamente sulla base delle statistiche relative alla popolazione carceraria negli USA, se ne trarrebbe un risultato viziato in partenza, poiché è noto che gli Afro-americani rappresentano una quota preponderante di tale popolazione.

In terzo luogo, può rivelarsi problematica la tipologia di dati presa in considerazione. Ad esempio, se le scelte in materia di occupazione fossero fatte automaticamente in base al *ranking* delle università di provenienza, ciò avrebbe verosimilmente come risultato quello di premiare le fasce più alte, per censo ed istruzione, della popolazione.

In quarto luogo, le *proxies* utilizzate potrebbero correlarsi a fattori indici di disparità sociale: si pensi soltanto al codice di avviamento postale utilizzato come strumento predittivo del rischio di *default* rispetto alla restituzione di un credito: si tratta anche qui di un criterio formalmente neutro, ma che in realtà fotografa – specie se unito ad altri dati – una ben precisa storia di vita della persona in questione.

Infine, l'algoritmo potrebbe essere stato programmato in maniera intenzionalmente discriminatoria, come nei casi riportati sulla stampa di pubblicità *on line* richieste a *social network* in modo da escludere persone di origine ispanica, o individui con un determinato orientamento sessuale.

3.1. Etica, governo e regolazione degli algoritmi

Queste brevi considerazioni inducono a sottolineare tre dati.

Il primo è che gli algoritmi possono apportare notevoli benefici non soltanto per la loro intrinseca attitudine alla razionalizzazione in senso weberiano del processo decisionale, con aumento dei livelli di rapidità ed efficienza rispetto ai costi, ma anche come strumenti di riduzione delle disuguaglianze tramite, ad esempio, l'allocazione mirata delle prestazioni sociali, il contrasto alle frodi o all'evasione fiscale, o più in generale lo stimolo ai processi partecipativi.

Il secondo è che perché i benefici attesi si traducano in effettiva prassi operativa e non siano sopravanzati dai rilevati effetti distorsivi, è necessario pre-formare le modalità di funzionamento degli algoritmi, assicurandone una sorta di *legality by design,* in modo da ridurre al minimo, e possibilmente eliminare, i rischi di impatto negativo sui diritti civili, sociali e politici delle persone[54]. Quando si parla di rischi specifici della decisione algoritmica, si fa soprattutto riferimento in letteratura a tre principali ordini di problemi:

a) la segretezza o l'inintelligibilità della logica sottesa al processo decisionale, la quale è particolarmente acuta nel caso degli algoritmi di apprendimento automatico (problema del *black box*)[55];
b) l'attitudine discriminatoria dell'algoritmo (problema del *bias*)[56];
c) la mortificazione della persona umana, resa oggetto di decisioni interamente automatizzate (problema della *dignità*)[57].

Il terzo dato è che per governare i problemi suindicati non è sufficiente affidarsi unicamente allo strumento tecnologico, quale ad esempio lo sviluppo di appositi algoritmi di auto-apprendimento volti a scovare e correggere l'esistenza di *bias* decisionali (c.d. *bias busting)* e a promuovere il valore della "correttezza" decisionale (*fairness formulas*)[58]; né a dichiarazioni d'impegno e codici di autoregolamentazione dei soggetti professionali coinvolti (come quelli prodotti dall'organizzazione *Fairness, Accountability, and Transparency in Machine Learning*, dalla *IEEE*, dal *Future of Life Institute*)[59].

Questi sono certamente strumenti utili e meritevoli di essere incoraggiati, ma che si muovono pur sempre in una logica di autodisciplina, la quale è per propria natura soggetta soltanto a quei vincoli che la cultura degli operatori e le prassi tecnologiche condivise in un dato momento storico possano suggerire[60]. Dato il rango costituzionale delle situazioni incise, è imprescindibile apprestare, prima ancora, un'adeguata infrastruttura istituzionale, composta di norme, rimedi

---

[54] Vedi D. Cardon, *Le pouvoir des algortihmes, Pouvoir,* 2018, 63 ss.

[55] J.A. Kroll, *The Fallacy of Inscrutability, Phil. Trans. R. Soc. A* 376:20180084; H. Shah, *Algoritmic Accountability, Phil. Trans. R. Soc. A,* 376:20170362 (2018); D. Pedreschi – F. Giannotti et al., *Open the Black Box. Data-driven Explanation of Black Box Decision Systems,* cit.

[56] A. Chander, *The Racist Algorithm?,* 115 *Michigan L. Rev.* 1023 (2017).

[57] Sachverständigenrat für Verbraucherfragen (SVRV), *Lösungsoptionen,* in H. Micklitz – L.A. Reisch et al., a cura di, *Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt,* Baden-Baden, 2017, 25; G. Noto La Diega, *Against the De-Humanisation of Decision-Making,* 1 *JIPITEC* 3 (2018).

[58] In tema v. D.R. Desai – J.A. Kroll, *Trust But Verify: A Guide to Algorithms And the Law,* 31 *Harvard J. Law & Tech.* 1 (2018), 35 ss. Per molti utili esempi sul punto v. AI NOw, 24 ss.

[59] Per un utile panorama sulle principali iniziative di auto-disciplina v. Council of Europe, *Discrimination, artificial intelligence, and algorithmic decision-making,* a cura di F.Z. Borgesius, cit., 27.

[60] Sachverständingenrat für Verbraucherfragen (SVRV), *Lösungsoptionen,*cit., 26, 36.

e procedure adeguati agli interessi in gioco e in grado di assicurare un capillare controllo sociale sull'uso dell'algoritmo. Si tratta cioè di arricchire un modello di *digital ethics* con un più penetrante sistema di *digital regulation*[61].

La consapevolezza dei tre profili indicati ha ispirato la formazione di prassi innovative, l'adozione di codici di auto-regolamentazione e la formulazione di indirizzi di *policy* particolarmente impegnativi. Basti citare, dal primo punto di vista, le iniziative della *Algorithmic Justice League* e dell'*AI Now Institute*, che al pari di numerose altre organizzazioni non governative, sono impegnate nel disvelare e contrastare attraverso azioni giudiziarie i fenomeni di uso discriminatorio dell'algoritmo. O si pensi alla campagna "OpenSchufa" recentemente promossa in Germania dalla *Open Knowledge Foundation* e da *AlgorithmWatch* al fine di ottenere l'ostensione del codice sorgente, o comunque la comunicazione dei dettagli operativi, dell'algoritmo utilizzato dalla potentissima società *Schufa* (Schutzgemeinschaft für allgemeine Kreditsicherung), la quale raccoglie dati relativi alla solvibilità finanziaria di 67 milioni di persone e 5 milioni di imprese tedesche e le cui valutazioni negative possono determinare l'impossibilità di accedere al credito, stipulare un contratto di locazione, etc.[62] Dal secondo punto di vista, mette conto ricordare la *Sharing Cities Declaration* adottata a Barcellona nel 2018 e finalizzata a delineare un quadro impegnativo per assicurare condizioni di vita, produzione e sussistenza urbane che siano inclusive, aperte e sostenibili[63]. In essa trovano specifica emersione alcuni dei temi sin qui evocati, come la differenziazione delle piattaforme in collaborative e non collaborative in base, tra l'altro, al grado di inclusione sociale promosso nell'offrire servizi a condizioni identiche a differenti segmenti della popolazione e senza indulgere in discriminazioni (Principio # 1); il principio del contrasto al pregiudizio e alla discriminazione attraverso la predisposizione di condizioni eque e giuste di accesso all'occupazione per persone di qualsivoglia provenienza sociale (Principio # 4); la più ampia garanzia dei diritti digitali, specificamente inclusiva del diritto alla *accountability* algoritmica e alla portabilità dei dati personali (Principio #4).

3.2. I modelli di disciplina emergenti: l'approccio europeo

Oltre alle prassi e alle dichiarazioni, che richiederebbero anche uno specifico panorama sull'ampio universo del *soft la*w, non può prescindersi – come si no-

---

[61] Per un'utile tassonomia dei 3 principali modelli di governo della tecnologia, *digital ethics, digital governance* e *digital regulation*, v. L. Floridi, *Soft ethics, the governance of the digital, and the General Data Protection Regulation, Phil. Trans. R. Soc. A* 376:20180081.

[62] E. Erdmann, *Schufa, öffne dich, Zeitonline,* 17-3-2018.

[63] http://www.share.barcelona/declaration/.

tava pocanzi – dal ruolo del diritto in senso formale, quale strumento di mediazione tra le varie istanze sociali emergenti e soprattutto quale tecnica di controllo democratico dei nuovi poteri tecnologici[64].

Il ricorso al diritto in questo campo non è privo di problemi, né si sottrae alle obiezioni di chi abbia il timore di ingessare l'impetuoso sviluppo tecnologico attraverso regole troppo rigide e esposte a rapida obsolescenza. Non a caso esso è osteggiato negli ambienti culturali che ripongono una maggior fiducia nelle virtù di autoregolazione dei mercati, mentre esso è maggiormente incoraggiato nei contesti a più alta propensione regolatoria. Tra questi spicca lo spazio giuridico europeo. È qui che hanno trovato emersione i primi e più compiuti esempi di governo giuridico della decisione algoritmica. Se ne analizzeranno nel prosieguo due, il primo tratto dal diritto dell'Unione Europea e il secondo dall'esperienza francese.

Il primo esempio è costituito dal Regolamento generale per la protezione dei dati personali (GDPR). Esso contiene una disciplina piuttosto avanzata delle salvaguardie da adottare in caso di decisione automatizzata che coinvolga dati personali, la quale si colloca in un'immediata linea di continuità con la previgente direttiva 95/46/CE. Al tema in oggetto sono dedicati – a tacer d'altro – il Considerando n. 71, e due articoli: il 15 e il 22.

L'art. 15 configura una prima, fondamentale, garanzia di fronte a un processo decisionale automatizzato, compresa la profilazione (ai sensi dell'art. 22), che si avvalga di dati personali: il diritto di sapere. La norma, in particolare, stabilisce il diritto di ottenere informazioni circa *"la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*".

Per contro l'art. 22 fissa un limite sostanziale all'uso del trattamento algoritmico. Esso stabilisce che "l'interessato ha il *diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato*, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Si tratta di un vero e proprio divieto[65], sia pur corredato da una serie di eccezioni delle quali si farà ora cenno, alla cui violazione conseguono effetti preclusivi per il titolare del trattamento. Sottese a tale proibizione sono diverse esigenze, tra cui quella di proteggere

---

[64] Sachverständigenrat für Verbraucherfragen (SVRV), *Lösungsoptionen,* cit., 25 ss.; V. Boehme-Nessler, *Die Macht des Algorithmen und die Ohnmacht des Rechts, NJW,* 2017, 3031.

[65] Art. 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* last revised February 2018, 19-20; P. Voigt – A. Von Dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide,* Cham, 2017, 180.

la dignità umana, evitando che la persona sia resa oggetto passivo di decisioni assunte in forma de-umanizzata, e di assicurare la trasparenza e la controllabilità della decisione stessa.

Tale divieto non opera qualora la decisione: *a*) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento[66]; *b*) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; *c*) si basi sul consenso esplicito dell'interessato.

Nel caso della conclusione del contratto e del consenso esplicito, il Regolamento obbliga il titolare del trattamento ad attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Tra queste assumono particolare rilievo il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Inoltre viene fissato un limite sostanziale invalicabile, costituito dal principio per cui le decisioni algoritmiche autorizzate non possono avvalersi dei dati particolari di cui all'art. 9 (cioè i dati sulla salute, sull'orientamento sessuale, sulle opzioni ideologiche e sindacali, sulle appartenenze etniche, etc.), a meno che non sussistano le scriminanti previste dall'art. 9, par. 2, lett. *a*) (consenso esplicito della persona) o *g*) (trattamento necessario per motivi di interesse pubblico rilevante) e che non siano state adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Tali norme riflettono il lodevole sforzo di elaborare una disciplina che sia trasversale al settore pubblico e al settore privato, trovando applicazione in entrambi ogniqualvolta si sia in presenza di una decisione automatizzata presa a partire da dati personali. Esse soffrono di alcuni limiti intrinseci e di qualche elemento di ambiguità.

Iniziamo da questi ultimi.

Per quanto concerne l'art. 15, esso ha senza dubbio un'importanza non trascurabile quale strumento capace di rispondere almeno in parte all'esigenza indicato in precedenza come problema della "trasparenza" dell'algoritmo[67]. Se non già a livello "proattivo" (stimolando indirettamente la leggibilità dell'algoritmo in

---

[66] Ad esempio, alcuni studi legali hanno iniziato a far uso di tecniche predittive automatizzate al fine di decidere se accettare il patrocinio nel campo dell'infortunistica (J. Croft, *Legal firms unleash office automatons, Financial Times,* 16 maggio 2016).

[67] M. Temme, *Algorithms and Transparency in View of The General Data Protection Regulation,* 3 *Eur. Data Prot. L. Rev.* 473 (2017), 481.

fase di programmazione)[68], quanto meno a livello "reattivo" esso testimonia della necessità di dotarsi di una chiave di accesso e possibilmente di comprensione della logica funzionale dell'algoritmo, come chiaramente indicato in ambito amministrativo dalla prima decisione del TAR Lazio, che ha riconosciuto il diritto per il privato cittadino di accedere al codice sorgente del software relativo all'algoritmo usato dalla p.a. per gestire le procedure di assegnazione degli insegnanti nelle sedi vacanti[69].

Si discute, tuttavia, se il diritto ad ottenere informazioni di cui all'art. 15 si appunti sulle generali caratteristiche del modello e la logica utilizzata dal *software,* o attenga invece più specificamente al rapporto tra tale logica e i risultati per la sfera del singolo individuo della decisione adottata[70]. Si tratta cioè di un modello di controllo generale circa le conseguenze attese del trattamento, oppure di un canone conoscitivo volto a comprendere *il modo in cui la decisione è stata presa in relazione alla specifica situazione soggettiva e fattuale dell'interessato*?

Se si opta per questa seconda, più estensiva, interpretazione, vi sono due ostacoli da tener presenti. Il primo consiste nel fatto che l'applicabilità della disciplina è condizionata alla circostanza che, usati per fini di decisione, siano *dati personali*, sicché i dati non personali (si pensi ancora ai dati forniti da un'autovettura intelligente) o i dati in forma anonima (molte delle inferenze a carattere predittivo sono basate su dati anonimi, come la residenza di certi gruppi sociali in determinate aree di territorio) ne sono esclusi[71]. Il secondo è rappresentato dal considerando 63, il quale – come la legge francese che verrà di seguito discussa – fa espressamente salve le prerogative della proprietà intellettuale. Ciò significa che se l'algoritmo computerizzato sottende un *software* protetto dal diritto d'autore, o siano coinvolti segreti commerciali la richiesta di accesso potrebbe infrangersi di fronte a un siffatto scoglio e essere neutralizzata dai privilegi dominicali cristallizzati nell'ultima generazione delle regole in materia di IP[72]. Quanto ciò sia importante è dimostrato da alcune controversie statunitensi in materia di voto elettronico, là dove la richiesta di ostensione del codice operativo del *software* è stata rigettata in nome del principio dei *trade*

---

[68] G. Malgieri – G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data-Protection Regulation,* 7 *Int'l Data Privacy Law* 243 (2017).

[69] Tar Lazio, 22-3-2017, n. 3769; 21-3-2017, n. 3742, in *Foro amm.,* .

[70] L. Edwards – M. Veale, *Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?, IEEE Security & Privacy* (2018) 16(3), 46–54.

[71] Tar Lazio, 22-3-2017, n. 3769.

[72] Su questo problema v. M. Temme, *Algorithms and Transparency in View of The General Data Protection Regulation,* cit., 484.

secrets[73]. Ovviamente, qualora si tratti di un algoritmo computerizzato realizzato su commissione per conto di una pubblica amministrazione, potrebbe invocarsi il disposto dell'art. 11, primo comma, della legge sul diritto d'autore, sostenendo l'intervenuto acquisto a titolo originario del monopolio di sfruttamento in capo all'ente committente; per poi desumerne l'inopponibilità al privato dell'argomento tratto dalla tutela della proprietà intellettuale[74]. Il problema, però, rimane quanto meno per il settore privato e per i trattamenti algoritmici condotti dalla p.a. sulla base di rapporti contrattuali con effetti obbligatori e non traslativi della titolarità; sarebbe auspicabile, a tal proposito, optare per un'interpretazione restrittiva della clausola di salvaguardia dei diritti di proprietà intellettuale e affermare la prevalenza del diritto d'accesso dell'interessato, in linea peraltro con quanto espresso nei Considerando 34 e 35 della Direttiva 2016/943/UE sulla protezione dei segreti commerciali[75].

Quanto invece all'art. 22, difficoltà derivano:

a) dall'essere il diritto in oggetto limitato all'ipotesi in cui il processo decisionale sia *integralmente* basato sul trattamento automatizzato, il che avviene in un numero limitato di casi, posto che in particolare per le decisioni che interessano il settore pubblico è generalmente previsto un intervento umano (il quale però è spesso fortemente condizionato da una previa valutazione automatizzata della fattispecie);
b) dalla ristrettezza della nozione di "decisione", la quale implica, a tacer d'altro, l'esclusione dall'ambito applicativo della norma di tutte le forme – per quanto invasive – di *microtargeting*[76]. Che si tratti di questioni rilevanti è testimoniato non solo dal problema oggi cruciale del *data-driven political microtargeting*[77], ma anche dai casi di sollecitazione pubblicitaria discriminatoria, come quello in cui si inviavano pubblicità di servizi di assistenza legale in ambito penale soltanto ai soggetti con cognomi che rivelassero l'origine afro-americana della persona[78].

---

[73] D. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure,* 59 *Fla. L. Rev.* 135 (2007)*;* v. anche AI NOw, 11.

[74] In questa linea v. Tar Lazio, 22-3-2017, n. 3769, che attribuisce valore assorbente ai principi della trasparenza del procedimento amministrativo, configurando l'algoritmo come un documento amministrativo.

[75] G. Malgieri, *Trade Secrets v. Personal Data: a possible solution for balancing rights,* 6 *Int'l Data Privacy L.* 102 (2016); G. Malgieri – G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data-Protection Regulation,* cit., 262-264.

[76] Martini, sub §22, in B. Paal – D. Pauly, *Datenschutz-Grundverordnung,* München, 2017, Rn. 23.

[77] F.J.Z. Borgesius et al, *Online Political Microtargeting: Promises and Threats for Democracy,* 14 *Utrecht L. Rev.* 82 (2018).

[78] L. Sweeney, *Discrimination in Online Ad Delivery,* 11 *Queue* 10 (2013).

c) Dal requisito dell'"effetto giuridico" come conseguenza di una decisione automatizzata. Si tratta di una limitazione alquanto rilevante dell'ambito applicativo della norma, che copre essenzialmente i casi di decisioni suscettibili di incidere situazioni giuridiche soggettive. Vi rientrano certamente le ipotesi di atti amministrativi particolareggiati, il rifiuto di una domanda di credito presentata online o scelte in materia di assunzione operate in via elettronica (cfr. Cons. 71), ma altre importanti fattispecie ne risulterebbero escluse. Si è già citato il caso del *microtargeting*, che non produce tecnicamente effetti giuridici, ma è atto a condizionare comportamenti sia di mercato sia extra-mercato, come nel caso delle *fake news* indirizzate in maniera mirata a classi di soggetti. L'interrogativo che va sollevato in relazione a tale modello regolamentare è il seguente: ha senso limitare l'impatto rilevante di cui si discorre nella norma alla posizione del singolo individuo, quando invece è la somma delle micro-violazioni individuali a produrre un effetto lesivo o discriminatorio per l'intero gruppo di riferimento?

Il quesito appena sollevato disvela il primo dei limiti intrinseci dell'approccio regolatorio delineato dal GDPR, consistente nella prevalente logica individualistica attraverso la quale ci si accosta a un tema di rilevanza decisamente meta-individuale e collettiva, quale è quello delle decisioni algoritmiche[79]. Non è detto, infatti, che l'assenza di lesione individualmente rilevante ai sensi della normativa sulla protezione dei dati privi la fattispecie dei caratteri di disvalore, poiché ad esempio il suddetto trattamento potrebbe produrre effetti pregiudizievoli o discriminatori per lo specifico gruppo al quale il cittadino appartenga.

Tale considerazione induce da un lato a ricordare che la normativa sulla tutela dei dati deve essere intesa come un tassello, certo al momento il più avanzato, di un più ampio mosaico regolatorio, al quale dovranno contribuire gli altri segmenti dell'ordinamento, e in primo luogo il diritto antidiscriminatorio (come delineato a partito dalle direttive 2000/43 CE, sull'uguaglianza razziale, 2000/78/CE sulla parità di trattamento in materia di lavoro, 2006/54/CE sull'uguaglianza di genere)[80], il diritto dei consumatori, il diritto amministrativo e il diritto del lavoro[81]. Dall'altro essa spinge ad affermare che anche gli strumenti di tutela, finalizzati ad assicurare

[79] L Edwards – M. Veale, *Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?,* cit.

[80] Per una specifica applicazione del diritto antidiscriminatorio al caso dei *selective advertisements* in materia di lavoro, v. D.J. Dalenberg, *Preventing discrimination in the automated targeting of job advertisements,* 34 *Computer Law & Security Rev.* 615 (2108).

[81] In quest'ottica v. A. Mantelero, *AI and Big Data: A Blueprint for a human rights, social and ethical impact assessment, Computer Law & Security Rev.* 34 (2018), 754.

un controllo esterno sulle decisioni algoritmiche, dovrebbero essere improntati ad una logica di azione *collettiva* piuttosto che individuale. È vero che il primo comma dell'art. 80 GDPR prevede la possibilità di conferire mandato ad enti del terzo settore, ma il secondo comma rimette agli stati membri la scelta discrezionale se adottare il modello dell'*opt out,* ossia dell'azione promossa direttamente dagli enti non profit, salvo il diritto di opporsi da parte del singolo[82]. Tale forma di azione collettiva sembrerebbe l'unica in grado di apprestare una tutela efficace, assieme ovviamente all'iniziativa delle autorità amministrative indipendenti competenti nel settore, che però scontano in molti casi un ritardo di mezzi e organizzazione tecnologica.

Inoltre andrebbe incoraggiato il ricorso a tecniche di controllo *ex-ante* che contribuiscano ad orientare le modalità di impiego dell'algoritmo[83]. Il GDPR contiene a tal proposito indicazioni importanti, che potrebbero essere valorizzate nella prassi al fine di inglobare nel sistema normativo in oggetto l'ulteriore istanza di tutela contro gli effetti discriminatori dell'algoritmo. Tra queste meritano di essere ricordate la progettazione preventiva delle macchine in maniera 'privacy-enhancing' (art. 25); la valutazione di impatto da redigere qualora il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35); le certificazioni adottate ai sensi dell'art. 42. Di questa attitudine espansiva della disciplina in materia di protezione dei dati v'è una traccia precisa nello stesso GDPR, il cui Considerando 71 recita al secondo comma:

"Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato *e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o delle origini etniche, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportino misure aventi tali effetti".*

---

[82] In tema v. F. Casarosa, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi?,* in A. Mantelero – D. Poletti, a cura di, *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali,* Pisa, 2018, 235 ss.

[83] L Edwards – M. Veale, *Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?,* cit.

3.3. Algoritmi e decisioni amministrative: la riforma francese

Le regole contenute nel GDPR hanno il pregio di guardare trasversalmente al fenomeno del trattamento automatizzato dei dati personali, al fine di prefissare garanzie minime per i diritti della persona le quali siano applicabili sia ai trattamenti nel settore pubblico sia nel settore privato. L'attitudine onnicomprensiva della normativa in oggetto ne costituisce però anche un limite, in quanto il ricorso all'algoritmo nel settore pubblico, ed in particolare nell'ambito delle procedure preordinate all'emanazione di un provvedimento amministrativo (senza poi considerare le ipotesi, delle quali oggi si discute molto, di "giustizia predittiva")[84], ha indubbie particolarità di ordine funzionale e strutturale, che richiedono una disciplina più specifica e puntuale rispetto a quella del settore privato (il quale pure richiederebbe di essere disarticolato in più microsettori, come il credito, la sanità, il lavoro, etc.)[85]. Si comprende, quindi, che negli ordinamenti europei per tradizione più sensibili all'interazione tra tecnologie e diritti, come la Francia, il recepimento del GDPR abbia offerto il destro per introdurre, oltre a norme di dettaglio sulle decisioni automatizzate contemplate dal Regolamento, apposite regole sui provvedimenti amministrativi algoritmici.

La legge n. 2018-493 del 20 giugno 2018 ha modificato l'art. 10 della celebre legge *Informatique et libertés* del 1978, prefissando i seguenti principi:

a) nessuna decisione giudiziaria che implichi la valutazione del comportamento di una persona può fondarsi su un trattamento automatizzato di dati personali preordinato a giudicare aspetti della personalità di tale persona [se ne desume che un sistema del tipo COMPAS non potrebbe trovare accoglimento nell'ordinamento francese];
b) nessuna decisione che produca effetti giuridici su una persona e basata sul trattamento automatizzato dei dati può essere assunta al di fuori delle condizioni stabilite dall'art. 22 del GDPR;
c) provvedimenti amministrativi individualizzati che si basino su un trattamento automatizzato sono ammissibili, purché rispettino le condizioni previste dal *Code des relations entre le public et l'administration* e purché il trattamento non coinvolga categorie particolari di dati (dati sulla salute, sulle preferenze politiche, dati sulla configurazione genetica, etc.).

---

[84] P.Y. Gaudemet, *La justice à l'heure des algorithmes, Rev. Dr. Pub.,* 2018, 651; M. Luciani, *La decisione giudiziaria robotica, Rivista AIC,* n. 3/2018, 872 ss.

[85] H. Pauliat, *La décision administrative et les algorithmes: une loyauté à consacrer, Rev. Dr. Pub.,* 2018, 641 ss.

d) tali provvedimenti devono contenere espressa menzione del trattamento automatizzato; relativamente ad essi, il responsabile del trattamento deve assicurare la piena comprensione del trattamento algoritmico e delle sue evoluzioni affinché possa spiegare alla persona interessata, nel dettaglio e in una forma intellegibile, il modo in cui il trattamento sia stato posto in opera nei suoi confronti.

Se questa disciplina è contenuta nella legge di recepimento del GDPR, già la legge sulla *République Numérique* e un successivo decreto attuativo avevano prefissato le condizioni di ammissibilità dei provvedimenti amministrativi algoritmici[86].

L'art. L 311-3-1 prevede che "una decisione individuale presa sul fondamento di un trattamento algoritmico comporta una menzione esplicita e l'informazione all'interessato. Le regole che definiscono tale trattamento, come pure le principali caratteristiche della sua messa in opera sono comunicate dall'amministrazione all'interessato che ne faccia domanda".

La norma in esame rinviava a un decreto attuativo per la definizione delle specifiche applicative.

Tale decreto, approvato il 14 marzo 2017, ha stabilito, all'art. R 311-3-1-1, che "la menzione esplicita prevista dall'art. L. 311-3-1 indica la finalità perseguita attraverso il trattamento algoritmico. Essa richiama il diritto, garantito dal suddetto articolo, di ottenere la comunicazione delle regole che definiscono tale trattamento e delle principali caratteristiche della sua messa in atto, nonché delle modalità di esercizio di tale diritto alla comunicazione e di ricorso, ove ne sussistano le condizioni, alla commissione di accesso ai documenti amministrativi, come definita dal presente libro". La norma successiva, l'art. R 311-3-1-2, dà specifica concretezza al diritto dell'interessato di essere informato circa il modo in cui la logica generale dell'algoritmo è stata applicata alla sua condizione particolare, comprendendo così il modo e le forme in cui essa ha inciso sui risultati della decisione. "L'amministrazione comunica alla persona destinataria di un provvedimento preso sul fondamento di un trattamento algoritmico, su istanza di parte, in forma intellegibile e a condizione di non violare segreti protetti dalla legge, le seguenti informazioni:

– il grado e il *modo in cui il trattamento algoritmico ha contribuito* alla decisione;
– i *dati trattati* e la loro origine;
– i parametri del trattamento e, se del caso, la loro ponderazione, *applicati alla situazione dell'interessato;*
– le operazioni effettuate attraverso il trattamento".

[86] J.B. Duclercq, *Le droit public à l'ère des algorithmes, Rev. Dr. Pub.,* 2017, 1401 ss.

Si tratta di principi particolarmente innovativi e rilevanti, poiché da un lato prefissano una serie di garanzie procedurali e sostanziali (prima tra tutte l'impossibilità di far uso di dati sensibili nel trattamento algoritmico) che elevano la tutela della persona-cittadino rispetto alle decisioni automatizzate, ma dall'altro ammettono espressamente la validità di un provvedimento amministrativo, che incida sulla situazione soggettiva del singolo, assunto sulla base di un trattamento automatizzato di dati. Si comprende, quindi, che tale disciplina abbia sollevato anche obiezioni da parte di chi ravvisi, nella parziale delocalizzazione dello spazio deliberativo agli algoritmi computerizzati, un *vulnus* ai principi che governano il procedimento amministrativo[87].

Anche nel nostro ordinamento, peraltro, il problema era già emerso ed aveva trovato una prima valutazione giudiziaria da parte del TAR Lazio, che con pronunzia 10 settembre 2018, ha annullato i provvedimenti del Ministero dell'Istruzione conclusivi delle procedure di mobilità straordinaria degli insegnanti, in quanto assunti invece che con ordinaria istruttoria procedimentale, con valutazione demandata ad apposito algoritmo[88]. Ha osservato il collegio, in particolare, che "gli istituti di partecipazione, di trasparenza e di accesso, in sintesi di relazione del privato con i pubblici poteri non possono essere legittimamente mortificate e compresse soppiantando l'attività umana con quella impersonale, che poi non è attività, ossia prodotto delle azioni dell'uomo, che può essere svolta in applicazione di regole o procedure informatiche o matematiche. Ad essere inoltre vulnerato non è solo il canone di trasparenza e di partecipazione procedimentale, ma anche l'obbligo di motivazione delle decisioni amministrative, con il risultato di una frustrazione anche delle correlate garanzie processuali che declinano sul versante del diritto di azione e difesa in giudizio di cui all'art. 24 Cost., diritto che risulta compromesso tutte le volte in cui l'assenza della motivazione non permette inizialmente all'interessato e successivamente, su impulso di questi, al Giudice, di percepire l'iter logico-giuridico seguito dall'amministrazione per giungere ad un determinato approdo provvedimentale". Si tratta probabilmente, di un approccio eccessivamente rigido, che portato alle estreme conseguenze finirebbe per precludere l'utilizzo di algoritmi di apprendimento automatico nell'ambito dell'azione amministrativa.

---

[87] In generale v. il panorama offerto da H. Pauliat, *La décision administrative et les algorithmes: une loyauté à consacrer,* cit.

[88] Tar Lazio, 10-9-2018, n. 9227. In tema v. L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte,* in *Foro amm.,* 2018, 9, 1598 ss.; P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.,* in *www.federalismi.it,* 2018, 2, 15.

Che ciò non sia un esito desiderabile, né necessitato sul piano dell'assetto giuridico vigente, è dimostrato da una recente pronunzia del *Conseil Constitutionnel* francese. La Corte nel 2018 è stata chiamata a giudicare della costituzionalità della norma interna di adeguamento al GDPR, precedentemente discussa[89]. Tra i vari profili di illegittimità denunziati, vi era anche quello del contrasto con i principi di legittimità dell'azione amministrativa, derivanti dall'ammissione delle decisioni individualizzate assunte in base a trattamento algoritmico; in particolare, i ricorrenti sostenevano che il ricorso ad algoritmi privasse l'amministrazione nel necessario di potere di apprezzamento delle situazioni individuali, e che in particolare gli algoritmi di apprendimento automatico, implicando una continua revisione delle regole di funzionamento dell'algoritmo stesso, precludesse alla stessa amministrazione la facoltà di comprendere la logica motivazionale sottesa alla decisione. La Corte ha rigettato tutte le censure, avanzando i seguenti argomenti[90]:

a) non vi è una delega del potere regolamentare allo strumento tecnologico, per ciò che i criteri e le modalità di funzionamento dell'algoritmo sono stabiliti ex ante e validati dal responsabile del procedimento;
b) il ricorso al trattamento algoritmico è subordinato alle specifiche condizioni e garanzie previste dal suddetto decreto del 2017;
c) contro il provvedimento individuale assunto sulla base di trattamento algoritmico è comunque sempre concesso ricorso amministrativo, che richiede una decisione evidentemente non basata soltanto sull'algoritmo, e se ne ricorrono le condizioni, ricorso al giudice;
d) il responsabile del trattamento deve essere sempre in grado di comprendere il funzionamento del trattamento algoritmico e le sue evoluzioni, in modo da poter spiegare alla persona interessata, nel dettaglio e in una forma intellegibile, il modo in cui il trattamento è stato posso in essere nei suoi riguardi;
e) per quanto detto, devono ritenersi preclusi all'amministrazione quegli algoritmi di apprendimento automatico il cui funzionamento sfugge alla comprensione del responsabile del procedimento, ma non tutti gli algoritmi che possano semplificare e rendere più precisa e neutrale l'azione amministrativa.

---

[89] Cons. const., déc. 12-6-2018, n. 2018-765.

[90] Per alcune considerazioni in merito alla pronunzia v. E. Rulli, *Giustizia predittiva, intelligenza artificiale e modelli probabilistici. Chi ha paura degli algoritmi?,* in *Analisi giuridica dell'economia,* 2, 2018, 533 ss., 540 ss.

4. Gli algoritmi come opportunità e la politica (del diritto)

Le ultime norme citate suggeriscono quale dovrebbe essere, ad avviso di chi scrive, l'approccio tecnicamente corretto al tema dei *big data* e dell'intelligenza artificiale, intorno a cui stiamo costruendo le basi della nostra convivenza futura. Non ci si dovrebbe ispirare a un *laissez-faire* tecnologico, né a un luddismo di retroguardia.

È invece necessario operare, in tutte le sedi, perché i processi in atto, i quali sono destinati a regolare segmenti crescenti della vita sociale dell'uomo, siano sottoposti a una logica di controllo democratico, che assicuri un adeguato bilanciamento tra la 'funzionalità "tecnologica" e la desiderabilità sociale degli scopi perseguiti, e rispetto alla quale la mediazione giuridica svolge un ruolo centrale.

Si deve cioè lavorare all'adozione di strumenti regolatori e di governo, preordinati ad evitare che la saldatura tra potere economico e potere tecnologico produca una società della sorveglianza e della discriminazione, in cui tutti siano profilati, segmentati in gruppi e resi destinatari di effetti giuridici o sociali in funzione dell'assetto di potere esistente. Non può, infatti, ignorarsi il pericolo che, come si è bene osservato, i nuovi modelli algoritmici creino le condizioni per un nuovo medioevo digitale. Si delinea cioè il rischio "di una società connotata da una segmentazione per caste, ove lo *status* non è però dato dalla nascita o dall'appartenenza a classificazioni sociali tradizionali (quelle su cui vigilano le norme in materia di non-discriminazione), ma da algoritmi e dai valori di coloro li generano. Classificazioni che sono poi impiegate per prendere decisioni che coinvolgono una pluralità di soggetti, i quali però non hanno contezza della propria posizione"[91].

Se ciò implica rigettare tanto un modello sregolato di "capitalismo della sorveglianza", il quale finirebbe per inchiodare la società alle sue iniquità e ai suoi pregiudizi, codificandoli nel linguaggio informatico[92], quanto un sistema programmato di "sorveglianza di stato", come nel già descritto caso del "social credit system" cinese[93], è necessario stabilire quale tecnica di intervento sia più adeguata al controllo dei trattamenti algoritmici. La logica del divieto *tout court* non sembra percorribile, per il semplice fatto che l'innovazione tecnologica, se attentamente monitorata, può apportare immensi benefici sociali, creando le

---

[91] A. Mantelero, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di* Artificial Intelligence, in A. Mantelero – D. Poletti, a cura di, *Regolare la tecnologia: il Regolamento UE 2016/679 e la protezione dei dati personali,* cit., 289 ss., 302.

[92] S. Barocas – A.D. Selbst, *Big Data's Disparate Impact,* cit., 671 ss.

[93] V. supra, par. 3.

premesse per una società più aperta ed inclusiva. Del pari, sembra utopistico pensare a un meccanismo di co-decisione pubblico-privato o a un'approvazione preventiva da parte di appositi enti pubblici degli algoritmi utilizzabili anche da soggetti privati. La strada più proficua appare quella dell'intervento a geometria variabile, composto cioè da forme più *soft* di incentivazione all'adozione di tecnologie e prassi organizzative *human rights compliant* (come nella logica dell'*accountability* prescritta dal GDPR per assicurare un trattamento conforme a parametri di sicurezza da valutare caso per caso e su iniziativa del singolo titolare del trattamento, oppure del ricorso a certificazioni e marchi che attestino l'uso di *transparency enhancing technologies*) e strumenti più incisivi con funzione prettamente regolamentare (come nel caso dei limiti sostanziali alle decisioni automatizzate posti dall'art. 22 GDPR), i quali dovrebbero poi ricadere a cascata sulla fase della programmazione dell'algoritmo, incentivando in ultimo una sorta di *legality by design*)[94]. Le regole emergenti in ambito in europeo, pur perfettibili da molti punti di vista, si ispirano ad una logica siffatta. Converrà, in conclusione, ribadire sinteticamente alcuni dei tratti caratterizzanti di questo modello.

Innanzitutto è caratteristico dell'approccio europeo sottoporre a un'attenta disciplina l'ecosistema informativo che sta a monte del funzionamento degli algoritmi, fissando alcuni requisiti di qualità e quantità (esattezza, accuratezza, minimizzazione dei dati, etc.) dei dati destinati a rappresentare l'input dei processi di *machine learning*. Le prime e più efficaci garanzie partono proprio dalla "giuridificazione" dei fenomeni di trattamento dei dati personali e dal controllo sulla profilazione individuale (par. 2.1.). Coerente, peraltro, con questa prospettiva è il divieto di sottoporre a trattamento algoritmico i dati che attengono al nucleo duro della *privacy,* e cioè i dati sulla salute, sull'orientamento politico, sulle fedi religiose, sull'origine etnica, etc. Per altro verso per sfruttare al massimo la capacità innovativa delle tecniche di *machine learning,* andrebbe tenuto fermo un principio di libera utilizzazione dei dati non personali, resistendo con forza ai tentativi di introdurre surrettiziamente diritti di proprietà sui dati grezzi (par. 2.2.).

In secondo luogo si attribuisce grande rilevanza al principio della trasparenza, il quale viene declinato in forme diverse e spesso convergenti: diritto di essere informato *ex ante* circa l'esistenza di un trattamento automatizzato; diritto di conoscere la logica di cui tale trattamento si avvale; diritto di comprendere

[94] In quest'ottica v. il ricco contributo di J.A. Kroll – J. Huey – S. Barocas et al., *Accountable Algorithms,* 165 *U. Pa. L. Rev.* 633 (2017); G. Malgieri – G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data-Protection Regulation*, cit.; M. Hildebrandt, *Algorithmic regulation and the rule of law, Phil. Trans. R. Soc. A* 376:20170355.

il modo e il grado in cui il trattamento algoritmico ha influito sui risultati della decisione che coinvolga la sfera del singolo; diritto di accedere all'algoritmo in quanto parte integrante di un procedimento amministrativo. Tutto ciò può contribuire in maniera rilevante alla 'leggibilità' e alla *accountability* degli algoritmi stessi, specie là dove si opti per un'interpretazione restrittiva delle clausole di salvaguardia poste a protezione della proprietà intellettuale e dei segreti commerciali in caso di richieste volte a conoscere la logica sottesa ai trattamenti algoritmici (par. 3.2.).

In terzo luogo, si va affermando un principio di massima, per cui l'individuo non deve essere sottoposto a una decisione integralmente automatizzata, allorché questa incida in maniera significativa sulla propria sfera giuridica. Quando ciò venga ammesso dall'ordinamento, si applicano una serie di garanzie sostanziali, tra le quali risalta lo strumento del riesame della decisione attraverso un diretto coinvolgimento dell'uomo, oltre ovviamente al controllo giudiziario *ex post* sulla conformità del trattamento algoritmico ai requisiti di legge (par. 3.3.).

Perché tali rimedi acquistino maggiore efficacia, appare necessario fare un ulteriore passo in avanti e, oltre ad estendere il perimetro di applicabilità delle norme in oggetto, valorizzare la dimensione collettiva del controllo sugli algoritmi. Ciò significa non soltanto sottolineare, come si è già fatto, che l'impatto potenzialmente distorsivo degli algoritmi sul piano richiede il concorso di diversi sotto-settori dell'ordinamento, e in primo luogo del diritto anti-discriminatorio, che va declinato in funzione del nuovo ecosistema digitale. Significa soprattutto potenziare il quadro dei rimedi di natura collettiva (come le azioni collettive promosse da enti *non profit* anche senza mandato preventivo da parte dei singoli) e affiancare alle tecniche di controllo individuale le iniziative del potere pubblico, valutando ad esempio l'introduzione di un'apposita autorità amministrativa indipendente che assommi le competenze frammentate tra le altre autorità per il settore del digitale[95].

[95] In questo senso è indirizzata la proposta del Sachverständigenrat für Verbraucherfragen (SVRV), *Lösungsoptionen,* cit., 38 ss.

Riccardo Rovatti

Termini e applicazioni dell'intelligenza artificiale

1. Premessa

Questo contributo riprende l'intervento fatto dall'autore il 30 marzo 2022 a Napoli per la Scuola Superiore della Magistratura nell'ambito del corso "I rapporti patrimoniali e le nuove tecnologie".

L'obiettivo di quell'intervento e quindi di questo scritto è dare qualche elemento utile alla comprensione dei temi scientifici e tecnologici che stanno dietro allo sviluppo delle odierne intelligenze artificiali nonché evidenziare alcune caratteristiche che possono costituire punti di primo contatto tra questa nuova tecnologia e la riflessione giuridica.

Per tentare di raggiungere tale obiettivo il primo passo e fare chiarezza su alcuni termini che vengono ormai quotidianamente impiegati nella narrazione di come l'intelligenza artificiale influenza e influenzerà la società civile. Ogni termine di provenienza tecnica, infatti, è generalmente carico di significati che si sono andati via via definendo durante lo sviluppo di quella disciplina e che, conosciuti, permettono di muoversi con più precisione sulla linea di confine con altre discipline.

Per uno dei concetti che si passeranno in rassegna, l'apprendimento automatico, che è il punto cardine della moderna intelligenza artificiale, si fornirà anche un esempio giocattolo sia con l'intento di chiarirne le potenzialità che per evidenziarne il fondamentale rapporto con i *dati*, entità che nelle loro varie incarnazioni sono ormai da tempo oggetto di cure da parte del Giurista e che per l'AI svolgono un ruolo cardine.

Seguono, infine, tre esempi di applicazione dell'intelligenza artificiale in contesti progressivamente dematerializzati: dal veicolo autonomo che percepisce l'ambiente fisico e agisce su di esso, attraverso l'intelligenza artificiale diagnostica che si limita all'osservazione e alla classificazione di ciò che proviene da sensori, fino ad intelligenze artificiali che vivono interamente all'interno dell'astrazione che chiamiamo "mercato" senza alcune necessità di controparti fisiche.

In tutti i casi sarà evidente come l'aggancio con le problematiche giuridiche sia forte indipendentemente dalla materialità delle azioni, e dipenda sostanzialmente dalle abilità cognitive e decisorie potenzialmente autonome di questa nuova tecnologia.

2. Termini e acronimi

L'intelligenza artificiale che cominciamo a vedere in azione intorno a noi, è il frutto di un impegno scientifico e tecnologico di più di 50 anni. In tale lasso di tempo si sono sviluppati teorie, metodi, macchine, applicazioni e, ovviamente, un linguaggio con termini (e acronimi: la volontà di sintesi di chi sviluppa tecnologia ne produce sempre molti) il cui significato, pur non sempre precisamente definito, è opportuno conoscere nel momento in cui si accoglie questa nuova tecnologia in un ambito di riflessione diverso da quello originale.

Il fatto che in questo caso si menzioni l'intelligenza, proprietà che tutti gli esseri umani, soprattutto quelli dotti, sentono come intimamente propria, ha generato sui termini che delineeremo qui discussioni molto approfondite di cui non sarà possibile dar conto. La scelta è quindi quella di limitarsi alle principali definizioni e distinzioni che permettano un veloce orientamento tra i concetti base, anche a costo di una approssimazione che si cercherà comunque di tenere al minimo.

L'Intelligenza Artificiale (acronimo italiano IA, ben meno frequente dell'inglese AI che utilizzeremo da ora in poi) è lo sforzo scientifico e tecnologico per rendere macchine che fanno calcoli (i *computer*) capaci di svolgere compiti per i quali si ritiene necessaria intelligenza, avendo come obiettivo le capacità umane.

Il termine ha origine non recentissima perché è stato concepito e per la prima volta utilizzato nella richiesta di finanziamento del "Dartmouth Summer Research Project on Artificial Intelligence", un evento di 8 settimane tenutosi nel 1956 e considerato il momento fondativo della disciplina[1].

Da allora lo sviluppo scientifico, per quanto discontinuo, è stato notevolissimo e ha portato all'AI di cui si comincia a fare esperienza quasi quotidiana.

Tale sviluppo ha, fra l'altro, permesso di chiarire che esiste una importante distinzione tra AI "deboli" o "specializzate" e AI "forti" o "generali". La maggior parte della AI in circolazione è di tipo debole ovvero è progettata per risolvere un numero limitato di compiti specifici e ben definiti a priori. Per risolvere il problema a cui è dedicata, un'AI debole si basa pesantemente sulla sua definizione, tanto da non risultare di per sé adatta ad affrontare compiti differenti per quanto analoghi dal punto di vista umano.

[1] https://en.wikipedia.org/wiki/Dartmouth_workshop.

Contrariamente a ciò, un'AI generale dovrebbe essere in grado di affrontare problemi multipli, non completamente o mal definiti che variano nel tempo, applicando a ciascuno di essi una strategia opportuna e differente. Il condizionale è qui necessario in quanto la costruzione di AI generali è un obiettivo sostanzialmente ancora non raggiunto pur esistendo prototipi di AI multispecializzate che ne sono una prima approssimazione.

È a questo punto importante distinguere l'ambito dell'AI da quello della robotica, scienza e tecnologia dei "robot", termine ancora più risalente, originato dalla fantasia dello scrittore Karel Čapek che nella sua opera teatrale «Rossumovi Univerzální Roboti», la cui prima messa in scena risale al 2 gennaio 1921, descrive macchine antropomorfe dedicate a servire gli esseri umani svolgendo "robota", ovvero *corvèe*.

L'origine della parola evidenzia chiaramente l'accento sulla fisicità delle azioni di un robot piuttosto che l'intelligenza eventualmente necessaria per compierle. I robot attuali sono infatti macchine programmabili in grado di svolgere compiti complessi interagendo con la realtà fisica anche in modo autonomo, solo in alcuni casi guidati da particolari AI.

La non identità dei due concetti, al di là del suggestivo uso combinato che se ne fa in divulgazione (si pensi al termine "giudice robot" che appare nelle narrazioni meno precise), è importante perché la maggior parte delle nuove implicazioni giuridiche della tecnologia che stiamo descrivendo viene dall'AI e non dai robot, in quanto da tempo gli esseri umani convivono con macchine in grado di agire nella realtà fisica anche in modo sofisticato senza dover per questo essere intelligenti e neanche autonome.

Concentrandoci sull'AI vale infine la pena di considerare due termini chiave come Apprendimento Automatico ("Machine Learning" con acronimo ML universalmente accettato) e Reti Neurali Profonde ("Deep Neural Networks" con acronimo DNN universalmente accettato).

Il ML è la chiave degli sviluppi più recenti e appariscenti dell'AI. Si tratta di un rovesciamento di prospettiva rispetto al normale flusso concettuale di progettazione di una macchina. Classicamente infatti, il tecnico cerca di comprendere il problema da affrontare, ne concepisce la soluzione in termini di sequenza di azioni elementari e attuabili da una macchina, e fa in modo che tale sequenza venga effettivamente eseguita. Si tratta di una procedura molto solida che dipende però dalla possibilità che un essere umano descriva la sequenza di operazioni elementari che porta alla soluzione.

Per compiti complessi, è possibile che il vincolo di considerare operazioni elementari (ovvero alla portata di una macchina non intelligente) renda la sequenza risolutiva non conoscibile o semplicemente troppo complessa per essere disegnata da un essere umano. In questo caso è possibile un approccio diverso.

Si predispone una macchina capace di svolgere un grande numero di operazioni elementari che possono essere programmate e combinate in molti modi. Si applica poi un *algoritmo di apprendimento automatico* che, considerando le possibilità della macchina e osservando esempi di soluzione valida del compito, configura le operazioni disponibili in modo che la macchina *impari* a risolverlo. L'essere umano quindi non disegna la macchina ma l'algoritmo di ML che, in base agli esempi di comportamento corretto che gli vengono sottoposti, la modifica a partire da uno stato iniziale sostanzialmente inutile fino ad uno stato finale nel quale è in grado di risolvere il problema.

Gli *esempi* che servono sono i *dati* dei quali è ormai ben noto come le AI si alimentino in maniera massiva e, per esempio, mostrano quale risposta ci si aspetta per possibili stimoli a cui si richiede di reagire. Ulteriormente esemplificando, ad una tipica AI dedicata al riconoscimento di oggetti contenuti in immagini, si forniranno campioni di immagini e corrispondenti classificazioni, di modo che, una volta terminato l'apprendimento, l'AI sia in grado di ricevere in ingresso un immagine mai vista prima producendo autonomamente una classificazione coerente con tutti gli esempi noti.

Tra le macchine che possono essere addestrate dal ML, le DNN sono particolari sistemi riconfigurabili la cui struttura si ispira (ormai molto da lontano) alla struttura biologica di alcune parti del nostro sistema nervoso centrale. Sono costituite da unità base chiamate neuroni che corrispondono alle già citate operazioni elementari che si concretizzano nell'accettare in ingresso un certo numero di segnali che vengono combinati in modo semplice per produrne uno in uscita. Questi neuroni sono organizzati in strati in modo che i neuroni di un certo strato accettino in ingresso le uscite dello strato precedente e forniscano la loro uscita ai neuroni dello strato successivo. L'elaborazione procede quindi strato per strato fino alla generazione dell'uscita complessiva di tutta la DNN che viene definita "profonda" in quanto di composta da molti strati.

La recente tecnologia elettronica ha permesso di gestire DNN di grande profondità con un numero di neuroni che supera agevolmente i molti milioni ai quali si applicano algoritmi di ML generalmente ispirati ad una strategia di base (la cosiddetta Stochastic Gradient Descent – SGD) anch'essa molto semplice e facilmente replicabile.

La composizione di queste innumerevoli semplicità fornisce comportamenti globali sofisticati utili a realizzare le AI attuali che riescono ad esibire a volte prestazioni superiori agli essere umani in alcuni ben definiti compiti cognitivi. È infatti del 2012 la celeberrima AlexNet[2], la prima DNN che, oppor-

[2] https://en.wikipedia.org/wiki/AlexNet.

tunamente allenata, individua quale tra un certo numero di oggetti predefiniti è raffigurato in una data immagine, con una probabilità di errore inferiore a quella dell'essere umano medio. Da allora, le prestazioni anche estreme nel risolvere un compito cognitivo specifico che possono essere raggiunte da una DNN sono state i mattoni fondamentali per la composizione delle AI di maggior successo.

Per quanto ad altre prestazioni le odierne AI specializzate commettono comunque errori che, pur riguardando compiti cognitivi, possono avere ripercussioni non trascurabili sul mondo reale. Come vedremo in seguito, questa fallibilità si aggiunge all'intelligenza del comportamento, nel rendere tutto ciò di rilevante interessante per il Giurista.

3. Un'AI giocattolo e l'importanza dei dati

In questo paragrafo il meccanismo astratto di ML viene esemplificato definendo e addestrando un'AI giocattolo il cui unico scopo è quello di distinguere i numeri positivi da quelli negativi. La banalità del compito implica che non sia necessaria una DNN ma sia sufficiente un solo "neurone" e per di più in forma estremamente semplificata. Il punto cardine è che questo unico componente non viene configurato direttamente per svolgere il compito ma, a partire da uno stato nel quale sarebbe totalmente inutile, viene sottoposto ad un elementare forma di ML che lo modifica gradualmente fino a renderlo capace di commettere solo un bassissimo numero di errori.

Il neurone giocattolo di cui ci occupiamo accetta un unico ingresso x che è il numero che vogliamo classificare come positivo o negativo ed esegue solo una elementare operazione di confronto con una soglia che indicheremo con θ, restituendo in uscita "positivo" se $x \geq \theta$ ovvero "negativo" se $x < 0$. Il comportamento del neurone è chiaramente definito dal solo parametro θ al quale viene inizialmente assegnato un valore qualunque e non il valore 0 che sarebbe naturale imporre immediatamente per ottenere il comportamento desiderato. Nel nostro esempio supporremo che inizialmente θ valga 2.

Sarà infatti compito dell'algoritmo di ML modificare il valore di θ in base a quanto osserva negli esempi di comportamento corretto che gli vengono forniti, ovvero, in questo caso, coppie di un numero e dell'etichetta "positivo" o "negativo". L'algoritmo di ML avrà quindi a disposizione una serie di coppie del tipo

(1 "positivo")
(-3 "negativo")
(-0,4 "negativo")
(1,5 "positivo")

Con un po' di approssimazione e sfruttando la semplicità del caso in esame possiamo sintetizzare l'algoritmo di ML in poche righe. Esso considera ciascuno degli esempi separatamente eseguendo per ognuno le stesse operazioni. In particolare sottopone al neurone il valore numerico da classificare e ne osserva la decisione. Se la decisione presa dal neurone in termini di "positivo"/"negativo" coincide con quella riportata nell'esempio il valore di θ non viene modificato. Viceversa, se il neurone classifica "positivo" un esempio che è in realtà "negativo" il valore di θ viene aumentato di una piccola quantità, mentre se il neurone classifica come "negativo" un esempio che è in realtà "positivo" il valore di θ viene diminuito di una piccola quantità.

Nel nostro caso, quando si considera il primo esempio, essendo $\theta = 2$, il neurone classificherà l'ingresso 1 (che è minore di θ) come "negativo" invece che il corretto "positivo". Questo fa sì che θ venga diminuito di una piccola quantità e, per esempio, portato a $\theta = 1{,}9$. Con questo nuovo valore si possono considerare il secondo e terzo esempio che vengono classificati correttamente come "negativi" essendo sia -3 che -0,4 minori di θ, che quindi non viene cambiato dall'algoritmo di ML. Quando si arriva al quarto esempio, però, il neurone classifica 1,5 come "negativo" e, di nuovo, il valore di θ viene diminuito arrivando a, per esempio, $\theta = 1{,}8$. Già seguendo questi pochi passi è chiaro come, a partire dal valore iniziale 2, θ venga fatto progressivamente avvicinare al valore corretto $\theta = 0$ che garantirà il funzionamento voluto. Infatti, più in generale, qualunque esempio con un numero positivo ma minore di un $\theta > 0$ viene classificato erroneamente come "negativo" e dà luogo ad una diminuzione di θ. Al contrario, se si ha $\theta < 0$, ogni esempio di numero negativo ma maggiore di θ viene classificato erroneamente come "positivo" e dà luogo ad un incremento di θ. Se opportunamente amministrato, questo procedimento di piccoli passi porta ad imparare il comportamento corretto $\theta = 0$ che rispecchia gli esempi forniti.

Il compito da imparare è in effetti così facile che i vantaggi del ML non si percepiscono: il flusso di progetto classico sarebbe stato molto più efficiente nel porre dall'inizio $\theta = 0$ senza dover ricorrere ai dati di esempio. Ciononostante, è già possibile apprezzare un vantaggio del nuovo approccio. Infatti, la stessa macchina (il nostro neurone giocattolo) e lo stesso algoritmo di ML avrebbero potuto risolvere un problema differente a patto di essere esposti ad esempi di ciò che si voleva. Se i dati avessero dichiarato, per ogni numero di esempio, "grande" o "piccolo" a seconda che si trattasse di una quantità minore o maggiore di 10, il risultato dell'addestramento sarebbe stato un neurone con $\theta = 10$ in grado di distinguere, con un trascurabile cambiamento di etichette, non più positivi da negativi ma grandi da piccoli.

Questa caratteristica di generalità delle strutture a DNN fa sì che molte delle tecniche sviluppate per un caso particolare possa essere poi riusato nell'affron-

tare applicazioni differenti a partire da nuovi insiemi di dati. Dati che si rivelano, quindi, il punto critico dell'approccio ML all'AI: le loro quantità e qualità influenzano radicalmente le prestazioni finali. La raccolta e la conservazione corretta (anche dal punto di vista giuridico) dei dati diventa così un prerequisito irrinunciabile allo sviluppo delle moderne AI.

4. Veicoli autonomi come robot intelligenti

Nonostante la radicale distinguibilità dei due concetti, la combinazione di robotica e AI ha importanti implicazioni. Infatti, anche se la maggior parte degli attuali robot in attività interagisce poco con la società essendo impiegato su linee di produzione dell'industria manifatturiera, la possibilità che l'AI ne aumenti l'intelligenza prelude a scenari come quello dei tanto attesi veicoli a guida autonoma: probabilmente l'esempio più attuale e emozionale di un robot dotato di una AI molto complessa e potenzialmente problematica

Il veicolo autonomo che si evolverà dalle versioni di livello inferiore già in circolazione sarà certamente un robot molto sofisticato nel quale le capacità di indirizzare la traiettoria di un corpo fisico lungo una strada saranno accoppiate a strumenti di cognizione e decisione artificiale equivalenti se non auspicabilmente superiori a quelli di un guidatore umano. Saranno proprio questi strumenti i più critici e soggetti a malfunzionamenti con effetti impattanti, come i guidatori umani sono i principali responsabili degli attuali incidenti.

Volendo menzionare solo il primo incidente mortale causato dal sistema "Autopilot" di Tesla, è noto[3] che il 7 maggio 2016 un veicolo in quel momento controllato a tutti gli effetti da un'AI si è schiantato contro un camion a causa del fatto che il sistema di interpretazione delle immagini non era stato in grado di riconoscere il suo cassone bianco sullo sfondo di un cielo molto luminoso.

Nessun malfunzionamento meccanico né del sistema di controllo di sterzo e frenata, solo un problema di cognizione ad evidenziare quanto sia proprio la parte AI a proporre gli interrogativi giuridici più rilevanti nell'inquadrare questa nuova tecnologia.

A tale proposito, nell'ottica di una valutazione più oggettiva del rischio che l'AI porta nel contesto sociale, è probabilmente utile riportare che quel primo incidente mortale è avvenuto dopo che il sistema di Tesla aveva guidato autonomamente veicoli per 210 milioni di Km complessivi. A titolo di confronto,

[3] Per una descrizione dell'accaduto: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.

le statistiche ci dicono che negli Stati Uniti si verifica 1 incidente mortale ogni 150 milioni di Km di guida umana, mentre nel mondo in generale se ne verifica 1 ogni 97 milioni di Km di guida umana.

Dopo 6 anni di ulteriori valutazioni ed esperienza su strada, l'affidabilità della guida autonoma è del tutto confermata e molto dello sviluppo tecnologico che rimane promette di rendere questa modalità di trasporto estremamente sicura.

Per quanto, quindi, l'applicazione di AI in questo campo stimoli discussioni in tema di responsabilità, trasparenza dei meccanismi interni, tracciabilità dei malfunzionamenti, ecc., la cui complessità non può essere riportata qui, è comunque opportuno tener presente che si tratta di riflessioni su eventi potenzialmente rarissimi e, come tali, dal presumibile basso impatto sociale ed economico.

Sarà verosimilmente molto più rilevante capire come la disponibilità di veicoli a guida autonoma trasformerà l'intero settore della mobilità, la cui importanza nel tessuto dell'economia globale è difficilmente sopravvalutabile.

5. AI per la diagnostica e tipi di errore

In ordine di dematerializzazione crescente, è interessante analizzare un'applicazione diversa dell'AI, le cui capacità di apprendimento di criteri di classificazione a partire da immagini o risultati di prove quantitative ben si prestano ad affrontare compiti di tipo diagnostico in medicina.

La complessità dei sistemi biologici e, di conseguenza, della scienza medica, impedisce la costruzione di AI che riproducano anche solo approssimativamente le capacità diagnostiche a largo spettro di un medico umano. Ciononostante, coerentemente con la definizione di AI specializzata, esistono nicchie nelle quali il problema diagnostico può essere così ben definito da permettere ad un'AI di estrinsecare il proprio potenziale.

Chiaro esempio di ciò è la prima applicazione di AI alla diagnostica per immagini autorizzata dalla Food and Drug Administration degli Stati Uniti. Si tratta di IDx-DR, un programma di analisi delle scansioni della retina di pazienti diabetici alla ricerca di indicatori dell'insorgenza di retinopatia[4]. Il fatto che si tratti di un caso di AI specializzata è evidente dal corposo insieme di prerequisiti esplicitati come necessari al corretto funzionamento dell'algoritmo, che arrivano a prescrivere non solo le modalità di acquisizione delle immagini della retina ma addirittura il modello della macchina di diagnostica per immagini da usare.

---

[4] M.D. Abràmoff, P.T. Lavin, M. Birch, N. Shah, J.C. Folk "Pivotal trial of an autonomous AI-based diagnostic system for detection of diabetic retinopathy in primary care offices," npj Digital Medicine volume 1, Article number: 39 (2018) – https://www.nature.com/articles/s41746-018-0040-6.

In queste condizioni strettamente controllate, le prestazioni diagnostiche dell'AI sono perfettamente confrontabili con quelle dei migliori esperti umani, come confermato da molteplici studi sia precedenti che successivi alla commercializzazione di IDx-DR. Lungo la strada aperta da questa AI si sono poi sviluppati innumerevoli altri tentativi di applicare la capacità cognitive dell'AI a problemi di diagnostica, soprattutto a partire da immagini, molti dei quali con prestazioni per lo meno paragonabili a quella dei medici umani.

Ancora nell'ottica di una maggior consapevolezza in merito alle prestazioni dell'AI, è sicuramente opportuno qualche dettaglio sulla valutazione delle capacità di diagnosi. Limitandosi al contesto ristretto della diagnosi binaria, nella quale bisogna solo decidere se una certa patologia è presente o meno, è facile convincersi che questa si componga in realtà di due abilità di tipo differente: l'abilità di identificare un soggetto malato come tale e l'abilità di identificare un soggetto sano come tale. A queste due abilità la medicina dà il nome, rispettivamente, di "sensibilità" e "specificità" cosicché il bravo diagnosta viene caratterizzato sia da alta sensibilità che da alta specificità.

Dal punto di vista di chi guarda ai possibili errori di valutazione piuttosto che ai successi nella diagnosi, la mancanza di sensibilità causa i cosiddetti "falsi negativi", ovvero casi a cui non viene associata una patologia che invece è presente. Dualmente, la mancanza di specificità genera "falsi positivi", ovvero casi considerati patologici quando invece non lo sono. Entrambi gli eventi di "falso" generano dei costi economici e sociali anche se l'importanza relativa tra di essi dipende dalla patologia.

Negli scenari reali, la complessità dei fattori che vengono considerati rende difficile non solo ridurre la probabilità dei "falsi" complessivi ma fa anche sì che nel momento in cui si cerca di diminuire fortemente il numero di falsi negativi si aumentino i falsi positivi e viceversa. Questo compromesso tra i due tipi di errore è facilmente comprensibile ragionando per estremi. Un modo ovvio per essere certi di dichiarare malati i pazienti che lo sono è, banalmente, quello di dichiarare malati tutti i pazienti, indipendentemente dalle evidenze cliniche. Questo azzera i falsi negativi ma, dal momento che dichiara malati anche tutti i pazienti sani, rende massimo il numero di falsi positivi. All'estremo opposto, se volessimo la certezza di annullare i falsi positivi potremmo dichiarare sani tutti i pazienti, aumentando però così al massimo i falsi negativi perché sarebbero dichiarati sani anche tutti i pazienti malati. Ogni metodo diagnostico concreto si piazza in un punto intermedio tra questi due estremi.

Un punto che molto spesso nella costruzione di un'AI diagnostica può essere spostato, con precise scelte progettuali, verso la riduzione dei falsi negativi o dei falsi positivi, eventualmente in seguito ad un'analisi dei costi sociali ed economici associati a ciascuno dei due tipi. Ciò aggiunge un grado di libertà che non

è del tutto proprio del medico umano per il quale il numero di falsi positivi e dei falsi negativi dipendente sostanzialmente dalla preparazione ed esperienza.

Quando si afferma, quindi, che un'AI di tipo diagnostico ha le stesse prestazioni di un medico si intende che nell'insieme di combinazioni falsi negativi-falsi positivi che possono essere ottenute programmando opportunamente l'AI ce ne è una molto prossima a quanto comunemente sperimentato nel caso di decisore umano.

6. AI per i mercati e collusione automatica

L'ultimo esempio in ordine di dematerializzazione dell'AI coinvolta è quello delle decisioni degli attori di un mercato.

È sicuramente noto che il mondo della finanza ha da tempo adottato sistemi automatizzati di gestione delle proprie attività tanto che si stima che nel 2020 più del 60% degli scambi di valore superiore a 10 milioni di dollari sia stato effettuato da algoritmi, anche se non necessariamente di AI. Sulla base di ciò, tutti i *trader* di alto livello ritengono che l'adozione di tecniche di AI nei mercati finanziari avrà un'importanza crescente nel prossimo futuro[5].

L'AI non è però applicabile solo ai mercati finanziari ma anche a quelli dei beni reali. Un esempio importante è quello dei metodi di assegnazione del prezzo ai beni offerti, il cosiddetto *pricing*[6]. Il *pricing* è un importante componente della strategia di offerta, soprattutto nei mercati in cui il bene offerto da ciascuno degli attori e poco distinguibile da quello offerto dagli altri, un tipico esempio essendo quello del carburante[7].

Un attore che vuole offrire beni su un tale mercato può allenare un'AI che osservando la storia dei prezzi praticati da tutti gli offerenti e delle quantità acquistate dai consumatori, decida il prezzo della propria offerta in modo da massimizzare il guadagno. Una volta imposto tale prezzo il mercato si riconfigura e la nuova situazione viene analizzata dall'AI per decidere eventuali variazioni, e così via in un inseguimento nel tempo del massimo profitto.

La potenziale complessità di comportamento di una singola AI dedicata al *pricing* viene amplificata dal fatto che anche gli altri attori possono dotarsi di AI analoghe. Si concretizza, quindi, un sistema nel quale i prezzi offerti ai consumatori sono decisi da un insieme di AI che competono tra di loro osservando lo

---

[5] Per un rapporto autorevole sul tema: https://www.jpmorgan.com/solutions/cib/markets/e-trading-2020.

[6] A titolo di esempio: https://www.intelligencenode.com/.

[7] A titolo di esempio: https://www.a2isystems.com/.

stesso mercato ma senza comunicare tra di loro. Il termine competizione assume a questo punto un significato differente da quello classico. In particolare, si viene ad instaurare un regime che può essere molto differente da quello della concorrenza perfetta che garantirebbe la massima efficienza economica. Si verifica infatti che è possibile che, nonostante l'indipendenza delle loro decisioni, le AI pilotino gli scambi verso un punto più vicino al monopolio, realizzando implicitamente quello che normalmente si otterrebbe se gli attori che offrono il bene colludessero tra loro[8].

Dal punto di vista sociale, l'attenuazione della competizione tra attori che offrono il bene si concretizza in uno svantaggio per i consumatori ed è per questo che la collusione è generalmente vietata negli ordinamenti giuridici, assumendo in alcuni casi anche rilevanza penale.

Il *pricing* governato da AI basate su ML permette di superare la logica dell'insieme di regole predefinite che era sottesa ai precedenti approcci e lascia che le decisioni prese non seguano altra logica se non quella della massimizzazione del profitto. Questo fa sì che il decisore autonomo impari e metta in atto strategie reattive che prevedono non solo la convergenza ad un prezzo più alto di quello perfettamente concorrenziale quando anche gli altri attori perseguono quella strada, ma anche la previsione di azioni "punitive" (ovvero decisioni sul proprio prezzo con lo scopo di causare temporanee perdite agli altri attori) nei confronti di chi non si allinea e tenta di innescare una guerra di prezzo al ribasso, così come la rimozione della punizione e un implicito "perdono" quando l'attore punito ritorna a convergere verso prezzi più alti.

Tutto ciò in assenza di comunicazione esplicita tra le AI quando, spesso, dal punto di vista giuridico, la comunicazione esplicita è uno dei prerequisiti per la perseguibilità dei tentativi degli attori di un mercato di formare un cartello ai danni dei consumatori.

7. Conclusioni

Negli ultimi 10 anni, lo sviluppo tecnologico ha permesso di realizzare intelligenze artificiali (AI), prevalentemente basate su reti neurali profonde (DNN) e su un uso intenso di apprendimento automatico (ML), le cui prestazioni in compiti spiccatamente cognitivi e comunque intelligenti si sono avvicinate a quelle degli esseri umani, superandole in qualche caso.

---

[8] E. Calvano, G. Calzolari, V. Denicolò, J.H. Harrington Jr., S. Pastorello, "Protecting consumers from collusive prices due to AI," Science, novembre 2020

Per quanto di tipo specializzato o ristretto, ovvero ciascuna dedicata ad un singolo compito ben definito, queste AI possono essere applicate nei più svariati contesti. Questa breve rassegna ha descritto tre tipi di applicazioni, in ordine decrescente di interazione con la realtà fisica: dal veicolo autonomo, attraverso i sistemi di diagnosi per immagini, fino al decisore dei prezzi di vendita di un bene in un mercato competitivo. In tutti i casi, sono chiaramente critici sia la dipendenza dai dati necessari all'addestramento delle DNN sia il fatto che, per quanto ridotta, esiste sempre una probabilità di errore che in qualche caso può essere amministrata ma non annullata.

Oltre a ciò, l'ultimo caso ha evidenziato che in un sistema che vede l'interazione tra più di un'AI, l'intelligenza può spingere i comportamenti verso un coordinamento implicito facendo emergere situazioni che, se ottenute da comportamenti umani, potrebbero essere considerate illecite.

Se qualcosa si può trarre già da queste poche note è che dotare oggetti inanimati di comportamenti intelligenti e autonomi ha le potenzialità di una rivoluzione. Una rivoluzione che fa leva sulla caratteristica che gli esseri umani sentono come più propria e che è alla base della stessa costruzione sociale. Una rivoluzione che per poter essere governata ha bisogno che Diritto e Tecnologia sviluppino un linguaggio condiviso e una fiducia reciproca che si costruiscono, anche, con iniziative come quella a cui questo contributo deve la propria origine.

Giusella Finocchiaro

Intelligenza artificiale e responsabilità*

Sommario: 1. Sul metodo: la verifica della necessità di un intervento legislativo. – 2. Il ruolo del legislatore europeo. – 3. L'intelligenza artificiale e le sue implicazioni giuridiche. – 4. La retorica. – 5. Nuove questioni concernenti la responsabilità.

1. Sul metodo: la verifica della necessità di un intervento legislativo

L'intelligenza artificiale è un tema che oggi non manca di suscitare attenzione anche presso i giuristi[1]. Si susseguono convegni e articoli in materia che mirano a descrivere e inquadrare il fenomeno di cui oggi quotidianamente si parla e a vagliare le implicazioni giuridiche delle nuove applicazioni tecnologiche. La conclusione di questi approfondimenti è sovente quella di auspicare un intervento del legislatore.

Tale esito, condivisibile in taluni casi, tuttavia non può che rappresentare la conclusione di un'indagine volta a verificare se le norme vigenti consentano di prospettare una soluzione interpretativa, che si porrebbe evidentemente, in tutto o in parte, come alternativa all'intervento legislativo e che renderebbe quest'ultimo superfluo.

Preliminarmente e con evidenza, si pone dunque un problema metodologico, sovente trascurato, sul quale è importante rinnovare la consapevolezza del

---

* Il presente saggio è stato pubblicato in Contratto e impresa, 2, 2020, 713 ss.

[1] Il tema è di grande interesse anche in ambito bancario, tanto da essere stato menzionato nella Relazione del Presidente dell'ABI alla Giornata del risparmio 2019. Si veda il recentissimo *Expert Group on Regulatory Obstacles to Financial Innovation* (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission*, December 2019, disponibile al seguente link https://ec.europa.eu/info/publications/191113-report-expert-group-regulatory-obstacles-financial-innovation_en, consultato il 12 gennaio 2020. Si rinvia inoltre al rapporto CEPS (*Centre for European Policy Studies*), *Artificial Intelligence: Ethics, Governance and Policy Challenges*, curato da Renda, 2019, disponibile al link https://www.ceps.eu/ceps-publications/artificial-intelligence-ethics-governance-and-policy-challenges/ e presentato in Assonime il 25 marzo 2019, nonché al rapporto dell'AI *Now Institute at New York University, AI Now Report 2019*, dicembre 2019, disponibile al link https://ainowinstitute.org/AI_Now_2019_Report.pdf, consultato il 12 gennaio 2020.

giurista: occorre innanzitutto comprendere se e quali interventi normativi siano davvero necessari[2].

L'approccio teso a richiedere comunque nuove regole ha caratterizzato, negli anni, l'atteggiamento di una parte della dottrina giuridica verso l'informatica, forse per una sorta di timore reverenziale o forse di ritrosia nei confronti delle nuove tecnologie. Già dagli anni '60 ci si è interrogati sulla necessità di nuove leggi con riferimento a nuove fattispecie. Si può risalire al dibattito sulla tutela del *software*[3], alla richiesta di disposizioni per la protezione della *privacy*[4] e più tardi alla genesi delle norme sul documento informatico[5] e sul commercio elettronico[6].

---

[2] Si interroga sul ruolo del diritto in relazione ai nuovi fenomeni emergenti anche G. Alpa, *Fintech: un laboratorio per i giuristi*, in Fintech: *diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, a cura di Finocchiaro e Falce, Bologna, 2019, p. XIII-XXII.

[3] Si fa riferimento a G. Santini, *La tutela giuridica della programmazione elettronica*, in *Giur. it.*, 1968, coll. 225-232, il quale, facendo presente che alcuni autori hanno negato «come cosa pacifica, che il programma, e dunque il programmatore, godano di una qualunque tutela nell'ordinamento italiano», dal canto suo sostiene che vada «respinta, nel nostro ordinamento, la semplicistica conclusione che non vi sia *de iure condito* alcun mezzo per tutelare l'attività originale dei programmatori di calcolo elettronico»; a E. Luzzato, *Una norma di legge francese da non imitare (a proposito della brevettabilità o meno dei programmi o serie di istruzioni per lo svolgimento delle operazioni dei calcolatori elettronici)*, in *Riv. dir. ind.*, 1968, p. 297-306, che riconosce come «certe forme di *software* indubbiamente meritano una protezione brevettuale, altre non meritano protezione alcuna e per altre, infine, si potrà trovare una diversa forma di protezione nel quadro delle leggi esistenti, interpretate tenendo conto della nuova realtà tecnica, o nel quadro di nuove norme di legge» e conclude ritenendo che ciò che «occorre in questo campo, se mai, è un'approfondita elaborazione tecnica del problema e non la redazione di affrettate, drastiche e ingiustificate norme di legge». Infine, interrogandosi sulla tutela del *software*, R. Borruso, Computer *e diritto. Problemi giuridici dell'informatica*, Milano, 1988, II, p. 389 ss., ricerca una normativa appropriata ritenendo che il *software* non possa essere tutelato né dalle norme civili e penali né dal diritto d'autore.

[4] Cfr. V. Frosini, *La protezione della riservatezza nella società informatica*, in *Informatica e diritto*, 1981, p. 5-14, che riteneva imprescindibile l'esigenza di colmare con nuove disposizioni normative la lacuna in tema di protezione dei dati esistente all'epoca nel nostro ordinamento giuridico; M. Losano, *Un progetto di legge sulla protezione dei dati personali*, in *Dir. inf.*, 1987, p. 465-485.

[5] Si interrogano sull'opportunità di ricondurre la forma elettronica a quella orale o a quella scritta ovvero di considerare la forma elettronica come una nuova forma, L. Montesano, *Sul documento informatico come rappresentazione meccanica della prova civile*, in *Dir. inf.*, 1987, p. 23-31; Parisi, *Il contratto concluso tramite computer*, Padova, 1987; F. Stallone, *La forma dell'atto giuridico elettronico*, in *questa rivista*, 1990, p. 756-778.

[6] V. *ex multis* G. Mirabelli, *I contratti di informatica: modelli, tipicità, collegamento,* in *I contratti di informatica. Profili civilistici, tributari e di bilancio,* a cura di G. Alpa e V. Zeno Zencovich, Milano, 1987, p. 9-19, il quale molto chiaramente afferma che «il legislatore può e deve intervenire solo quando si sia accertato che la situazione nuova presenta degli elementi che non si riescono ad inserire in alcun modo nell'ordinamento vigente, cioè quando la realtà abbia dimostrato che

Tuttavia, si può fin d'ora anticipare che solo in un caso, quello della normativa sulla protezione dei dati personali, si è giunti ad emanare un corpo normativo integralmente nuovo, mentre negli altri casi il legislatore si è risolto ad apportare modifiche ed integrazioni alle leggi vigenti.

Si potrebbe, con lieve ironia, parlare di apocalittici e integrati, di conservatori e interventisti, e così tracciare una distinzione fra chi ritiene che le norme vigenti siano sufficienti e chi, al contrario, ritiene comunque un intervento legislativo necessario e spesso, urgente e indifferibile.

Il tema è stato ampiamente discusso di recente in occasione dell'«*UNIDROIT-UNCITRAL Joint Workshop on smart contracts, artificial intelligence and distributed ledger technology*» che si è tenuto a Roma presso la sede Unidroit il 6-7 maggio 2019[7] e che aveva l'obiettivo di valutare se e quali interventi normativi a livello internazionale fossero necessari con riguardo agli *smart contract*, all'intelligenza artificiale e alla *distributed ledger technology*.

Nelle conclusioni del *workshop* il Professor Kanda ha evidenziato che occorre adottare un duplice approccio: da un lato, per così dire, difensivo, volto ad adattare gli strumenti già esistenti emanati da queste organizzazioni internazionali alle nuove tecnologie, e dall'altro, proattivo, volto ad emanare poche regole semplici per facilitare lo sviluppo delle tecnologie, in alcuni limitati settori.

Benché si corra forse il rischio di affermare l'ovvio, occorre ribadire che gli ordinamenti giuridici sono caratterizzati da una elasticità che consente di assorbire le sollecitazioni provenienti dai cambiamenti in ogni settore: dai cambiamenti del costume, a quelli sociali, a quelli tecnologici, per citarne solo alcuni. L'interpretazione, strumento principe nel lavoro del giurista, consente di rinnovare la norma dal suo interno, spesso lasciandone immutato l'aspetto formale. L'evoluzione interpretativa dell'art. 2043 c.c., ad esempio, rende evidente quali siano le potenzialità interpretative e quali le «mobili frontiere»[8].

---

gli interessi, che emergono da una situazione nuova, non possono in alcun modo trovare soddisfacimento inquadrando questa situazione negli schemi noti»; Z. Zencovich, *Sul rilievo pratico e sistematico della categoria dei c.d. contratti di informatica*, in *I contratti di informatica. Profili civilistici, tributari e di bilancio,* a cura di G. Alpa e V. Zeno Zencovich, cit., p. 31-41, che avverte della «pericolosa ambiguità dei termini "contratti di informatica" o "contratti informatici" qualora, travalicando semplici esigenze descrittive, si volesse attribuire loro autonomia concettuale e sistematica rispetto a contratti di altro genere o aventi diverso "oggetto" (…)».

[7] Ho partecipato all'incontro in qualità di Presidente del Gruppo di lavoro sul commercio elettronico dell'Uncitral presiedendo la sessione «*DLT, Smart contracts and AI in the transactional lifecycle: general contract law issues*». Per ulteriori approfondimenti, si invita a consultare il sito www.unidroit.org.

[8] Secondo la celebre espressione di F. Galgano, *Le mobili frontiere del danno ingiusto*, in *questa rivista*, 1985, p. 1 ss.

Talora lo strumentario del giurista basato principalmente sull'interpretazione, si rileva comunque insufficiente e l'intervento del regolatore si profila necessario: o per fare chiarezza, così eliminando l'incertezza giuridica, o per colmare lacune. Ma questa conclusione non può che profilarsi come l'esito di un processo di attenta verifica delle strade interpretative percorribili e della normativa applicabile e non in maniera apodittica, seguendo suggestioni di innovazione.

Se si esaminano i settori investiti dalla tecnologia e citati come esemplari all'inizio di questo lavoro, emerge che soltanto in un caso è stato ritenuto necessario effettuare interventi normativi radicali e precisamente con riguardo alle disposizioni in materia di protezione dei dati personali, sulla base di spinte provenienti da organizzazioni internazionali e istituzioni europee: basti pensare alla Convenzione 108 del Consiglio d'Europa[9] e alla dir. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[10]. Negli altri casi, invece, si è trattato di integrazione di norme già esistenti. Così nel caso della tutela del *software*, quando è stata modificata e integrata la disciplina in materia di diritto d'autore[11]; così nel caso del documento informatico, quando sono state emanate delle disposizioni di raccordo al Codice civile che hanno sviluppato in parallelo al codice la disciplina delle firme elettroniche[12]; così in materia di commercio elettronico, quando si è scelto di non modificare la disciplina dettata dal Codice civile e dal Codice del consumo in materia di contratto[13].

---

[9] «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», firmata a Strasburgo il 28 gennaio 1981. Il 5 marzo 2019 l'Italia ha adottato il protocollo emendativo della Convenzione 108, ora detta anche «Convenzione 108», con cui si conclude il processo di modernizzazione della Convenzione.

[10] Come è noto, la direttiva è stata abrogata dal Reg. (UE) 2016/679 che, a partire dal 25 maggio 2018, è applicato direttamente in tutti gli Stati membri e detta la nuova disciplina in materia di protezione dei dati personali. Per approfondimenti, cfr. il volume da me diretto, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

[11] Il riferimento è evidentemente al d.lgs. 29 dicembre 1992, n. 518, «Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore», che ha modificato e integrato la l. 22 aprile 1941, n. 633, «Protezione del diritto d'autore e di altri diritti connessi al suo esercizio».

[12] Si pensi al d.lgs. 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale», modificato a più riprese, da ultimo con il d.lgs. 13 dicembre 2017, n. 217, «Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale».

[13] La disciplina del commercio elettronico è contenuta nel d.lgs. 9 aprile 2003, n. 70 di attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazio-

Dunque talora gli interventi normativi non sono necessari, talaltra sono opportuni per fare chiarezza e dirimere incertezze, talaltra ancora sono necessarie vere e proprie innovazioni.

Ciò che certamente è da respingere è l'aprioristico ricorso a una normazione emergenziale che spesso non rispetta i principi consolidati in ambito internazionale. L'esempio negativo è costituito dalla disposizione contenuta nell'art. 8 *ter*[14] del d.l. 14 dicembre 2018, n. 135 (meglio noto come, "Decreto Semplificazioni")[15], che definisce la tecnologia della *blockchain* e le applicazioni di *smart contract*[16] [17].

La norma citata, sotto il profilo giuridico, è errata per almeno due ordini di ragioni. In primo luogo, perché viola il principio della neutralità tecnologica, consolidato nel dibattito internazionale. In secondo luogo, perché vincola il soddisfacimento del requisito della forma scritta degli *smart contract* all'identificazione delle parti secondo un processo che dovrà essere disciplinato da AgID,

---

ne nel mercato interno, con particolare riferimento al commercio elettronico. L'art. 68 dello stesso d.lgs. 6 settembre 2005, n. 206 «Codice del consumo» rinvia al sopra citato d.lgs. 70/2003 per la disciplina delle offerte di servizi della società dell'informazione, effettuate ai consumatori per via elettronica, con riguardo a quegli aspetti non disciplinati dal Codice del consumo.

[14] Questa disposizione non era presente nel testo originario del decreto legge citato, ma è stata introdotta dalla legge di conversione 11 febbraio 2019, n. 12 (in G.U. 12 febbraio 2019, n. 36).

[15] D.l. 14 dicembre 2018, n. 135, *Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*, pubblicato in G.U. del 14 dicembre 2018, n. 290.

[16] L'art. 8 *ter* così dispone: «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, 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. 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. 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».

[17] Per la critica a questa norma rinvio al mio contributo, *Intelligenza artificiale e protezione dei dati personali,* in *Giur. it*., 2019, p. 1670-1677.

finendo, dunque, col rallentare l'espansione della tecnologia che si regola. Oltre a ciò, quando la forma scritta del documento informatico è materia già ampiamente disciplinata dal Codice dell'amministrazione digitale[18] che certamente non richiede ulteriori precisazioni.

2. Il ruolo del legislatore europeo

Il settore dell'intelligenza artificiale è caratterizzato dalla pluralità dei livelli di normazione e dalla complessità delle regole astrattamente applicabili o auspicabili. Dalle regole dell'etica il cui contributo è sempre più frequentemente invocato[19], alle regole dettate dalla stessa tecnologia[20], alle regole contrattuali dettate dai provider, alla *soft law*.

Se ci si riferisce alle norme vere e proprie, cioè alla *hard law*, il livello al quale le norme devono essere dettate è quanto meno quello europeo, dal momento che gli interessi che si confrontano sono interessi, politici ed economici, globali, per le dimensioni del mercato e degli attori.

Basti pensare ai grandi attori nell'ambito dei social media e dei motori di ricerca, i quali sono statunitensi o cinesi, come Facebook, Google, Baidu, Ali Baba, per citarne solo alcuni.

L'azione del legislatore nazionale è naturalmente limitata perché il fenomeno è globale e anzi paradigmatico dell'era della globalizzazione, così come le regole contrattuali, dettate dagli attori, che lo governano. Restano di competenza degli Stati nazionali le disposizioni di ordine amministrativo e regolamentare, mentre certamente è nazionale l'azione giudiziaria, nonché quella delle autorità di vigilanza e amministrative indipendenti.

A conferma di quanto illustrato è evidente che il legislatore europeo sta costruendo, anche attraverso l'azione normativa, il mercato digitale europeo.

---

[18] Il già citato d.lgs. 7 marzo 2005, n. 82, successivamente modificato e integrato con il d.lgs. 22 agosto 2016, n. 179 e poi con il d.lgs. 13 dicembre 2017, n. 217.

[19] Il riferimento è in particolare al tentativo della Commissione europea di delineare un nuovo approccio al problema basato sull'etica, nel rispetto di un "quadro etico basato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali dell'Unione europea". Un esempio è offerto da *La Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi*, adottata dalla *European Commission for the Efficiency of Justice* (organismo del Consiglio d'Europa) il 3-4 dicembre 2018. Si tratta del primo documento con cui vengono espressi alcuni principi etici alla cui osservanza lo sviluppo e l'adozione di sistemi di intelligenza artificiale devono essere subordinati. Tra questi principi vengono indicati, in particolare, il rispetto dei diritti fondamentali dell'uomo, la non discriminazione e il controllo dell'utente sui dati.

[20] Cfr. per tutti L. Lessig, *Code and other laws of cyberspace*, New York, 1999.

Anche in questo senso vanno letti il Reg. (UE) 2016/679 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»[21] (nel prosieguo, per brevità, «Regolamento») e il Reg. (UE) 2014/910 del Parlamento europeo e del Consiglio del 23 luglio 2014, «in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE»[22].

Il primo, come è noto, ha ad oggetto, sia la protezione dei dati personali che la libera circolazione dei dati, benché in Italia quest'ultima sia generalmente relegata in secondo piano. Il secondo ha ad oggetto il riconoscimento reciproco dei sistemi di identificazione on line, l'autenticazione e i servizi fiduciari.

Oggi la fonte normativa è europea e il legislatore europeo ha riscritto la normativa italiana sulle firme elettroniche e sul documento informatico, così come quella sulla protezione dei dati personali.

Come è noto, l'Italia aveva disciplinato la firma digitale, una particolare tipologia di firma elettronica, già nel 1997, con la l. n. 59 del 1997 e poi il

---

[21] Reg. (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), pubblicato in G.U.U.E. L 119/1 del 4 maggio 2016. In generale, sul Regolamento G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *questa rivista*, 2017, p. 723-733; *Le nuove frontiere della* privacy *nelle tecnologie digitali*, a cura di G. Busia, L. Liguori e O. Pollicino, Roma, 2016; *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, a cura di L. Califano, e C. Colapietro, Napoli, 2017; *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019; il già citato *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101,* a cura di G. Finocchiaro, Bologna, 2019; *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice* privacy*)*, a cura di R. Panetta, Milano, 2019; F. Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; *GDPR e Normativa* Privacy. *Commentario*, a cura di G.M. Riccio, G. Scorza e E. Belisario, Milano, 2018; *La nuova disciplina europea della* privacy, a cura di S. Sica, V. D'Antonio e G.M. Riccio, Padova, 2016; Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di E. Tosi, Milano, 2019; *Persona e mercato dei dati: riflessioni sul GDPR*, a cura di N. Zorzi Galgano, Padova, 2019.

[22] Pubblicato in G.U.U.E. L 257 del 28 agosto 2014. Il Regolamento è, in sigla, comunemente denominato «eIDAS», dove «e» sta per «*electronic*», «ID» per «*identification*», «A» per «*authentication*» e «S» per «*signature*». Per un commento si rinvia al mio, *Una prima lettura del regolamento europeo eIDAS: identificazione on line, firme elettroniche e servizi fiduciari*, in *Nuove leggi civ.*, 2015, p. 419 ss., nonché al volume da me curato con F. Delfini, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017 e al recente volume *EU eIDAS Regulation. Article-by-Article Commentary*, a cura di A. Zaccaria, M. Schmidt Kessel, R. Schulze e A.M. Gambino, Beck-Hart-Nomos, 2019.

d.p.r. n. 513/1997. Questa disciplina è stata poi riscritta per renderla compatibile con quella europea, di segno opposto, fino ad approdare al quadro normativo attuale dettato congiuntamente dal Reg. (UE) e-IDAS e dal Codice per l'amministrazione digitale.

Il legislatore europeo ha riscritto anche la disciplina sulla protezione dei dati personali con il Reg. (UE) 2016/679. Ciò che resta del Codice per la protezione dei dati personali, ormai privo dell'organicità, della struttura e dell'ordine che sono proprie di un codice, avrebbe dovuto essere abrogato, anche per favorire la maggiore chiarezza possibile nell'edificando sistema della protezione dei dati personali, come in più occasioni si è illustrato[23].

Dunque il ruolo del legislatore europeo è volto a costruire il mercato europeo e ad affermare un modello europeo anche sotto il profilo normativo.

Il legislatore europeo si trova, tuttavia, in una posizione non certamente semplice, quella di rendere compatibili spinte che appaiono, quanto meno in prima battuta, divergenti. Esse sono, da un lato, la valorizzazione anche economica dei dati personali e più in generale delle informazioni e dall'altro, la protezione dei diritti fondamentali.

L'approccio è dunque inevitabilmente ambivalente: da un lato si promuove il mercato, dall'altro lo si limita per tutelare i diritti fondamentali. I due interessi paiono tuttavia conciliabili e anzi devono essere conciliati, costruendo un modello europeo di circolazione sicura dei dati e delle informazioni, senza che l'una o l'altra esigenza prevalga a priori e necessariamente.

Tutela della persona e costruzione del mercato digitale europeo[24] costituiscono il duplice obiettivo da raggiungere per il legislatore europeo anche con riguardo al tema più attuale, quello dello sviluppo dell'intelligenza artificiale. È lo «spazio dei dati europeo» cui ci si riferisce già nella comunicazione della Commissione europea *L'intelligenza artificiale per l'Europa*[25] ove l'esigenza di disporre di dati personali viene controbilanciata dalla necessità di assicurare il pieno rispetto della legislazione sulla protezione degli stessi[26].

---

[23] Si rinvia al volume da me diretto, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

[24] «Persona e mercato dei dati. Riflessioni sul GDPR» è il titolo del libro curato da N. Zorzi Galgano, Milano, 2019. Sullo stesso tema v. anche V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, p. 689-726.

[25] Comunicazione della Commissione europea, *L'intelligenza artificiale per l'Europa*, COM (2018) 237, 25 aprile 2018, p. 11.

[26] Così anche COM(2018) 795 e l'allegato alla stessa, intitolato *Piano coordinato per lo sviluppo e l'utilizzo dell'intelligenza artificiale "*Made in Europe*"*, p. 14. Nello stesso senso la Risoluzione del Parlamento europeo del 12 febbraio 2019 che invita «la Commissione a garantire che qualsiasi

Infatti, come è noto, l'intelligenza artificiale si basa sui dati. Una delle ragioni per le quali, pur essendo stata ampiamente studiata già molti anni fa[27] e pur essendo sotto molti aspetti già matura, non aveva dato luogo ad applicazioni tecnologiche diffuse, era costituita dall'assenza di una grande quantità di dati a disposizione, oltre che naturalmente dalla differente potenza di calcolo e dalla minore connettività disponibili. Si stimano in miliardi gli utenti che quotidianamente forniscono dati, spesso non consapevolmente, per esempio attraverso i *social network* e i motori di ricerca, in tutto il mondo[28]. L'intelligenza artificiale si

futuro quadro normativo dell'Unione europea in materia di intelligenza artificiale garantisca la riservatezza e la confidenzialità delle comunicazioni, la protezione dei dati personali, compresi i principi di legalità, equità e trasparenza, la protezione dei dati fin dalla progettazione e per impostazione predefinita, la limitazione delle finalità, la limitazione della conservazione, la precisione e la minimizzazione di dati, nel pieno rispetto del diritto dell'Unione in materia di protezione dei dati». Sul punto, va segnalata anche la Risoluzione approvata il 21 gennaio 2020 dalla *Committee on the Internal Market and Consumer Protection* del Parlamento europeo, ove è ribadita l'importanza che i sistemi di intelligenza artificiale utilizzino *set* di dati di alta qualità e imparziali nonché «algoritmi spiegabili e imparziali» al fine di aumentare la fiducia e l'accettazione dei consumatori (p. 5). Da ultimo, anche il Comitato economico e sociale europeo ha espresso sul tema il proprio punto di vista nel parere *Creare fiducia nell'intelligenza artificiale antropocentrica* pubblicato nella G.U.U.E. dell'11 febbraio 2020 ove raccomanda di «prevedere, prevenire e impedire l'impiego doloso dell'IA e dell'apprendimento automatico» e di «sviluppare un approccio all'IA che ponga al centro l'essere umano ("antropocentrico") e conforme ai valori su cui l'Unione si fonda (quali) rispetto della dignità umana, libertà, democrazia, uguaglianza e non discriminazione, Stato di diritto, rispetto dei diritti umani».

[27] La nascita dell'intelligenza artificiale si fa risalire alla Conferenza di Dartmouth (Hanover, New Hampshire) del 1956. V. il testo della proposta con cui gli organizzatori della conferenza (nonché "padri fondatori" di questa tecnologia) affrontarono i temi principali del campo di ricerca, tra cui le reti neurali, la teoria della computabilità, la creatività, l'elaborazione e il riconoscimento del linguaggio naturale: J. McCarthy, M. Minsky, N. Rochester, C. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802.

[28] Secondo il *Global Digital Report 2019* di *We are Social* e *Hootsuite* (note agenzie di *social media management*), sono 4.39 miliardi gli utenti che si collegano a Internet nel 2019, con un aumento di 366 milioni (9%) rispetto a gennaio 2018; sono invece 3.48 miliardi gli utenti che frequentano *social media*, con un totale mondiale in crescita di 288 milioni (9%) rispetto allo scorso anno (il *report* integrale è disponibile al seguente link https://datareportal.com/reports/digital-2019-global-digital-overview, consultato in data 25 marzo 2019). Interessante è anche lo spaccato che offrono Lori Lewis e Chadd Callahan di *Cumulus Media* che mostra le attività svolte su varie piattaforme *web* nell'intervallo di un minuto: ad esempio, è stato rilevato che, nel 2018, ogni 60 secondi sono state effettuate 3.7 milioni di ricerche su Google; 973.000 accessi a Facebook; 481.000 post su Twitter; 187 milioni di *e-mail* inviate; 38 milioni di messaggi inviati attraverso il servizio *chat* di WhatsApp; 4.3 milioni di video visualizzati su YouTube (tale analisi, sotto forma di infografica, è ripresa da diverse testate, tra cui il Sole24Ore, ed è disponibile al seguente link https://www.infodata.ilsole24ore.com/2018/05/17/cosa-accade-internet-un-minuto/).

nutre di dati[29] e ora i dati sono certamente disponibili, spesso addirittura gratuitamente. Il nuovo petrolio, secondo la celebre metafora dell'*Economist*[30], costituisce la risorsa primaria della nuova economia digitale.

3. L'intelligenza artificiale e le sue implicazioni giuridiche

«L'intelligenza artificiale non è fantascienza: fa già parte delle nostre vite»[31]. Come si è accennato, al tema la Commissione ha dedicato molti studi e approfondimenti recentemente, a partire dalla nota Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, la quale si ricorda anche per la citazione delle leggi di Asimov[32].

Come si legge nella Comunicazione *L'intelligenza artificiale per l'Europa*, i sistemi basati sull'intelligenza artificiale possono consistere solo in *software* che agiscono nel mondo virtuale (per esempio assistenti vocali, *software* per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale); oppure incorporare l'intelligenza artificiale in dispositivi *hardware* (per esempio in *robot* avanzati, auto a guida autonoma, droni o applicazioni dell'*Internet* delle cose)[33].

Le applicazioni di intelligenza artificiale possono avere un rilevante impatto su alcuni istituti giuridici.

Ci si è chiesti, ad esempio, se gli *smart contract* siano davvero contratti[34], sotto il profilo giuridico, e in quale modo eventualmente modifichino l'istituto di riferimento. O se non si tratti piuttosto di modalità di esecuzione di contratti

---

[29] Cfr. Commissione consultiva della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, 25 gennaio 2019.

[30] *The Economist*, *The world's most valuable resource is no longer oil, but data*, pubblicato il 6 maggio 2017.

[31] Così la Commissione europea nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, COM(2018) 237, 25 aprile 2018, p. 1.

[32] «(…) le leggi di Asimov devono essere considerate come rivolte ai progettisti, ai fabbricanti e agli utilizzatori di *robot*, compresi i *robot* con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice macchina (…)», punto T della Risoluzione.

[33] Per maggiori approfondimenti, si rinvia al mio contributo *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, pp. 441-460.

[34] Cfr. F. Di Giovanni, *Attività contrattuale e intelligenza artificiale,* in *Giur. it.*, 2019, pp. 1677-1686.

altrimenti conclusi. Invero, essi possono integrare l'una o l'altra fattispecie, a seconda delle applicazioni concretamente prese in esame.

Se si passano in rassegna i requisiti del contratto, secondo il codice civile e nel diritto vivente, non pare che sia necessario superare le categorie consolidate, né inventarne di nuove. L'identificazione delle parti, le tecniche di imputazione della volontà, la conoscenza del contenuto del contratto concluso "per automatico"[35], la forma digitale sono temi già approfonditi dalla dottrina e dalla giurisprudenza e in taluni casi già oggetto di un intervento normativo[36].

In altri termini, con riguardo agli *smart contract*, che come oggi si usa ripetere non sono né *smart* né *contract*, occorre fare uno sforzo di comprensione e di qualificazione del fenomeno, ma non occorrono regole nuove.

Un altro tema di grande rilevanza è quello che ha ad oggetto la verifica della tenuta della recente copiosa normativa in materia di protezione dei dati personali di fronte alle applicazioni di intelligenza artificiale. Com'è noto, il Regolamento europeo, benché recente, è stato pensato prima che il tema che qui ci occupa avesse la diffusione odierna e soprattutto non è stato pensato per i grandi flussi di dati. Applicare la base giuridica del consenso anche al trattamento dei dati personali in applicazioni di *big data* è soluzione inefficace, sia per il titolare del trattamento che si trova a richiedere migliaia di consensi, sia per l'interessato che presta un consenso a trattamenti le cui finalità non possono che essere formulate con un difficile esercizio di acrobatico equilibrio fra genericità, non potendo conoscere tutte le implicazioni delle applicazioni di intelligenza artificiale, e specificità richiesta dalla legge. Il modello appare inadeguato al fenomeno da regolare: ci si concentra sul singolo dato invece che sul flusso dei dati da gestire e da governare[37].

Ancora e senza dubbio occorrerà anche verificare il sistema delle responsabilità, se esso sia idoneo ad accogliere nuove fattispecie relative alla responsabilità dei *robot*. Anzi, alla luce delle conclusioni emerse nell'«*UNIDROIT-UNCITRAL Joint Workshop on smart contracts, artificial intelligence and distributed ledger technology*», questo è uno dei pochi ambiti nei quali è auspicabile un intervento normativo. Infatti, mentre agli *smart contract* sono applicabili, oltre alle norme generali in materia di contratti, anche il *Model Law on Electronic Commerce dell'UNCITRAL*, la *United Nations Convention on the Use of Electronic*

---

[35] Si vuole richiamare qui il famoso articolo di A. Cicu, *Gli automi nel diritto privato*, estratto da *Il Filangieri*, n. 8, Milano, 1901.

[36] Rinvio al mio *Il contratto nell'era dell'intelligenza artificiale*, cit.

[37] Per una più ampia illustrazione della tesi, si rinvia al mio *Intelligenza artificiale e protezione dei dati personali*, cit.

Communications in International Contracts, i *Principles of International Commercial Contracts* dell'*UNIDROIT* e molte direttive europee e, dunque, sarebbe necessario soltanto uno sforzo interpretativo e comunicativo e, eventualmente, di adeguamento del linguaggio[38], invece, con riguardo alle questioni inerenti alla responsabilità, un intervento normativo sostanziale si ritiene necessario[39].

4. La retorica

C'è un sottinteso nei discorsi, anche giuridici, concernenti l'intelligenza artificiale. Il sottinteso è che l'intelligenza artificiale implichi un'entità che esprime l'intelligenza. Se c'è intelligenza, allora c'è un'entità intelligente. Come passaggio successivo della narrazione o del ragionamento, a questa entità è attribuita soggettività.

In altri termini si assume implicitamente che, se c'è un'intelligenza (benché artificiale), ci deve essere un soggetto intelligente (benché artificialmente) da cui quell'intelligenza promana.

A ben vedere, già utilizzare il termine "intelligenza" è condizionante.

L'intelligenza, infatti, si attribuisce all'essere umano o agli animali. Dunque già utilizzare questo termine induce a sviluppare la narrazione in termini antropomorfici.

Si ritiene che se le applicazioni di intelligenza artificiale sono intelligenti, allora c'è un essere umano o un animale a cui l'intelligenza va attribuita.

Le parole utilizzate, come sempre, condizionano il discorso e il ragionamento. Occorre sgombrare invece il campo dai pregiudizi, ritrovare la pagina bianca, per poi interrogarsi sulla soggettività.

---

[38] Ad esempio, l'art. 12 della convenzione delle Nazioni Unite sull'uso delle comunicazioni elettroniche nei contratti internazionali si fa riferimento a «automated message systems», mentre oggi, con riguardo ai sistemi di intelligenza artificiale, sarebbe opportuno riferirsi non soltanto ad «automatico» ma ad «autonomo».

[39] Già con la Risoluzione del 16 febbraio 2017 il Parlamento europeo invitava la Commissione «a proporre un quadro giuridico coerente per lo sviluppo della robotica, compresi i sistemi autonomi e i robot autonomi intelligente». Sulla scorta di tale invito, il 9 marzo 2018 la Commissione europea ha annunciato l'istituzione di un gruppo di esperti sull'intelligenza artificiale che consigli e supporti la Commissione nelle decisioni e iniziative sul tema. In occasione della sua recente risoluzione del 12 febbraio 2019, il Parlamento europeo ha poi ribadito che «le norme e le procedure esistenti dovrebbero essere riviste e, se del caso, modificate in modo tale da tenere conto dell'intelligenza artificiale e della robotica (e che) il quadro europeo per l'IA deve essere sviluppato nel pieno rispetto dei diritti sanciti dalla Carta dei diritti fondamentali e, in particolare, dei principi della protezione dei dati, della vita privata e della sicurezza» (cfr. punti K e L della Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale).

Diversa è la prospettiva se invece si assume con Turing che piuttosto che definire cosa sia l'intelligenza, impresa assai ardua, è opportuno confrontare i risultati di un processo. Se il processo è qualificato intelligente quando è svolto da un essere umano, allora lo si può qualificare intelligente se è svolto da una macchina[40]. Quindi l'intelligenza artificiale può essere definita la scienza di far fare ai computer cose che richiedono intelligenza quando vengono fatte dagli esseri umani[41].

È noto che si sono susseguite molte definizioni di intelligenza artificiale. Basti citare quella contenuta nella già menzionata comunicazione della Commissione europea del 25 aprile 2018, secondo la quale l'espressione «indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»[42].

Appare dunque un metodo meno fuorviante e meno condizionante nell'approccio metodologico, rispetto ad altri metodi spesso adottati senza piena consapevolezza metodologica, e che non induce ad assunzioni implicite di soggettività, quello di confrontare i risultati di due processi: se il primo è qualificato intelligente, la medesima qualificazione si attribuirà anche al secondo.

È utile e anzi necessario sfrondare il discorso dalla retorica che inesorabilmente lo popola. La fattispecie si delinea così in modo neutro e senza "pre-giudizi".

Un conto è affermare che un robot intelligente ha operato in un certo modo, altro è affermare che un *software* basato su un'applicazione di intelligenza artificiale ha prodotto un determinato risultato. Le parole usate e la narrazione scelta possono portare con sé un condizionamento. Basti pensare ai casi in cui cinema e letteratura hanno umanizzato robot e programmi che certamente non avrebbero avuto il medesimo fascino senza nomi, volti e voci sensuali.

---

[40] Si fa riferimento al metodo dell'«*Imitation Game*», elaborato da Alan Turing a cui l'autore dedica il primo paragrafo del suo *Computing Machinery and Intelligence*, in *Mind*, New Series, 1950, v. 59, n. 236, pp. 433-460. Il test è stato ideato da Turing al fine di determinare se una macchina sia in grado di pensare, ossia capace di effettuare collegamenti, concatenare idee e di esprimerle. Il test si basa sulla valutazione delle capacità di un computer di imitare il comportamento di un essere umano: in caso di esito positivo, dovrà ritenersi che la macchina sia in grado di pensare in modo equivalente o, comunque, indistinguibile da un essere umano.

[41] Lo stesso Alan Turing, considerato il padre fondatore della scienza informatica e dell'intelligenza artificiale, affermava «*The idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer*» nel suo *Computing Machinery and Intelligence*, *op. cit.*, p. 436.

[42] Comunicazione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, COM (2018) 237, 25 aprile 2018, p. 1. Un'ulteriore definizione è offerta dal già citato rapporto CEPS in nota 1 del presente contributo che fa riferimento all'intelligenza artificiale come «*the use of man-made techniques (Latin meaning of artificialis) to replicate the ability to "read inside" reality*» (p. 4).

Il termine "intelligenza" o "intelligente" conduce inevitabilmente all'antropomorfizzazione del discorso.

5. Nuove questioni concernenti la responsabilità

Ora, sgombrando il campo dalla retorica, ci troviamo davanti a programmi informatici che svolgono alcune attività per le quali sono stati programmati. Fin qui nulla di nuovo rispetto a ciò che è noto. La responsabilità per il malfunzionamento del programma o per i danni da questo cagionati andrà attribuita, secondo le note regole, all'autore del programma o al produttore, secondo le norme sulla responsabilità civile e sulla responsabilità da prodotto[43]. Non è fuori luogo ricordare che anche in relazione al tema dei danni cagionati dal *software* ebbe luogo un analogo approfondimento dottrinale alcuni anni fa[44], in cui, allora come ora, si indagava chi dovesse rispondere dei danni cagionati dal *software*[45].

Oggi la novità è costituita dalla fattispecie in cui vi sia una certa autonomia decisionale nel programma, o addirittura nel caso in cui ci sia una imprevedibilità nei risultati, quando cioè il metodo utilizzato per raggiungere il risultato non sia deterministico. Sono i casi, ad esempio, delle applicazioni di intelligenza artificiale costituite da modelli di *machine learning* che usano reti neurali e algoritmi di *deep learning*[46], a cui talvolta ci si riferisce come algoritmi "*black box*" che costi-

---

[43] Indaga sulle norme in materia di responsabilità applicabili all'intelligenza artificiale, il volume *Intelligenza artificiale e responsabilità*, a cura di U. Ruffolo, Milano, 2017.

[44] Cfr. G. Alpa, *Responsabilità extracontrattuale ed elaboratore elettronico*, in *Dir. inf.,* 1986, p. 387-393; C. Rossello, *La responsabilità da inadeguato funzionamento di programmi per elaboratore elettronico: aspetti e problemi dell'esperienza nord-americana,* in *Computers e responsabilità civile*, a cura di G. Alpa, Milano, 1985, p. 87-142; J.P. Triaille, *L'applicazione della direttiva comunitaria sulla responsabilità del produttore nel campo del* software, in *Dir. inf.*, 1990, p. 724-735.

[45] In ambito internazionale, già dagli anni '90, l'UNCITRAL, con riferimento alla conclusione automatica dei contratti e dei c.d. «*agenti*», afferma che il principio di imputazione della responsabilità ben possa essere applicato agli «*electronic agent*», anche nel caso in cui questi agiscano non solo in maniera automatica ma anche autonoma, rivelando così di previlegiare un'operazione di chiarificazione ed interpretazione piuttosto che di innovazione normativa. Cfr. *United Nations*, *General Assembly*, *Legal aspects of electronic commerce*, A/CN.9/WG.IV/WP.95, parr. 71-73.

[46] Le diverse tipologie di *Machine Learning* sono illustrate dall'*Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG)*, *30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission,* December 2019, p. 28, che definisce il *Deep Learning* un tipo di *Machine Learning* che utilizza le reti neurali. Anche la Commissione europea, nella già citata Comunicazione *L'intelligenza artificiale per l'Europa*, parla di apprendimento profondo come di «un elemento rivoluzionario per l'intelligenza artificiale, che ha comportato un incredibile miglioramento delle prestazioni per compiti specifici quali il riconoscimento di immagini o vocale o la traduzione

tuiscono una nuova tipologia di rischio anche nel mondo finanziario[47]. Tuttavia, i rischi della *black box* possono essere limitati, secondo il citato report dell'*Expert Group on Regulatory Obstacles to Financial Innovation*, con un approccio che coinvolga contestualmente la rappresentazione della conoscenza, *deep learning*, *machine learning* e *natural language processing*[48].

La complessità può dipendere dal numero di dati che devono essere processati e analizzati e dal modo in cui si creano le connessioni, attraverso le cosiddette reti neurali.

In questo caso, l'autore, il produttore, il venditore, l'utilizzatore del programma e, in generale, i soggetti che beneficiano dell'applicazione non sono in grado di prevederne a priori il risultato.

Si pone, dunque, il problema di attribuire la responsabilità giuridica in caso di danni cagionati dall'applicazione. Se il quesito si pone a legislazione vigente, allora con un necessario sforzo interpretativo si applicheranno le norme in materia di responsabilità civile e responsabilità del produttore[49].

---

automatica. Addestrare un algoritmo di apprendimento profondo a classificare gli oggetti significa fornirgli una grande quantità di esempi etichettati (per esempio immagini) che sono correttamente categorizzati (per esempio immagini di aeroplani). Una volta addestrati, gli algoritmi possono classificare correttamente oggetti che non hanno mai visto, in alcuni casi con una precisione che supera quella umana. Progressi significativi in queste tecnologie sono stati ottenuti mediante l'impiego di grandi set di dati e una potenza di elaborazione senza precedenti» (p. 11), mentre «l'apprendimento automatico, un tipo di IA, opera mediante l'individuazione di modelli a partire dai dati disponibili e la successiva applicazione di questa conoscenza ai dati nuovi. Quanto più è grande il set di dati, tanto più accurata sarà l'individuazione delle relazioni anche impercettibili tra i dati. Quando si tratta di utilizzare l'intelligenza artificiale, gli ambienti ad alto contenuto di dati offrono anche le maggiori opportunità, perché i dati sono il mezzo attraverso il quale l'algoritmo apprende e interagisce con il suo ambiente» (p. 10).

[47] Cfr. il *Report* menzionato in nota n. 42, pp. 11 e 39.

[48] Cfr. il *Report* menzionato in nota n. 42, p. 31. Si usa l'espressione «*perceptual computing*» che implica l'utilizzo di sofisticati sistemi di riconoscimento dell'analisi predittiva: «*In the perceptual computing paradigm, models/algorithms attempt to match incoming digital inputs (and engage associated cognition) with previously labelled digital categories. Predictive models may then be employed, in the form of 'if A, then B'. One use case could be facial recognition or biometric models (e.g. that carry out risk assessments for insurance purpose*» (ancora nel *Report*, pp. 28-29).

[49] Il rapporto tra responsabilità civile e intelligenza artificiale è esaminato approfonditamente all'interno della sezione monografica della rivista *Giurisprudenza italiana* dedicata al tema «Intelligenza artificiale e responsabilità», a cura di U. Ruffolo e di E. Gabrielli. In particolare, si vedano i contributi di M. Costanza, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, p. 1686-1689, che individua la responsabilità in capo al soggetto più vicino al fatto lesivo causato dall'applicazione di intelligenza artificiale, toccando un tema ampiamente approfondito anche da M. Franzoni, *La "vicinanza della prova", quindi..*, in *questa rivista*, 2016, p. 360 ss.; di U. Ruffolo, *Intelligenza artificiale,* machine learning *e responsabilità da algoritmo,* p. 1689-1704, che vaglia le possibilità di individuazione e qua-

Se invece la ricerca si svolge cercando di definire nuove norme e nuovi modelli, occorre innanzitutto dare conto che vi è chi propone di riconoscere una soggettività giuridica al programma e conseguentemente attribuire ad esso una responsabilità[50]. Questa possibilità è menzionata anche nella Risoluzione del Parlamento europeo del 16 febbraio 2017, ove si invita la Commissione europea a valutare «l'istituzione di uno *status* giuridico specifico per i *robot* nel lungo

---

lificazione della responsabilità da intelligenza artificiale alla luce del Codice civile, esaminando altresì le ipotesi di riconoscimento di personalità giuridica; di M. Gambini, *Algoritmi e sicurezza*, p. 1726-1740, che affronta il tema della sicurezza nel settore dell'intelligenza artificiale esaminando le soluzioni già esistenti e adottate nell'ambito dei servizi della società dell'informazione e dei trattamenti automatizzati di dati personali. Con particolare riferimento al tema della responsabilità civile delle c.d. *autonomous car*, si rinvia ad E. Al Mureden, Autonomous cars *e responsabilità civile tra disciplina vigente e prospettive* de iure condendo, in *questa rivista*, 2019, p. 895-924.
Approfondisce il tema della responsabilità derivante dalle applicazioni di sistemi di intelligenza artificiale anche il libro curato da F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018 e in particolare il contributo di M. Bassini, L. Liguori e O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability. *Verso nuovi paradigmi?*, p. 333-371, nel quale gli autori offrono una panoramica dei diversi orientamenti espressi da dottrina e giurisprudenza in relazione al tema della responsabilità civile e penale derivante da eventuali danni causati da sistemi di intelligenza artificiale; A. Massolo, *Responsabilità civile e IA*, p. 373-382, valuta invece l'idoneità del quadro giuridico nazionale ed europeo a regolare i rapporti civili nell'era dell'intelligenza artificiale.
Per una rassegna delle problematiche sollevate, v. anche il volume curato da A. De Franceschi e R. Schulze, *Digital Revolution. New challenges for Law,* C.H.Beck-Nomos, 2019, e in particolare i contributi di G. Mazzini, *A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law*, p. 245-298, e di F. Mezzanotte, *Risk Allocation and Liability Regimes in the IoT*, p. 169-189; O. Rachum Twaig, *Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots*, in *University of Illinois Law Review*, vol. 2020; R. Weber, D.N. Staiger, *New Liability Patterns in the Digital Era*, in *EU Internet Law*, a cura di T.E. Synodinou, P. Jougleux, C. Markou, T. Prastitou, Springer, 2017, p. 197-214.

[50] Sul tema del riconoscimento della personalità giuridica, A. Bertolini, G. Aiello, *Robot companions: A legal and ethical analysis*, in *Information Society*, 2018, 34, 1, p. 130-140; A. Bertolini, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, Innovation and Technology*, 2013, 1, p. 214-247; U. Pagallo, *The Laws of Robots,* Springer, 2013; G. Sartor, *Cognitive automata and the law: electronic contracting and the intentionally of software agents*, in *Artificial Intelligence Law*, 2009, p. 253-290; G. Teubner, *Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law*, in *Journal of Law and Society*, 33, 2016, 33, p. 497-521. G. Teubner approfondisce il tema nel recente volume *Soggetti giuridici digitali? Sullo status privatistico degli agenti software*, Napoli, 2019. In senso contrario, invece, L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, IV/2018, p. 713-739; S. Toffoletto, *IoT e intelligenza artificiale: le nuove frontiere della responsabilità civile (e del risarcimento)*, note a margine del convegno «Intelligenza artificiale e primi profili applicativi: Giustizia, IoT e Lavoratori» (Aula Magna del Palazzo di Giustizia di Milano, 17 aprile 2018). Cfr. anche il mio contributo, *La conclusione del contratto telematico mediante i* "software agents": *un falso problema giuridico? Brevi considerazioni*, in *questa rivista*, 2002, p. 500-509.

termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi»[51].

Tuttavia, questa soluzione è, a ben vedere, una soluzione solo apparente la quale cede al fascino retorico della soggettività delle applicazioni di intelligenza artificiale, senza in realtà giungere ad una soluzione compiuta del problema. Infatti, se pure fosse riconosciuta all'applicazione una soggettività giuridica, nel caso in cui l'applicazione fosse ritenuta responsabile, occorrerebbe comunque risolvere il problema del risarcimento del danno cagionato. Il programma di intelligenza artificiale non avrebbe, infatti, un patrimonio di cui poter disporre con il quale risarcire il danno. Rimarrebbe dunque non risolto il problema del risarcimento.

Si obietta che si potrebbe costituire un patrimonio da riservare all'applicazione di intelligenza artificiale, proprio allo scopo di consentire il risarcimento del danno[52]. Tuttavia, se si vuole preservare un patrimonio a questo scopo, non è necessario costruire il complesso edificio della soggettività del programma. Si può comunque costituire un patrimonio riservato al risarcimento di queste tipologie di danni.

A differenza di quanto accadde per la persona giuridica[53], in questo caso sembra che si tratti di una costruzione che aumenti la complessità giuridica piuttosto che diminuirla[54]. Soprattutto l'attribuzione della soggettività all'applicazione di intelligenza artificiale non risolve il problema più complesso: quello di indi-

---

[51] Cfr. punto 59, lett. *f)* della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103 (INL).

[52] Cfr. U. Pagallo, *Robotrust and Legal Responsibility*, in *Know Techn Pol,* vol. 23, 2010, p. 367-379; G. Sartor, *Gli agenti* software*: nuovi soggetti del ciberdiritto?*, in *questa rivista*, 2002, p. 465-499.

[53] Cfr. F. Galgano, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010, il quale attribuisce alla metafora il ruolo di semplificazione linguistica della complessità dei rapporti giuridici e, citando a sua volta F. D'Alessandro, *Persone giuridiche e analisi del linguaggio*, Padova, 1989, p. 70 ss., afferma: «la persona giuridica è, pertanto, un'entità "rilevabile solo sulla scena giuridica verbalizzata", mentre "sulla scena effettuale o esistenziale non v'è che un soggetto di diritto: l'uomo". Ma, individuato l'ambito entro il quale il concetto di persona giuridica assolve la propria funzione, non si può fare a meno di apprezzare il valore di questo concetto, che nessuna parafrasi – "per quanto complessa e ingegnosa" – potrebbe sostituire; a esso si deve guardare, anzi, come una a una "ammirevole creazione originale del linguaggio giuridico"» (p. 49).

[54] Cfr. F. Di Giovanni, *op. cit*.

viduazione dei criteri di allocazione della responsabilità. Questo, infatti, sembra essere il nodo della questione.

A conclusione del seminario Unidroit-Uncitral già richiamato, si è convenuto sulla necessità di elaborare un nuovo modello di responsabilità. Il nuovo modello di responsabilità dovrebbe completamente affrancarsi da condizionamenti di natura soggettiva[55].

Fuorviante e poco efficace è tentare di applicare categorie e criteri di natura soggettiva, quali il dolo o la colpa, all'applicazione informatica cui si sarebbe attribuita la soggettività.

Se invece si tratta di attribuire una responsabilità oggettiva, senza dolo e senza colpa, allora la soggettività dell'applicazione di intelligenza artificiale è inutile. Qualcuno risponderà indipendentemente dalla soggettività del programma. Ancora una volta, occorre fermarsi davanti all'illusione della facile soluzione del problema.

Se si vuole costruire un nuovo modello normativo altrettanto poco utile sembra addirittura essere la ricerca dell'errore, sotto il profilo giuridico. La ricerca dell'errore *ex post*, indubbiamente utile per chi sviluppa i programmi informatici, è assai dispendiosa e non sempre percorribile con successo, se si tratta di applicazioni che operano in modo non deterministico. Dunque il nuovo modello di responsabilità dovrebbe essere caratterizzato dall'essere la responsabilità oggettiva e collettiva, ripartita su più soggetti, indipendentemente dalla infruttuosa e dispendiosa ricerca dell'errore. Dovrebbe trattarsi di un modello di allocazione del rischio.

Un principio che può rivelarsi di grande utilità è quello basato *sull'accountability*[56], cioè sulla responsabilizzazione del soggetto che trae vantaggio dall'applicazione di intelligenza artificiale. Utilizzando questo criterio, il soggetto che trae maggior vantaggio risponde adottando esso stesso le misure necessarie ad evitare il rischio. Si pone, dunque, sul soggetto più vicino al rischio l'onere di adottare le misure per evitarlo e di dimostrare in che modo si è adoperato per evitarlo.

---

[55] Pure presenti nell'elaborazione della Risoluzione del Parlamento europeo del febbraio 2017 che, come osserva U. Ruffolo, *Per i fondamenti di un diritto alla robotica* self-learning*: dalla* machinery *produttiva all'auto* driverless*: verso una "responsabilità da algoritmo"?*, in *Intelligenza artificiale e responsabilità*, a cura di U. Ruffolo, Milano, 2017, pp. 11-12: «pare non affrancarsi del tutto da una certa centralità dell'elemento soggettivo colposo come criterio di attribuzione della responsabilità per lesioni cagionate da robot *self-learning*».

[56] Cfr. M. Costanza, *op. cit.*, p. 1689; Comandé, *Intelligenza artificiale e responsabilità tra* liability *e* accountability, in *Analisi giuridica dell'economia*, 2019, I, p. 169-188. Sul punto v. anche il mio contributo, *L'*accountability *nel Regolamento europeo,* in *Commentario del Codice Civile delle persone*, a cura di A. Barba e S. Pagliantini, Torino, 2019.

Se si ragiona di nuovi modelli normativi è opportuno allora dirigersi verso un modello di responsabilità che sia un sistema puro di allocazione del rischio, prescindendo dalla ricerca dell'errore[57], e ripartendo i costi sui soggetti che sono parte dell'operazione economica, in modo collettivo[58], eventualmente prospettando la costituzione di un fondo ovvero la formulazione di meccanismi di assicurazione in capo ai soggetti che potrebbero essere chiamati a risarcire il danno.

[57] In favore di un regime di "*strict liability*" è D.C. Vladeck, *Machines without Principals: Liability Rules and Artificial Intelligence*, in *Wash. L. Rev.*, vol. 89/117, 2014, p. 117-150, il quale tuttavia propende per la creazione della soggettività pura delle applicazioni autonome.

[58] Per approfondimenti sulla responsabilità dell'organizzazione nel suo complesso, con riguardo al compimento di atti informatici, si rinvia al mio volume, *I contratti informatici,* in *Tratt. dir. comm. e dir. pubbl. econ.*, diretto da Galgano, XXII, Padova, 1997, in particolare p. 187 ss. Già G. Calabresi parlava di «*enterprise liability*» nel suo *Some Thoughts on Risk Distribution and the Law of Torts*, in *Yale Law Journal*, 1961, p. 449-553.

Pasquale Serrao d'Aquino

Responsabilità civile e IA. La posizione dell'Unione Europea

1. Le diverse iniziative delle istituzioni europee sull'intelligenza artificiale

Le istituzioni europee hanno individuato l'Intelligenza Artificiale come una priorità dell'agenda politica, adottando un intenso programma di azione sul tema dell'intelligenza artificiale, evidenziando i vantaggi: dei cittadini ad esempio ad una migliore assistenza sanitaria (E-Health) e a servizi pubblici migliori; delle imprese ad avvalersi di nuove generazioni di prodotti e servizi, dei servizi di interesse pubblico alla riduzione dei costi di fornitura, migliorando la sostenibilità dei prodotti e dotando le forze dell'ordine di strumenti appropriati per garantire la sicurezza[1], con adeguate garanzie quanto al rispetto dei loro diritti e delle loro libertà. Inoltre, tecnologie digitali come l'IA risultano fondamentali per conseguire gli obiettivi del Green Deal europeo, dedicato alle sfide legate al clima e all'ambiente, nonché risultano utili al sostegno al processo democratico e ai diritti sociali.[2]

---

[1] Il Libro Bianco "sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia"(Commissione Europea, COM (2020) 65 final, 16 febbraio 2020, Libro bianco sull'intelligenza artificiale – Un approccio europea all'eccellenza e alla fiducia.) che, sul punto indica come «*Gli strumenti di IA possono costituire un'opportunità per migliorare la protezione dei cittadini dell'UE dalla criminalità e dagli atti di terrorismo. Tali strumenti potrebbero, ad esempio, contribuire a individuare la propaganda terroristica online, scoprire transazioni sospette nelle vendite di prodotti pericolosi, individuare oggetti pericolosi o sostanze o prodotti illeciti nascosti, offrire assistenza ai cittadini in situazioni di emergenza e contribuire a guidare il personale di primo intervento.*»

[2] Libro Bianco, cit.

La Commissione, quindi, adotta un approccio normativo orientato agli investimenti «*con il duplice obiettivo di promuovere l'adozione dell'IA e di affrontare i rischi associati a determinati utilizzi di questa nuova tecnologia*.»

Il 16 febbraio 2017 il PE ha approvato una Risoluzione di raccomandazioni alla Commissione "*concernenti norme di diritto civile sulla robotica*"[3], al quale è seguita la Comunicazione del 25 aprile 2018 "*L'intelligenza artificiale per l'Europa*" con la quale ha definito una strategia per l'IA[4] che affronta gli aspetti socioeconomici parallelamente a un aumento degli investimenti nella ricerca, nell'innovazione e nelle capacità di IA in tutta l'UE, e ha concordato con gli Stati membri un piano coordinato[5] per l'allineamento delle strategie. Con tale Comunicazione[6] la Commissione accoglie con favore i sette requisiti fondamentali individuati negli orientamenti del gruppo di esperti ad alto livello: intervento e sorveglianza umani; robustezza tecnica e sicurezza; riservatezza e governance dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale e ambientale e accountability.

La Commissione ha inoltre istituito un gruppo di esperti ad alto livello che, nell'aprile 2019, ha pubblicato orientamenti per un'IA affidabile.[7]

Sono stati elaborati anche principi etici[8] – le *Ethics Guidelines*[9] Di rilievo è anche la redazione a Strasburgo, il 3 dicembre 2018, della *European Ethical Charter*

---

[3] Risoluzione del Parlamento europeo del 16.2.2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2013 (INL)).

[4] COM (2018) 237 final.

[5] COM (2018) 795 final.

[6] COM (2019) 168 final.

[7] Nel maggio 2019 è stato pubblicato un Report di un gruppo di esperti, i cui risultati sono stati ripresi nel febbraio 2020 nella Relazione della stessa Commissione "sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità" (Commissione Europea, COM (2020) 64 final, 16 febbraio 2020, Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità), allegato al Libro Bianco "sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia" (Commissione Europea, COM (2020) 65 final, 16 febbraio 2020, Libro bianco sull'intelligenza artificiale – Un approccio europea all'eccellenza e alla fiducia.

[8] L'intelligenza artificiale, per essere affidabile, deve possedere tre requisiti: la legittimità, la moralità, la solidità. Mentre le Linee Guida non si occupano del primo profilo, che è affidato alle fonti primarie e secondarie dell'Unione europea, alla Convenzione europea sui diritti umani, alla disciplina dei singoli Stati ove già si prevedono regole sull'impiego della intelligenza artificiale, più articolata è l'analisi della moralità e della solidità. Le radici degli aspetti etici sono ancora una volta rinvenute nei diritti fondamentali, e sono espresse in quattro direttrici: il rispetto dell'autonomia umana, la prevenzione del danno, la correttezza, la comprensibilità (*explicability*). G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contratto e Impr.*, 2021, 4, 1003.

[9] Definiti dalla Commissione, e condivisi dal Parlamento, emerge dalla ricerca degli esperti pubblicata nell'aprile del 2019 (*Independent High-Level Group on Artificial Intelligence set up by the European Commission, Ethics Guidelines for Trustworthy AI*, Brussels, 8 april 2019).

on the Use of Artificial Intelligence in Judicial Systems and their Environment, adottata dalla Commissione europea per l'efficienza dei sistemi di giustizia (CEPEJ) che rileva l'esigenza di preservare la tutela dei diritti fondamentali, prevede la lotta alla discriminazione e il ricorso a criteri di trasparenza ed equità delle decisioni assunte con l'impiego delle nuove tecnologie, enucleando i seguenti principi: principio del rispetto dei diritti fondamentali, volto ad assicurare l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali; principio di non-discriminazione, volto a prevenire specificamente lo sviluppo o l'intensificazione di discriminazioni tra persone o gruppi di persone; principio di qualità e sicurezza, in ordine al trattamento di decisioni e dati giudiziari, utilizzare fonti certificate e dati intangibili con modelli elaborati multidisciplinarmente, in un ambiente tecnologico sicuro; principio di trasparenza, imparzialità ed equità, per rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne; principio "del controllo da parte dell'utilizzatore", al fine di precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte.

Una definizione di intelligenza artificiale è contenuta nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni. "L'intelligenza artificiale per l'Europa" [COM (2018) 237 final]: secondo la quale con tale espressione di indicano "*sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*". Essi possono consistere in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose).

2. La proposta di Regolamento di regole armonizzate sull'intelligenza artificiale

La proposta di regolamento di armonizzazione, definisce come "sistema di intelligenza artificiale" (sistema di IA) il «*software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*» (art. 1).

Dopo diversi atti intermedi, il 20 ottobre 2020 il PE ha approvato tre risoluzioni e due proposte di *regolamento su etica, responsabilità e proprietà intellettuale*[10] dei sistemi di IA.

Una quarta risoluzione , invece, ha avuto luce il 20 gennaio 2021 e tratta del delicato tema dei sistemi autonomi di armi letali (*lethal autonoums weapon system*), i robot assassini, con la quale chiede alla Commissione l'adozione di una strategia volta a proibire i "*sistemi d'arma se non soggetti al controllo umano*".

Il 21 aprile 2021, è stata altresì adottata la Proposta di Regolamento del Parlamento europeo e del Consiglio che dovrebbe succedere alla Direttiva macchine, che si applica anche ai robot.[11] Alle macchine dovranno infatti applicarsi, coordinandosi sia il Nuovo Regolamento Macchine 2021 sia il cd. Regolamento IA.

Contestualmente è stato approvata il 21 aprile 2021 la Proposta di regolamento COM (2021) 206[12] che reca una serie di norme armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio, così come restrizioni in relazione a determinati usi, tra i quali in particolare i sistemi di identificazione biometrica remota. Essa detta: a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione; b) il divieto di determinate pratiche di intelligenza artificiale; c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; d) regole di trasparenza armonizzate

---

[10] Quanto ai diritti di proprietà intellettuale, il Parlamento, invece, ha sottolineato l'importanza di un sistema efficace per l'ulteriore sviluppo dell'intelligenza artificiale, compresa la questione dei brevetti e dei nuovi processi creativi indicando, tra le questioni da risolvere, quelle della tutela e della titolarità della proprietà intellettuale di quanto interamente sviluppato dall'intelligenza artificiale assegnando la loro titolarità alla persona umana (e non alla IA, alla quale è negata la personalità giuridica) e distinguendo, inoltre, tra le creazioni umane ottenute con l'assistenza dell'intelligenza artificiale e quelle generate autonomamente dall'IA.

[11] La Direttiva 2006/42/CE definisce un quadro normativo armonizzato per l'immissione delle macchine sul mercato unico, garantendone la libera circolazione nell'Unione e un livello elevato di protezione per gli utilizzatori e le persone esposte e che si applica anche ai robot. Oltre alle macchine in senso stretto, il campo di applicazione comprende altri prodotti correlati, come i componenti di sicurezza e le quasi-macchine.

[12] La scelta di adottare un regolamento, come indica la Relazione, è giustificata dalla necessità di un'applicazione uniforme delle nuove regole, come la definizione di IA, il divieto di talune pratiche dannose consentite dall'IA e la classificazione di taluni sistemi di IA. L'applicabilità diretta di un regolamento, conformemente all'articolo 288 TFUE, ridurrà la frammentazione giuridica e faciliterà lo sviluppo di un mercato unico per sistemi di IA leciti, sicuri e affidabili. Tale obiettivo sarà conseguito in particolare introducendo una serie armonizzata di requisiti di base per quanto concerne i sistemi di IA classificati come ad alto rischio e di obblighi riguardanti fornitori e utenti di tali sistemi, migliorando la tutela dei diritti fondamentali e garantendo certezza del diritto tanto per gli operatori quanto per i consumatori.

per i sistemi di IA destinati a interagire con le persone fisiche, i sistemi di riconoscimento delle emozioni, i sistemi di categorizzazione biometrica e i sistemi di IA utilizzati per generare o manipolare immagini o contenuti audio o video; e) regole in materia di monitoraggio e vigilanza del mercato (cfr. art. 1).

2.1. Questioni e criticità correlate all'uso dell'IA nella proposta di regolamento

La Commissione europea, con le iniziative indicate e, soprattutto, con la proposta di regolamento COM (2021) 206 ha indicato una serie di rischi specifici potenzialmente elevati per la sicurezza e i diritti fondamentali posti dall'impiego dell'IA, di fronte ai quali il diritto vigente dell'UE è considerato inadeguato, se non del tutto inapplicabile.

La Commissione europea li ha individuati, ad esempio, nel fatto che spesso non sia possibile stabilire il motivo per cui un sistema di IA è giunto a un risultato specifico (opacità del processo che porta dall'elaborazione dell'input dei dati all'output), determinando una serie di difficoltà nel valutare e dimostrare se qualcuno è stato ingiustamente svantaggiato dall'uso di sistemi di IA, ad esempio nel contesto di una decisione di assunzione o di promozione oppure di una domanda di prestazioni pubbliche. Particolare attenzione, inoltre, è stata prestata ai sistemi di riconoscimento facciale negli spazi pubblici, i quali, in assenza di una disciplina adeguata, possono essere invasivi della vita privata. Altre criticità riguardano i casi di scarso addestramento o una cattiva progettazione del sistema di IA, con ciò causando errori significativi in grado di discriminare le persone, in particolare nei processi applicati alle dinamiche del mercato del lavoro, al settore del credito, nei procedimenti penali, causando ineguaglianze ad esempio sul piano dell'etnia, del genere, e dell'età o essere comunque invasivi della vita privata.[13]

---

[13] Ad esempio, la Commissione europea ha sottolineato come la sottorappresentazione di alcuni gruppi sociali nel processo di immissione dei dati in un sistema di IA possa generare discriminazioni sugli studi clinici (se caratterizzati dall'inclusione di un numero maggiore di dati provenienti da uomini), con l'effetto di generare conclusioni errate e conseguenze negative in ordine al trattamento del sesso femminile. Nello stesso senso, un esempio frequentemente citato dalle Istituzioni europee, quello concernente sistemi di intelligenza artificiale utilizzati nella gestione delle risorse umane nel mondo del lavoro che, in base a dati contenenti distorsioni storiche impiegati per adottare una decisione, hanno finito per favorire assunzioni o promozioni maschili rispetto a quelle femminili.
La Commissione ricorda anche il tema dei rischi per l'ordinato svolgimento del dibattito pubblico determinati dall'uso dell'intelligenza artificiale nel contesto dell'informazione; è il caso per esempio dell'IA in grado di creare *bolle in rete* in cui i contenuti sono presentati in base ai dati con cui l'utente ha interagito in passato, con l'effetto di impedire la tutela di un ambiente aperto a un dibattito pluralistico, inclusivo e accessibile. L'IA può essere infine usata per creare immagini, video e audio falsi ma estremamente realistici, noti come *deepfake*, in grado di truffare, pregiudicare la reputazione e mettere in dubbio la fiducia nei processi decisionali, con il rischio che in definitiva si crei un processo di polarizzazione del dibattito pubblico e di manipolazione delle elezioni.

La nuova disciplina della proposta di regolamento di armonizzazione mira a ridurre al minimo i rischi per la sicurezza e i diritti fondamentali che potrebbero essere generati dai sistemi di IA prima della loro immissione sul mercato dell'UE. Si pensi, appunto, ai sistemi di riconoscimento delle emozioni, biometrici (in tempo reale, a posteriori, remota) che sono indicati nella proposta.

A tal fine, l'approccio della Commissione si basa su una "piramide di rischio" ascendente (che va dal rischio basso/medio a quello elevato, fino al rischio inaccettabile) per classificare, nell'ambito dell'IA, una serie di casi di pratiche generali e di impieghi specifici in determinati settori, cui la Commissione ricollega rispettive misure di attenuazione, o addirittura i divieti di alcune pratiche di IA.[14]

Tali divieti riguardano una serie limitata di utilizzi dell'IA ritenuti incompatibili con i valori dell'Unione europea, in particolare quelli che si sostanziano nei diritti fondamentali contenuti nella Carta europea. Si tratta in particolare di divieti concernenti i sistemi di IA che distorcono il comportamento di una persona attraverso tecniche subliminali o sfruttando vulnerabilità specifiche in modi che causano o sono suscettibili di causare danni fisici o psicologici; divieti concernenti l'attribuzione di un punteggio sociale (*social scoring*) con finalità generali mediante sistemi di IA da parte di autorità pubbliche.[15]

---

[14] Dossier n° 57 – della Camera del 12 novembre 2021 "Legge sull'intelligenza artificiale.

[15] Art. 5: Sono vietate le pratiche di intelligenza artificiale seguenti:
a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;
b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;
c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari:
i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;
ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

Il regime specifico di divieto si estende a determinati sistemi di identificazione biometrica remota (ad esempio strumenti di riconoscimento facciale per controllare i passanti in spazi pubblici), salvo casi eccezionalmente autorizzati dalla legge riconducibili in linea di massima ad attività di prevenzione e contrasto del crimine, in ogni caso soggetti a garanzie specifiche.

Una seconda categoria di sistemi di IA, pur consentiti ma classificati ad alto rischio, deve rispettare un insieme di requisiti specificamente progettati, che comprendono l'utilizzo di set di dati di alta qualità, l'istituzione di una documentazione adeguata per migliorare la tracciabilità, la condivisione di informazioni adeguate con l'utente, la progettazione e l'attuazione di misure adeguate di sorveglianza umana e il conseguimento degli standard più elevati in termini di robustezza, sicurezza, cibersicurezza e precisione. La proposta delinea un sistema di valutazione di conformità dei sistemi di IA ad alto rischio a tali requisiti, attivato prima che vengano immessi sul mercato o messi in servizio.

I sistemi di IA sono considerati ad alto rischio o perché specificamente individuati nell'Allegato III alla proposta di Regolamento[16] oppure, anche se estraneo

---

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:
i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;
ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro.

[16] ALLEGATO III SISTEMI DI IA AD ALTO RISCHIO DI CUI ALL'ARTICOLO 6, PARAGRAFO 2:
I sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, sono i sistemi di IA elencati in uno dei settori indicati di seguito.
1. Identificazione e categorizzazione biometrica delle persone fisiche:
a) i sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota "in tempo reale" e "a posteriori" delle persone fisiche.
2. Gestione e funzionamento delle infrastrutture critiche:
a) i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione del traffico stradale e nella fornitura di acqua, gas, riscaldamento ed elettricità.
3. Istruzione e formazione professionale:
a) i sistemi di IA destinati a essere utilizzati al fine di determinare l'accesso o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale;
b) i sistemi di IA destinati a essere utilizzati per valutare gli studenti negli istituti di istruzione e formazione professionale e per valutare i partecipanti alle prove solitamente richieste per l'ammissione agli istituti di istruzione.

all'elenco, congiuntivamente, (a) è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; (b) è soggetto a una valutazione della conformità prevista dalla normativa di armonizzazione dell'Unione elencata nell'allegato II.» (art. 6)

---

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:
a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove;
b) l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro.
5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi:
a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;
b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA messi in servizio per uso proprio da fornitori di piccole dimensioni;
c) i sistemi di IA destinati a essere utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi vigili del fuoco e assistenza medica.
6. Attività di contrasto:
a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali dei rischi delle persone fisiche al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati;
b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;
c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per individuare i "deep fake" di cui all'articolo 52, paragrafo 3;
d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;
e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;
f) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati;
g) i sistemi di IA destinati a essere utilizzati per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in set di dati complessi, correlati e non correlati, resi disponibili da fonti di dati diverse o in formati diversi, al fine di individuare modelli sconosciuti o scoprire relazioni nascoste nei dati.

Per integrarsi agevolmente con i quadri giuridici esistenti la proposta tiene conto, ove opportuno, delle regole settoriali per la sicurezza, assicurando la coerenza tra gli atti giuridici e la semplificazione per gli operatori economici.

Allo scopo di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, a proposta si conforma per i sistemi ad alto rischio al principio dell'*under human control*, prevedendo la "*Sorveglianza umana*": «1. *I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso*.» (art. 14, par. 1).

Per una serie di sistemi di IA considerati a basso rischio sono previsti soltanto requisiti minimi di trasparenza: è il caso di *chatbot* (programmi in grado di simulare conversazioni umane), sistemi di riconoscimento delle emozioni o "*deep fake*" (foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali, riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce).

Sono previste norme per promuovere il ricorso a spazi di sperimentazione normativa, che creano un ambiente controllato per testare tecnologie innovative per un periodo limitato, e l'accesso ai poli dell'innovazione digitale e a strutture di prova e sperimentazione, con l'obiettivo di sostenere le imprese innovative, le PMI e le *start-up*.

---

7. Gestione della migrazione, dell'asilo e del controllo delle frontiere:
a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;
b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per valutare un rischio (compresi un rischio per la sicurezza, un rischio di immigrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;
c) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per verificare l'autenticità dei documenti di viaggio e dei documenti giustificativi delle persone fisiche e per individuare i documenti non autentici mediante il controllo delle caratteristiche di sicurezza;
d) i sistemi di IA destinati ad assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status.
8. Amministrazione della giustizia e processi democratici:
a) i sistemi di IA destinati ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti.

3. La responsabilità civile derivante dall'utilizzo di sistemi di IA

Alla responsabilità civile è dedicata specificamente la Risoluzione del 20 ottobre 2020 "*raccomandazioni alla Commissione sul regime di responsabilità civile e intelligenza artificiale*", la quale evidenzia come con l'espressione IA si intendano tecnologie avanzate che incidono in quasi tutti i settori della vita sociale ed economica (trasporti, istruzione personalizzata, assistenza alle persone fragili, programmi di fitness, concessione di credito), all'ambiente di lavoro (alleggerimento di attività faticose e ripetitive), fino alle sfide globali (cambiamenti climatici, assistenza sanitaria, nutrizione, logistica) e che, nella sua stesura finale – se avrà luogo – dovrà essere coordinata con la proposta di armonizzazione.

La disciplina della "responsabilità" dell'IA svolge un duplice ruolo: garantisce il diritto al risarcimento della vittima di un danno e, al contempo, fornisce un incentivo alle persone fisiche e giuridiche affinché evitino sin dall'inizio di causare danni o pregiudizi, nonché quantifica il risarcimento dovuto per i loro comportamenti.

Al tempo stesso, il PE in tale atto si dichiara consapevole del fatto che l'utilizzo di sistemi di IA potrebbe causare danni gravi, come compromettere la dignità umana e i valori e le libertà europei, tracciando gli spostamenti delle persone contro la loro volontà, introducendo sistemi di credito sociale, prendendo decisioni di parte riguardanti assicurazioni sanitarie, concessioni di crediti, ordinanze giudiziarie o decisioni in materia di assunzione o di impiego o, ancora, costruendo sistemi d'arma autonomi letali (considerando 3 della proposta di regolamento).

Anche in tale atto si mette in evidenza la necessità di una incentivazione dell'IA in ragione dei vantaggi della diffusione dei sistemi di IA che aiuteranno a contrastare più efficacemente i cambiamenti climatici, a migliorare le visite mediche e le condizioni di lavoro, a migliorare l'integrazione delle persone con disabilità e degli anziani nella società e a fornire corsi di istruzione su misura a tutte le tipologie di studenti (considerando 4 della proposta di reg.)

Il quadro giuridico in materia di responsabilità civile, pertanto, deve «*infondere fiducia nella sicurezza, nell'affidabilità e nella coerenza di prodotti e servizi, compresa la tecnologia digitale*» (punto B della Risoluzione), garantendo e la certezza del diritto per tutte le parti, del produttore, dell'operatore, della persona interessata o di terzi.

Si è esclusa l'opzione radicale di attribuire la personalità giuridica ai sistemi di IA[17], ipotesi teorizzata da alcuni studiosi anglosassoni e, comunque, a mio av-

[17] Su proposta della Commissione Giuridica (27 aprile 2020), il Parlamento Europeo ha presentato il 20 ottobre 2020 una Risoluzione recante raccomandazioni alla Commissione su un regime di responsabilità civile sull'intelligenza artificiale (2020/2014 (INL)), in cui abbandona la tesi della soggettività, reputata non necessaria, e accoglie l'impostazione della Commissione.

viso, non impossibile sul piano giuridico-concettuale (per la personalità attribuita agli enti e, in una certa misura, per il riconoscimento di patrimoni separati), ma fortemente inopportuna per l'innescarsi di problemi eticamente e politicamente drammatici, connessi all'inevitabile riconoscimento anche di poteri e di diritti dell'IA. Ferma restando, quindi, la responsabilità in capo a persone fisiche o enti, la Risoluzione del PE individua nelle diverse ipotesi i soggetti responsabili; distingue le diverse tipologie di sistemi di IA; ne differenzia il regime di responsabilità; regola gli obblighi assicurativi, il diritto alla prova e il regime della prescrizione delle azioni risarcitorie delle vittime.

Il regolamento è destinato ad applicarsi nel territorio dell'Unione dove un'attività, dispositivo o processo virtuale o fisico guidato da un sistema di IA abbia arrecato un danno o un pregiudizio alla vita, alla salute, all'integrità fisica di una persona fisica, al patrimonio di una persona fisica o giuridica o abbia arrecato un danno non patrimoniale rilevante risultante in una perdita economica verificabile (art. 1).

Le norme del regolamento sono inderogabili per cui qualsiasi *contratto* tra l'operatore di un sistema di IA e una persona fisica o giuridica vittima di un danno o pregiudizio a causa di un sistema di IA che eluda o limiti i diritti e gli obblighi sanciti dal regolamento (stipulato tanto prima tanto dopo che il danno o il pregiudizio si sia verificato), è *nullo* per quanto riguarda i diritti e gli obblighi sanciti dal regolamento.

La tutela prevista dal regolamento è, in ogni caso, aggiuntiva rispetto a quella derivante dalle condizioni contrattuali o da altre norme: «*Il presente regolamento fa salve le eventuali ulteriori azioni per responsabilità derivanti da rapporti contrattuali nonché da normative in materia di responsabilità per danno da prodotti difettosi, protezione del consumatore, anti-discriminazione, lavoro e tutela ambientale tra l'operatore e la persona fisica o giuridica vittima di un danno o pregiudizio a causa del sistema di IA, e per il quale può essere presentato ricorso contro l'operatore a norma del diritto dell'Unione o nazionale.*» (art. 2, comma 3).

L'art. 3 della proposta di regolamento, che si compone di complessivi 14 articoli, contiene una serie definizioni, oggettive e soggettive: è "*sistema di intelligenza artificiale (IA)*" il sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici; è "*autonomo*" il sistema basato sull'intelligenza artificiale che opera interpretando determinati dati forniti, e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione; un sistema di IA che opera in modo autonomo è ad "*alto rischio*" quando sussiste un potenziale si-

gnificativo di causare danni o pregiudizi a una o più persone in modo casuale, e che va oltre a quanto ci si possa ragionevolmente aspettare; l'importanza del potenziale dipende dall'interazione dei vari possibili danni o pregiudizi, dal grado di autonomia decisionale, dalla probabilità che il rischio si concretizzi e dalla modalità e dal contesto di utilizzo del sistema di IA.

4. L'applicazione congiunta della direttiva sulla responsabilità per prodotto difettoso e di nuove regole specifiche per la responsabilità dell'IA

La Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità che accompagna il Libro bianco analizza il quadro giuridico pertinente, individuando le incertezze riguardanti l'applicazione di tale quadro giuridico in relazione ai rischi specifici derivanti dai sistemi di IA e da altre tecnologie digitali.

La conclusione è che la legislazione vigente in materia di sicurezza dei prodotti sostiene già un concetto ampio di sicurezza, con l'obiettivo di proteggere da tutti i tipi di rischi derivanti dal prodotto in funzione dell'uso dello stesso.

Per garantire una maggiore certezza del diritto tale Relazione suggerisce che si potrebbero tuttavia introdurre disposizioni che contemplino esplicitamente i nuovi rischi derivanti dalle tecnologie digitali emergenti:

- Il comportamento autonomo che mostrano alcuni sistemi di IA durante il loro ciclo di vita può comportare modifiche significative dei prodotti, che a loro volta hanno ripercussioni sulla sicurezza e possono rendere necessaria una nuova valutazione dei rischi. Potrebbe inoltre rendersi necessaria, come misura di salvaguardia, la sorveglianza umana dalla fase di progettazione e durante tutto il ciclo di vita dei prodotti e dei sistemi di IA.
- Ove opportuno potrebbero essere presi in considerazione obblighi espliciti per i produttori anche in relazione ai rischi per la sicurezza mentale degli utenti (ad esempio dovuti alla collaborazione con robot umanoidi).
- La legislazione dell'Unione in materia di sicurezza dei prodotti potrebbe prevedere prescrizioni specifiche che affrontino i rischi per la sicurezza derivanti dall'uso di dati errati in fase di progettazione, nonché meccanismi per garantire che sia mantenuta la qualità dei dati durante l'intero periodo di utilizzo dei prodotti e dei sistemi di IA.
- Il problema dell'opacità dei sistemi basati su algoritmi potrebbe essere affrontato mediante prescrizioni in materia di trasparenza.
- Potrebbe essere necessario adeguare e chiarire le norme vigenti in relazione ai casi di software indipendente immesso sul mercato senza altri componenti, oppure integrato in un prodotto dopo che quest'ultimo è stato immesso sul mercato, qualora ciò abbia un impatto sulla sicurezza.

- Data la crescente complessità delle catene di approvvigionamento in relazione alle nuove tecnologie, disposizioni che richiedano specificamente una collaborazione tra gli utenti e gli operatori economici attivi lungo la catena di approvvigionamento potrebbero garantire la certezza del diritto.

Ciò nonostante, in ambito europeo si è maturata la convinzione che non sia necessaria una revisione completa dei regimi di responsabilità correttamente funzionanti, ma che in ragione de «*la complessità, la connettività, l'opacità, la vulnerabilità, la capacità di modifica mediante aggiornamenti, l'autoapprendimento e la potenziale autonomia dei sistemi di IA, come pure la molteplicità degli attori coinvolti*» occorrano «*adeguamenti specifici e coordinati dei regimi di responsabilità*» onde evitare che le persone che subiscono pregiudizi o danni al patrimonio non siano risarcite (punto 6 delle Raccomandazioni).

La prospettiva di questo adeguamento è di prevedere l'applicazione delle direttive eurounitarie in materia di prodotti difettosi congiuntamente all'introduzione di regole specifiche, considerando responsabili le varie persone nella "*catena del valore che creano il sistema di IA, ne eseguono la manutenzione o ne controllano i rischi associati*" (punto 7 racc.).[18]

La direttiva sulla responsabilità per danno da prodotti difettosi (85/374/CE) ha dimostrato, infatti, per oltre trent'anni, di essere un mezzo efficace per ottenere un risarcimento per i danni cagionati da prodotto difettoso. Essa, tuttavia, – secondo il PE – deve essere rivista per adattarla al mondo digitale e alle tecnologie digitali emergenti, garantendo un elevato livello di efficace protezione dei consumatori e la certezza giuridica per consumatori e imprese.

Parallelamente deve essere aggiornata la direttiva 2001/95/CE del P.E. e del Consiglio, del 3 dicembre 2001, sulla sicurezza generale dei prodotti, per garantire che i sistemi di IA integrino la sicurezza e la protezione fin dalla progettazione.

Specifiche indicazioni sono rivolte, pertanto, dal Parlamento alla Commissione affinché: a) valuti se la direttiva sulla responsabilità per danno da prodotti difettosi debba essere trasformata in un regolamento; b) chiarisca la definizione di "prodotti", determinando se i contenuti e i servizi digitali rientrino nel suo ambito di applicazione; c) esamini l'adeguamento di concetti quali "pregiudizio", "difetto" e "produttore".

Le principali difficoltà applicative della direttiva n. 374/85 CEE derivano dal fatto che la prova a carico del danneggiato, ed in particolare l'onere di dimo-

[18] Si veda C. Leanza, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in Resp. civ. e prev., 2021, p. 1011 ss.

strare il difetto del prodotto e il nesso di causalità tra difetto e danno (art. 4), è particolarmente difficile per prodotti ad alta complessità tecnologica.[19]

Secondo il PE la responsabilità dei sistemi di IA, sotto tale profilo, non può *sic et simpliceter* essere assoggettata alla direttiva eurounitaria in materia di prodotti difettosi. A causa della loro opacità, connettività e autonomia, secondo il PE, sarebbe molto difficile o addirittura impossibile ricondurre specifiche azioni dannose dei sistemi di IA a uno specifico input umano o a decisioni adottate in fase di progettazione. Anche il Libro Bianco evidenzia come «*A norma della direttiva sulla responsabilità per danno da prodotti difettosi, il produttore è responsabile dei danni causati da un prodotto difettoso. Tuttavia, nel caso di sistemi basati sull'IA, come quelli delle auto a guida autonoma, può rivelarsi difficile provare che il prodotto è difettoso e dimostrare il danno cagionato e il nesso di causalità tra difetto e danno. In aggiunta non è chiaro come e in che misura si applichi la direttiva sulla responsabilità per danno da prodotti difettosi nel caso di alcuni tipi di difetti, ad esempio per quelli risultanti da carenze della cibersicurezza del prodotto*.».

5. I soggetti responsabili

Se in base di principi generali la responsabilità per il danno ricade sulla persona che crea o mantiene un rischio e se la stessa è tenuta a «*minimizzarlo ex ante o risarcirlo ex post nel caso in cui non riesca ad evitare il suo avverarsi*». Ne consegue che, in questo ambito, la responsabilità per i danni deve appuntarsi, quindi, su (a) chiunque crei un sistema di IA, (b) ne esegua la manutenzione, (c) lo controlli o (d) vi interferisca.

La responsabilità dell'operatore ai sensi della proposta di regolamento si basa sul fatto che egli esercita un certo grado di controllo su un rischio connesso all'operatività e al funzionamento di un sistema di IA, assimilabile a quello del proprietario di un'automobile (considerando 10 prop. Reg.).

L'"operatore di *front-end*" (lett. e) è la persona fisica o giuridica che esercita un *certo grado di controllo su un rischio* connesso all'operatività e al funziona-

[19] Il Libro Bianco evidenzia l'«*Incertezza in merito all'attribuzione delle responsabilità tra i diversi operatori economici lungo la catena di approvvigionamento: in linea generale, la legislazione dell'UE in materia di sicurezza dei prodotti attribuisce al fabbricante la responsabilità del prodotto immesso sul mercato e di tutti i suoi componenti, ad esempio i sistemi di IA. In alcuni casi le norme possono però divenire poco chiare, ad esempio se l'IA è integrata nel prodotto dopo che quest'ultimo è stato immesso sul mercato da un soggetto diverso dal produttore. Inoltre la legislazione dell'UE in materia di responsabilità per danno da prodotti difettosi prevede la responsabilità dei produttori e lascia alle disposizioni nazionali in materia il compito di disciplinare la responsabilità di altri soggetti nella catena di approvvigionamento*.»

mento del sistema di IA e che *beneficia* del suo funzionamento. Sulla base della Risoluzione, quindi, la responsabilità può ricadere sul deployer, nozione nella quale può, ad esempio, rientrare il conducente del veicolo non del tutto autonomo o il medico che utilizza un sistema di intelligenza artificiale.

L'"operatore di *back-end*", invece, la persona fisica o giuridica che, su base continuativa, *definisce le caratteristiche* della tecnologia e *fornisce i dati* e il *servizio di supporto* di back-end essenziale e pertanto esercita anche un *elevato grado di controllo* su un rischio connesso all'operatività e al funzionamento del sistema di IA.

Per "controllo" (art. 3 lett. g) si intende l'azione che *influenza* il funzionamento di un sistema di IA e che, quindi il grado quindi il grado di esposizione di terzi ai suoi potenziali rischi.

Laddove ci sia più un operatore, ad esempio, un operatore di back-end e un operatore di front-end,, il PE ritiene che in tal caso tutti gli operatori dovrebbero essere *responsabili in solido*, pur avendo il diritto di rivalersi reciprocamente su base proporzionale, in misura dei «*rispettivi gradi di controllo che gli operatori hanno esercitato sul rischio connesso all'operatività e al funzionamento del sistema di IA*» e non del criterio, concettualmente diverso, ma simile negli effetti pratici, del contributo causale apportato dalla condotta di ciascuno (sempre che una condotta sia concretamente individuabile) o del grado di colpa di ciascuno.

Il regolamento non si occupa, invece, della tutela alle persone che subiscono danni (patrimoniali e non) a seguito dell'*interferenza di un terzo* quale, ad esempio, un hacker. Essa, infatti, costituisce sistematicamente un'azione basata sulla colpa, per cui il vigente diritto degli Stati membri in materia di responsabilità civile per colpa offre già, il più delle volte, un livello sufficiente di protezione. Solo per casi specifici, inclusi quelli in cui il terzo sia irrintracciabile o insolvibile, risultano necessarie ulteriori norme in materia di responsabilità per integrare il diritto nazionale in materia di responsabilità civile (punto 9 racc.). È evidente, in tal caso, la necessità di prevedere che per tale attività pericolosa, come ad esempio, quella da circolazione stradale (non a caso richiamata per analogia come attività rischiosa – punto 10 racc.), siano istituiti fondi di garanzia che assicurino forme di risarcimento in favore del danneggiato.

Tali passaggi sembrano implicare che, oltre alla forza maggiore, anche il fatto del terzo porti ad escludere la responsabilità dell'operatore del sistema di IA ad alto rischio.

Quanto all'*utente*, ovvero la persona che utilizza il sistema di IA coinvolta nell'evento dannoso, questi dovrebbe essere chiamata a rispondere a norma del presente regolamento solo laddove si qualifichi anche come operatore. In caso contrario, la sua responsabilità può essere affermata solo per colpa, apprezzando l'entità del suo contributo al rischio per negligenza grave o intenzionale (considerando 11 prop. reg.).

6. IA ad alto rischio, e non ad alto rischio: responsabilità oggettiva e per colpa presunta

Le IA sono estremamente diverse nelle caratteristiche, funzionamento, settore operativo. La stragrande maggioranza dei sistemi di IA è utilizzata per gestire compiti banali, privi di rischi o con rischi minimi per la società (considerando 6 prop. reg.).

La Risoluzione, pertanto, preferisce utilizzare la diversa espressione di *"processo decisionale automatizzato"* la quale potrebbe evitare la possibile ambiguità del termine IA. Esso implica che «*un utente deleghi inizialmente una decisione, in parte o interamente, a un'entità utilizzando un software o un servizio; che tale entità a sua volta utilizza modelli decisionali automatizzati per lo svolgimento di un'azione per conto di un utente, o per informare le decisioni dell'utente nello svolgimento di un'azione*» (punto G ris. e considerando 6 pro. Reg.).

Onde non assimilarle tutte al medesimo regime di responsabilità, il PE ricorre al criterio del rischio, giustamente considerato come il più opportuno in relazione alla essenza dell'IA, consistente nell'essere una tecnologia che sia in grado di prendere decisioni autonome.

Distingue, pertanto, i sistema di IA *ad alto rischio*, quando il suo funzionamento autonomo ha un *elevato potenziale* di causare danni a una o più persone, in un modo che è casuale e che va ben oltre quanto ci si può ragionevolmente aspettare. La Risoluzione indica che occorre anche tenere conto del *settore* in cui è possibile prevedere l'insorgere di rischi significativi e della *natura* delle attività svolte; ritiene che l'importanza del potenziale dipenda dall'*interazione* tra la gravità dei possibili danni, la probabilità che il rischio causi un danno o un pregiudizio e la modalità di utilizzo del sistema di IA (punto 15 Racc.). Tra i sistemi a rischio elevato possono indicarsi gli aeromobili senza equipaggio, i veicoli con livello di automazione elevato (livello 4 e 5 delle norme SAE J3016).

Dal momento che all'avvio del funzionamento autonomo del sistema di IA, la maggior parte delle persone potenzialmente interessate è ignota e non identificabile, il PE ritiene che sistema di IA che agisce in modo autonomo è potenzialmente molto più pericoloso per il pubblico, ragione per cui la Risoluzione prevede una *responsabilità oggettiva* per le IA "ad alto rischio", previste nell'elenco allegato alla Risoluzione (da aggiornarsi semestralmente) e una *responsabilità colposa* per le IA che, invece, non presentano tale livello di rischio.

L'inserzione nell'elenco è decisiva in quanto tutte le attività, i dispositivi o i processi guidati da sistemi di IA che possono provocare danni o pregiudizi, ma

che non sono indicati nell'elenco contenuto nell'allegato al regolamento proposto, dovrebbero continuare a essere soggetti a un regime di colpa presuntiva, per cui la persona interessata dovrebbe comunque poter far valere una presunzione di colpa dell'operatore, che dovrebbe potersi discolpare dimostrando di aver rispettato l'obbligo di diligenza (punto 20).

Nel caso in cui, tuttavia un sistema di IA che non sia ancora stato valutato dalla Commissione e dal comitato permanente e che, di conseguenza, non sia ancora stato classificato come ad alto rischio e non sia stato incluso nell'allegato al regolamento proposto, essere dovrebbe soggetto alla responsabilità oggettiva qualora abbia causato *incidenti ripetuti che producono gravi danni o pregiudizi*, ferma restando la necessità per la Commissione di "*valutare, senza indebito ritardo, la necessità di rivedere*" l'allegato nonché l'effetto retroattivo dell'inclusione di tale sistema di IA nell'elenco, a partire dal momento in cui si è verificato il primo incidente provocato dal sistema di IA in questione, che ha causato un danno o un pregiudizio grave (punto 21 Racc.).

Gli operatori dei sistemi di sistemi di IA ad alto rischio possono esonerarsi da responsabilità, definita come "oggettiva" solo provando la *forza maggiore*. Non possono, pertanto, eludere la propria responsabilità sostenendo di avere agito con la dovuta diligenza o che il danno o il pregiudizio sia stato cagionato da un'attività, dispositivo o processo autonomo guidato dal loro sistema di IA.

La proposta di regolamento prevede che le sue norme prevalgano sui regimi nazionali di responsabilità civile in caso di discrepanze nella classificazione dei sistemi di IA ai fini della responsabilità oggettiva.

La proposta indica, quanto alla dimostrazione della colpa per l'utilizzo di sistemi di IA *non* ad alto rischio, «*la diligenza che ci si può attendere da un operatore dovrebbe essere commisurata i) alla natura del sistema di IA, ii) al diritto giuridicamente tutelato potenzialmente interessato, iii) al danno o pregiudizio potenziale che il sistema di IA potrebbe causare e iv) alla probabilità di tale danno.*» Occorre tener conto anche del fatto che l'operatore potrebbe avere una conoscenza limitata degli algoritmi e dei dati utilizzati nel sistema di IA (considerando 18 prop. Reg.).

L'art. 8 prevede che l'operatore non è responsabile se riesce a dimostrare che il danno o il pregiudizio arrecato non è imputabile a sua colpa per uno dei seguenti motivi: a) il sistema di IA si è attivato senza che l'operatore ne fosse a conoscenza e sono state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione al di fuori del controllo dell'operatore; b) è stata rispettata la dovuta diligenza: selezionando un sistema di IA idoneo al compito e alle competenze, mettendo debitamente in funzione il sistema di IA, monitorando le attività e mantenendo l'affidabilità operativa mediante la periodica installazione di tutti gli aggiornamenti disponibili.

Viene altresì precisato che l'operatore non può sottrarsi alla responsabilità sostenendo che il danno o il pregiudizio sia stato cagionato da un'attività, dispositivo o processo autonomo guidato dal suo sistema di IA.

L'operatore non è responsabile se il danno o il pregiudizio è dovuto a cause di forza maggiore.

7. La responsabilità per i danni cagionati dall'IA nel codice civile

Se si analizza l'impatto della proposta di regolamento sul piano interno, deve rilevarsi che diverse norme del Codice civile, nell'attesa dell'approvazione del Regolamento, appaiono astrattamente applicabili ai sistemi di IA. Ad esempio, qualora il sinistro avvenga nell'ambito della circolazione di autoveicoli su strada, si potrà fare riferimento all'art. 2054 c.c.

Analogamente le regole speciali della responsabilità aggravata o semioggettiva, dalla rovina di edificio, ai danni da aeromobili in volo, potranno risultare di volta in volta applicabili anche qualora siano utilizzati strumenti dotati di intelligenza artificiale.

Nelle ipotesi ulteriori, il danno cagionato dall'utilizzo di un sistema di IA appare astrattamente riconducibile a diverse disposizioni.[20]

Potrebbe farsi ricorso, in particolare, all'art. 2049 c.c. sulla responsabilità del datore di lavoro per l'illecito dei "domestici e commessi". Si è osservato, tuttavia, che in tale caso il datore di lavoro risponde per l'agire di un soggetto che è astrattamente imputabile, tanto che il dipendente risponde del danno cagionato in solido con il datore di lavoro, sulla base di un rapporto che ha scarse analogie con quello uomo-macchina.

Numerose, poi sono le forme di responsabilità indiretta, oggettiva o aggravata, a seconda della classificazione dottrinale alla quale si voglia fare riferimento.

Da un lato, si è richiamato l'art. 2047 c.c., sul danno causato dall'incapace, e l'art. 2048 c.c., in materia di responsabilità dei genitori, dei tutori e dei precettori, i quali rispondono per il fatto cagionato dal minore, dal soggetto sottoposto a tutela, dall'allievo o dall'apprendista.

Se è vero che l'IA non ha capacità giuridica, mentre gli incapaci si è sostenuto che l'applicabilità della norma al caso in esame è sostenibile in considerazione della natura evolutiva e autonoma dei dispositivi in esame, caratteristica che li distingue dagli oggetti inanimati.

---

[20] In merito v. diffusamente M. Ratti, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, il *Contratto e impresa* 3/2020, p. 1174 .s.; di V. Di Gregorio, *Intelligenza artificiale e responsabilità civile: quale paradigma per le nuove tecnologie?*, *Danno e Resp., 2022, 1, 51.*

L'utilizzo di dispositivi intelligenti nell'ambito produttivo può anche costituire un'attività pericolosa ai sensi dell'art. 2050 c.c. Si è sostenuto che tale connotazione sarebbe impropria in quanto l'IA è utilizzata come mezzo correttivo o integrativo delle imprecisioni umane e risultando capace di evitare i rischi legati allo svolgimento di certe attività, non escludendosi, tuttavia, che, qualora il dispositivo intelligente sia utilizzato nello svolgimento di un'attività ritenuta di per sé pericolosa, la disposizione potrebbe risultare applicabile.

Ancora si è proposto di applicare l'art. 2051 c.c. sulle cose in custodia o, piuttosto, l'art. 2053 c.c. sul danno cagionato da custodia di animali, in considerazione dell'autonomia decisionale e di spostamento che possano avere alcuni sistemi di IA.

Paradossalmente, per le attività non rischiose dovrebbe applicarsi l'art. 2051 c.c. che esclude la responsabilità solo per il fortuito, mentre il meno rigoroso art. 2050 c.c., che prevede la prova liberatoria dell'aver fatto tutto il possibile per evitare il danno, sarebbe destinato a trovare applicazione per le attività pericolose in luogo dell'art. 2050 c.c.

Si è quindi coerentemente proposto che dovrebbe applicarsi l'art. 2050 c.c. qualora il danno sia cagionato dalla cosa sottoposta alla direzione, ancorché inadeguata, di un soggetto, mentre l'art. 2051 c.c. dovrebbe essere applicato qualora la cosa non sia azionata direttamente dall'operatore.

Risulta evidente, peraltro, che trovando molte di tali norme applicazione per analogia, il regolamento, riempiendo il vuoto normativo, porterà ad escluderne l'applicazione o a limitarla a casi residuali.

Fondamentale per lo sviluppo dell'IA e la tutela dei danneggiati è la previsione dell'assicurazione obbligatoria per gli operatori a copertura della responsabilità civile adeguata agli importi e all'entità del risarcimento previsti dagli articoli 5 e 6 della proposta di regolamento, salvo che tale attività non sia già soggetta ad un regime di assicurazione obbligatoria ai sensi di un'altra legge dell'Unione o nazionale o fondi assicurativi aziendali volontari che copra tali gli importi e l'entità del risarcimento.

8. La prova della responsabilità: la "scatola nera" e l'accesso ai dati

La prova della responsabilità dell'IA può essere difficile o, eccessivamente onerosa o anche impossibile, perché la loro *opacità strutturale* potrebbe rendere estremamente oneroso, se non impossibile, identificare chi ha il controllo del rischio associato a quel sistema di IA o quale codice, input o dati abbiano causato, in definitiva, l'attività pregiudizievole.

La questione è resa più complessa dalla connettività, che spesso lega un sistema di IA e altri sistemi, di IA e non di IA, dalla dipendenza da dati esterni (si pensi alla tematica dell'Internet of Things – "IoT"), dalla vulnerabilità a violazioni

della cybersicurezza e dalla progettazione di sistemi di IA sempre più autonomi, che si avvalgono, tra l'altro, di tecniche di apprendimento automatico e di apprendimento profondo.

A tal fine il PE indica alla Commissione che occorre valutare in che modo i dati raccolti, registrati o salvati riguardanti sistemi di IA ad alto rischio potrebbero essere consultati e utilizzati dall'autorità inquirente e in che modo la tracciabilità e la verificabilità di tali dati potrebbero essere migliorate, tenendo conto di diritti fondamentali e del diritto alla tutela della vita privata.

I sistemi di IA più evoluti e complessi sono sviluppati e si basano su tecnologie come le reti neurali e i processi di apprendimento profondo. La loro opacità e autonomia potrebbe rendere molto difficile ricondurre determinate azioni a specifiche decisioni umane prese durante la loro progettazione o il loro funzionamento. L'operatore potrebbe sostenere, ad esempio, che l'attività, il dispositivo o il processo fisico o virtuale che ha causato il danno o il pregiudizio fosse al di fuori del proprio controllo in quanto attivato da un'operazione autonoma del proprio sistema di IA. Pertanto, vi potrebbero essere casi di responsabilità in cui l'attribuzione della responsabilità potrebbe essere iniqua o inefficiente o in cui la persona che ha subito un danno cagionato da un sistema di IA non possa dimostrare la colpa del produttore, di una terza parte che abbia interferito o dell'operatore, e non ottenga, pertanto, un risarcimento (considerando 7 prop. Reg.).

Ciononostante, secondo il PE deve affermarsi che chiunque crei un sistema di IA, ne esegua la manutenzione, lo controlli o interferisca con esso dovrebbe essere chiamato a rispondere del danno o pregiudizio che l'attività, il dispositivo o il processo provoca.

Ai sensi dell'art. 10, comma 2 un operatore ritenuto responsabile può utilizzare i dati generati dal sistema di IA per provare il concorso di colpa della persona interessata, in conformità del regolamento (UE) 2016/679 e di altre leggi pertinenti in materia di protezione dei dati.

La persona interessata può utilizzare tali dati anche come prova o ai fini di un chiarimento nell'ambito dell'azione per responsabilità.

Per ovviare tali inconvenienti la risoluzione afferma un principio di equità del risarcimento basata sull'equivalenza del livello di protezione assicurato al danneggiato dalla IA rispetto alle ipotesi nelle quali non sia coinvolto un sistema di IA.

9. La prescrizione

Le azioni per responsabilità civile intentate per pregiudizi subiti da sistemi di IA ad alto rischio (art. 4, paragrafo 1), se inerenti a danni alla vita, alla salute o

all'integrità fisica sono soggette a un termine di prescrizione speciale di 30 anni a decorrere dalla data in cui si è verificato il danno; se, invece, intentate per danni al patrimonio o rilevanti danni non patrimoniali che risultino in una "perdita economica verificabile" sono soggette a un termine di prescrizione speciale di: a) 10 anni a decorrere dalla data in cui si è verificato, rispettivamente, il danno al patrimonio o la perdita economica verificabile derivante dal danno non patrimoniale rilevante o b) 30 anni a decorrere dalla data in cui ha avuto luogo l'attività del sistema di IA ad alto rischio che ha provocato il danno al patrimonio o il danno non patrimoniale. Tali norme trovano applicazione senza pregiudizio l'applicazione del diritto nazionale che disciplina la sospensione o l'interruzione della prescrizione. Le azioni per responsabilità civile intentate per danni da attività di IA non ad alto rischio, invece, (art. 8, paragrafo 1 regolamento) sono soggette ai termini di prescrizione e agli importi ed entità di risarcimento delle leggi dello Stato membro in cui si è verificato il danno o il pregiudizio.

Infine, nella consapevolezza del carattere sperimentale della normativa e della velocità dei cambiamenti dei sistemi di IA, la proposta di regolamento prevede che entro tre anni dalla data di sua applicazione del presente regolamento, e successivamente ogni tre anni, la Commissione presenti una relazione dettagliata al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo riesaminando anche il testo normativo alla luce degli ulteriori sviluppi dell'intelligenza artificiale.

Erica Palmerini

Responsabilità civile e *self-driving cars*

Sommario: 1. Premesse introduttive. – 2. Un primo inquadramento giuridico della tecnologia. – 3. I veicoli autonomi nel sistema del codice civile. La responsabilità per i danni da circolazione stradale. – 4. La responsabilità per vizi di costruzione o difetto di manutenzione del veicolo. – 5. La responsabilità da prodotto difettoso. – 6. Considerazioni di sintesi e traiettorie future.

1. Premesse introduttive

Le auto a guida autonoma costituiscono la tecnologia che più di altre ha sollecitato l'attenzione dei giuristi, in particolare in rapporto all'adeguatezza delle attuali regole di responsabilità civile.[1] Benché una delle promesse legate all'avvento delle *self-driving cars* sia di incrementare la sicurezza del traffico stradale, e dunque ridurre esponenzialmente il rischio di incidenti, la loro velocità di

[1] Con particolare riferimento alla dottrina italiana, v. A. Albanese, *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, in *Europa e diritto privato*, 2019, 995 ss.; U. Ruffolo, Self-driving car, *auto* driverless *e responsabilità*, in *Intelligenza artificiale e responsabilità*, a cura di Id., Milano, 2017, 31 ss.; A. Davola, R. Pardolesi, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("driverless")?*, in *Danno e resp.*, 2017, 616 ss.; U. Ruffolo, E. Al Mureden, Autonomous vehicles *e responsabilità nel nostro sistema e in quello statunitense*, in *Intelligenza Artificiale e diritto*, a cura di E. Gabrielli e U. Ruffolo, in *Giur. it.*, 2019, 1704 ss.; E. Al Mureden, Autonomous cars *e responsabilità civile tra disciplina vigente e prospettive* de iure condendo, in *Contr. e. Impr.*, 2019, 895 ss.; M. Tampieri, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, *ivi*, 2020, 733 ss.; S. Pellegatta, *Automazione nel settore* automotive*: profili di responsabilità civile*, *ivi*, 2019, 1418 ss.; R. Lobianco, *Veicoli a guida autonoma e responsabilità civile: regime attuale e prospettive di riforma – I* e *II Parte*, in *Resp. civ. e prev.*, 2020, rispettivamente 724 ss. e 1080 ss.; M.C. Gaeta, *Automazione e responsabilità civile automobilistica*, *ivi*, 2016, 1718 ss.; F.P. Patti, *Autonomous Vehicles' Liability: Need for Change?*, in *Digital Revolution – New Challenges for Law*, a cura di A. De Franceschi, R. Schulze, München, Baden-Baden, 2019, 190 ss., Id., *The European Road to Autonomous Vehicles*, in *Fordham International Law Journal*, vol. 43, 2019, 125 ss.; G. Pulejo, *La gestione del rischio emergente da veicoli autonomi in due proposte di Regolamento dell'UE e le conseguenze sull'assicurazione degli operatori*, in *Juscivile*, 2021, 4, 1075 ss.; R. De Bruin, *Autonomous Intelligent Cars on the European Intersection of Liability and Privacy. Regulatory Challenges and the Road Ahead*, in *European Journal of Risk Regulation*, 2016, 7, 485 ss.

funzionamento, la complessità degli scenari in cui operano, la densità e il carattere non strutturato dell'ambiente in cui si muovono indicano nella gestione dei danni, potenzialmente molto seri, uno dei problemi cruciali da affrontare prima della commercializzazione.

Oltre all'elemento del rischio elevato, ad alimentare l'interesse della dottrina è la sfida che le caratteristiche stesse della tecnologia rivolgono al razionale sotteso alle regole di responsabilità: la perdita di controllo di un operatore umano in favore dell'azione autonoma del sistema sembra escludere che i criteri di imputazione della responsabilità tradizionali possano ancora rispondere all'esigenza di un'allocazione equa e razionale dei danni.

La reazione intuitiva, di fronte alla radicale novità della tecnologia, è predicare un ripensamento altrettanto profondo del quadro regolatorio, che sarebbe addirittura necessario per agevolare la traiettoria di produzione e diffusione dei veicoli autonomi, altrimenti ostacolata dai limiti della disciplina corrente.[2]

A ben vedere, tuttavia, il sistema attuale non è così mal equipaggiato; vi è semmai necessità di fare ordine tra una pluralità di regimi potenzialmente applicabili, a cominciare da quello che presenta maggiori affinità con il fenomeno da regolare, ossia la responsabilità da incidenti della circolazione stradale.

Una prima osservazione generale, a questo riguardo: essa nasce come disciplina speciale precisamente con lo scopo di controllare una tecnologia "pericolosa"; contiene dunque elementi che mettono in primo piano l'obiettivo della compensazione delle vittime rispetto a quello della prevenzione, in rapporto a eventi di danno che, almeno in certa misura, non sono evitabili nonostante tutte le precauzioni adottate. Questa finalità si accentua grazie alla combinazione con il meccanismo assicurativo, oggetto di armonizzazione a livello europeo.[3] Tale disciplina non trasforma dal punto di vista sostanziale i differenti regimi esistenti in Europa, che mantengono le loro differenze, ma esplica un'influenza inevita-

---

[2] In tal senso, ad esempio, A. Bertolini, M. Riccaboni, *Grounding the case for a European approach to the regulation of automated driving: the technology-selection effect of liability rules*, in *European Journal of Law and Economics*, 2020, che propongono l'adozione di un approccio di puro *risk-management*.

[3] L'obbligo di assicurazione r.c.a., introdotto in Italia nel 1969, è stato poi oggetto di più direttive europee, l'ultima delle quali è la dir. 2009/103/CE del 16 settembre 2009. Attualmente la disciplina interna è contenuta nell'art. 122 cod. ass. L'obbligo di stipulare una polizza assicurativa r.ca. che grava sul proprietario del veicolo opera sicuramente anche per quelli a guida autonoma, data l'ampia nozione assunta dall'art. 122 del codice delle assicurazioni private che si riferisce, ai "veicoli a motore senza guida di rotaie". La definizione peraltro corrisponde all'art. 1.1 della direttiva 2009/103: "any motor vehicle intended for travel on land and propelled by mechanical power, but not running on rails, and any trailer, whether or not coupled".

bile sull'assetto complessivo e crea un ambiente regolatorio tendenzialmente favorevole alle vittime.

2. Un primo inquadramento giuridico della tecnologia

Prima di procedere all'analisi dei diversi regimi evocati, occorre premettere che i veicoli autonomi o ad alta automazione che rivestono interesse per un discorso sulla responsabilità civile sono quelli che corrispondono ai livelli 4 e 5 della classificazione adottata dalla Society of Automotive Engineers.[4] Benché alcuni argomenti, ad esempio quelli relativi alla responsabilità da prodotto difettoso, siano validi anche per veicoli con un livello inferiore di automazione, per questi ultimi non vi sono particolari divergenze o criticità da segnalare rispetto all'applicazione degli attuali regimi in punto di responsabilità. Quanto al livello 3, la guida semi-autonoma, si discute circa la sua stessa desiderabilità, poiché la circostanza che il conducente debba sempre essere in grado di riprendere il controllo dell'auto annulla uno dei vantaggi della tecnologia, come il farsi trasportare dedicando il tempo dello spostamento ad altre attività, e la rende quindi meno appetibile sul mercato.[5] Nondimeno, vi è da segnalare a questo riguardo che sono stati recentemente approvati sistemi automatizzati di mantenimento della corsia (c.d. ALKS, *automatic lane keeoing systems*), che corrispondono proprio al livello 3 della classificazione menzionata, di cui i veicoli di nuova produzione possono essere dunque equipaggiati.[6]

Allo stato attuale, veicoli autonomi propriamente detti non potrebbero circolare in ambito nazionale se non rispettando i presupposti tracciati dal c.d. De-

---

[4] La Society of Automotive Engineers (SAE International) è un ente di normazione nel campo dell'industria aerospaziale e automobilistica che elabora standard tecnici. Nella classificazione operata, i livelli 1 e 2 sono costituiti da sistemi di assistenza alla guida come il *lane departure warning*, il *lane centering* o l'*adaptive cruise control*. Il livello 3 è dato dalla guida semiautonoma, in cui il conducente può affidare per interi tratti la guida al software, ma deve riprendere il controllo quando richiesto dal sistema. I livelli 4 e 5 sono caratterizzati dalla completa automazione, ma mentre nel primo il software potrebbe richiedere al conducente di assumere la guida in alcune circostanze, ad es. in condizioni meteorologiche avverse per le quali non è sufficientemente testato, questo non è previsto nel livello 5, dove addirittura dispositivi come i pedali o lo sterzo potrebbero essere assenti.

[5] R. Lobianco, *op. cit.*, 729 s. riferisce che per questo motivo alcune case automobilistiche non sarebbero interessate a produrle.

[6] Regolamento UNECE n. 157 – Disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda il sistema automatizzato di mantenimento della corsia, ECE/TRANS/WP.29/2020/81, in GUCE L 82/75, 9.3.2021.

creto Smart Roads, che ne autorizza a certe condizioni l'uso sperimentale sulle strade pubbliche.[7] Per un verso, infatti, non corrispondono alla definizione di veicolo data dal codice della strada, secondo cui "si intendono per veicoli tutte le macchine di qualsiasi specie, che circolano sulle strade guidate dall'uomo" (art. 46). Per un altro verso, per essere ammessi alla circolazione i veicoli devono essere omologati e possedere le caratteristiche tecniche e funzionali prescritte dalla normazione vigente. La disciplina relativa a sicurezza, conformità e omologazione dei veicoli secondo lo schema dell'omologazione per tipo – posta dal Regolamento UE 2018/858 (che ha abrogato la Direttiva 2007/46) – ancora non contempla i livelli più elevati di automazione, nonostante vi siano stati passi avanti in quella direzione, come appena detto.

Un'indagine volta a valutare le regole di responsabilità applicabili alla tecnologia non è tuttavia prematura o priva di utilità, e ciò per più ragioni: anzitutto, per adeguare la nozione di veicolo posta dal codice della strada e permettere alle auto a guida autonoma di circolare sarebbe sufficiente una semplice modifica legislativa, già intrapresa in altri ordinamenti. In Germania, ad esempio, una legge del 2017 ha emendato il codice della circolazione stradale al fine di ammettervi le macchine dotate di dispositivi tecnici in grado di guidare parzialmente o completamente in maniera autonoma.[8]

Anche la Convenzione di Vienna del 1968 sulla circolazione stradale contempla da poco un art. 34 *bis* intitolato alla "Guida autonoma", secondo cui "si considera soddisfatto il requisito della presenza di un conducente in ogni veicolo o complesso di veicoli in movimento quando tale veicolo … utilizza un sistema di guida autonoma", purché conforme alle regolamentazioni nazionali.[9]

---

[7] Il Decreto del Ministero delle Infrastrutture e dei Trasporti concernente modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni *Smart Roads* e di guida connessa e automatica, del 28 febbraio 2018, disegna una vera e propria *sandbox* normativa. In particolare, esso prevede che i veicoli autonomi possano circolare in forza di un'autorizzazione rilasciata dal Ministero delle Infrastrutture e dei Trasporti all'esito di apposita domanda da parte del costruttore e di enti di ricerca e università e della verifica dei requisiti per i sistemi di guida automatica, su strade dotate di certe infrastrutture digitali. A bordo deve esserci sempre un supervisore e un contrassegno che segnala la guida sperimentale deve essere apposto sul veicolo. Per una prima analisi v. D. Cerini, *Dal Decreto* Smart Roads *in avanti: ridisegnare responsabilità e soluzioni assicurative*, in *Danno e resp.*, 2018, 401 ss.

[8] Achtes Gesetz zur Änderung des Straßeverkehrsgesetzes, 16.6.2017. Tuttavia, nemmeno qui la guida completamente autonoma è consentita, salvo che in via sperimentale, poiché rimane fermo che tali dispositivi devono poter essere disattivati dal conducente in qualsiasi momento (§1b).

[9] L'articolo risulta dagli emendamenti del 14 dicembre 2020, entrati in vigore nel 2022. È stato sottolineato il valore simbolico di questa previsione, che richiede comunque di essere recepita nella legislazione nazionale: A. Dini, *Le prime regole internazionali sulle auto a guida autonoma*,

Inoltre, l'applicazione del regime di responsabilità disegnato dal codice civile per gli accidenti della circolazione stradale prescinde dalla nozione ristretta di veicolo accolta dal codice della strada. L'art. 2054 c.c., dove è presente soltanto la specificazione "senza guida di rotaie", si estende in sostanza a tutti i veicoli di trasporto terrestre a guida libera. E lo stesso elenco che compare all'art. 47 cod. str., che include, ad esempio, i veicoli a trazione animale, le slitte, i rimorchi, ecc., è considerato meramente esemplificativo e non esaustivo delle ipotesi cui si applicherà il regime di responsabilità di cui all'art. 2054 c.c.[10]

Una conferma della rilevanza della disciplina codicistica per gli incidenti che coinvolgano veicoli autonomi proviene dallo stesso decreto Smart road, il quale non ha introdotto regole apposite sul punto, ma l'ha data per presupposta. L'art. 11, comma 1, lett. a), infatti, prevede che nella domanda di autorizzazione alla guida sperimentale debba essere indicato il proprietario, quale responsabile ai sensi dell'art. 2054, comma 3.

3. I veicoli autonomi nel sistema del codice civile. La responsabilità per i danni da circolazione stradale

La prima ipotesi regolatoria da esplorare si impernia sulla norma dedicata nel codice civile alla "circolazione dei veicoli". Si tratta di situare la nuova tecnologia nel contesto di questa previsione per comprendere come essa reagisca alle caratteristiche tecniche del veicolo che attenuano il ruolo del conducente, fino a farlo sparire, nelle forme più avanzate, dall'orizzonte della fattispecie.

Nell'ambientare la guida autonoma nel contesto dell'art. 2054 c.c., la prima difficoltà si incontra proprio rispetto alla previsione generale circa la responsabilità del conducente (art. 2054, comma 1). A prescindere dalla sua qualificazione come forma di responsabilità per colpa (con inversione dell'onere della prova) od oggettiva, il problema deriva dalla circostanza che un conducente potrebbe non esserci, almeno nei casi di più avanzata automazione.

Una possibilità che si apre, a questo riguardo, è quella di considerare il conducente sempre esistente, poiché è colui che attiva il processo di guida.

Una soluzione simile – ossia, equiparare il conducente a chi aziona il software per far partire il veicolo – è stata proposta in Francia in vista di una possibile

---

in *Wired*, 12.7.2022, <https://www.wired.it/article/auto-guida-autonoma-convenzione-vienna-regole-14-luglio/>.

[10] F. Mezzanotte, *Circolazione di veicoli. Commento all'art. 2054 c.c.,* in *Codice della responsabilità civile*, a cura di E. Navarretta, Milano, 2021, 1370 s.

riforma della Loi Badinter.[11] In quel sistema, peraltro, tale risposta è pressoché risolutiva, poiché la disciplina adotta un criterio oggettivo di responsabilità e, dunque, non è necessario accertare la colpa ma semplicemente identificare una condotta del conducente che sia efficiente dal punto di vista causale.

La medesima scelta è stata operata in sede di riforma della legge tedesca sulla circolazione stradale, già menzionata, il cui §1a (4) ora recita: "è conducente del veicolo anche colui che attivi un sistema di guida altamente o completamente automatizzata e lo impieghi per il controllo del veicolo". E, come già precisato, la Convenzione di Vienna si è spinta anche oltre, in sostanza identificando il conducente con il sistema di guida autonoma.

È da chiedersi se un esito simile potrebbe essere raggiunto nel nostro sistema, in attesa di un intervento del legislatore,[12] anche in via interpretativa. Un indice favorevole in questo senso è dato dalla nozione lata di conducente, come colui che occupa la posizione di guida, che la giurisprudenza accoglie già oggi. Conducente, in altre parole, è considerato colui che si trova nella posizione di manovra anche se i comandi non siano materialmente esercitati.[13]

Tale risultato lascerebbe comunque irrisolto il problema di dover accertare il comportamento negligente di un soggetto che non è attivamente impegnato nella guida. Il criterio di imputazione della responsabilità basato sulla colpa sarebbe applicabile al caso della guida semi-autonoma, ovvero anche al livello sovrastante, almeno quando non sia stato tempestivamente ripreso il controllo nonostante le allerte del sistema. Certamente meno agevole è immaginare che il regime attuale, così inalterato, possa essere applicato nella versione più estrema della guida completamente autonoma.[14]

Difficoltà analoghe si apprezzano con riguardo al 3° comma dell'art. 2054 nella sua lettura corrente. Esso afferma la responsabilità solidale del proprietario (cui sono equiparati l'usufruttuario, l'acquirente con patto di riservato dominio, l'utilizzatore a titolo di locazione finanziaria) e in apparenza sembrerebbe risolvere il problema dell'assenza di un conducente, o di un conducente cui possa

---

[11] In particolare, è stato proposto di aggiungere all'art. 2 della l. 5 luglio 1985, n. 677, un secondo comma siffatto: "Est réputé conducteur celui qui active le système de conduite autonome d'un véhicule terrestre à moteur". V. al riguardo R. Lobianco, *op. cit.*, 730, nt. 20; F.P. Patti, *The European Road*, cit., 133.

[12] Esso sembra peraltro attuato, limitatamente al suo circoscritto ambito applicativo, con il Decreto Smart Roads, là dove introduce la figura del "supervisore del veicolo a guida automatica durante la sperimentazione", al quale viene attribuita la "responsabilità del veicolo" nelle modalità di guida sia automatica sia manuale (art. 10).

[13] F. Mezzanotte, *op. cit.*, 1368.

[14] Lo notano A. Davola, R. Pardolesi, *op. cit.*, 619.

essere applicato un giudizio di colpa. Tuttavia, tale ipotesi è considerata una forma di responsabilità indiretta per fatto altrui, con la funzione di rafforzare la garanzia patrimoniale generica del danneggiato, e non può quindi prescindere dal riscontro di un comportamento negligente del conducente.[15] Si tratta bensì di un caso di responsabilità oggettiva, che presuppone però la sussistenza di un illecito principale.

In sintesi, i primi 3 commi dell'art. 2054 si prestano ad essere applicati agli incidenti della circolazione in cui siano coinvolte auto con un grado elevato di automazione e persino dotate di dispositivi per la guida semi-autonoma. Con qualche forzatura del disposto normativo, sembra possibile sia interpretare la nozione di conducente in senso lato, assecondando una linea esegetica già presente nella giurisprudenza; sia tenere conto della tendenza a oggettivizzare la responsabilità del conducente. Di quest'ultima sono indice i termini rigorosi in cui viene articolata la prova liberatoria ai fini dell'esonero dalla responsabilità e, in positivo, l'esigere una condotta caratterizzata da una diligenza e un'accortezza particolarmente qualificate, e non la semplice osservanza delle norme del codice della strada.

Una riprova indiretta della plausibilità di questa ricostruzione la fornisce la riforma tedesca, che non ha interessato il regime sostanziale della responsabilità da circolazione dei veicoli. Poiché è previsto che vi sia sempre un conducente in grado di riprendere il controllo, a costui si applicherà il giudizio di responsabilità anche se non può essere riferito al comando in senso stretto del veicolo.

Ugualmente in Francia, al decreto che autorizza la guida autonoma in via sperimentale[16] non si accompagnano modifiche di rilievo del regime di responsabilità che è peraltro pacificamente di tipo oggettivo (restando esclusa solo se la vittima ha "cercato" il danno o questo dipende da una sua colpa inescusabile). E, come già detto, anche in Italia il decreto *Smart Roads* ha implicitamente mantenuto il meccanismo che combina la responsabilità solidale del guidatore e del proprietario, incidendo soltanto sul massimale assicurativo che è stato elevato di 4 volte rispetto a quello applicabile per lo stesso veicolo non dotato di dispositivi per la guida autonoma (art. 19).

Viceversa, a differenza che nei sistemi continentali, nel Regno Unito la responsabilità per gli incidenti stradali è ancora fondata sulla colpa del guidatore, con la conseguenza che in caso di incidente causato da un veicolo autonomo il proprietario o il conducente del veicolo non sarebbero mai stati chiamati a

---

[15] A. Albanese, *op. cit.*, 1004.

[16] Décret n 2018-211 du 28 mars 2018 relatif à l'expérimentation des véhicules à délégation de conduite sur les voies publiques.

rispondere, a meno di essere stati negligenti nella manutenzione o nell'aggiornamento del software. Una riforma era pertanto più urgente che altrove, ed è stata introdotta con lo *Automated and Electronic Vehicles Act 2018*. Questa disciplina, che può essere considerata un modello valido anche a prescindere dalle specificità dell'ordinamento inglese, ha posto direttamente a carico dell'assicuratore la responsabilità per i danni causati da un veicolo a guida autonoma (ovvero a carico del proprietario qualora il veicolo non fosse assicurato); i danni risarcibili sono peraltro sia quelli causati a terzi sia quelli subiti dallo stesso titolare della polizza. Con l'adozione di queste regole speciali, il Regno unito ha introdotto una soluzione che in altri Paesi poteva già considerarsi *law in action*.

4. La responsabilità per vizi di costruzione o difetto di manutenzione del veicolo

Nell'ambiente giuridico attuale, più problematico rimane certamente il caso della guida completamente autonoma. Per farvi fronte in maniera efficiente, è stata prospettata l'applicabilità dell'art. 2050 c.c. sulla responsabilità da attività pericolose.[17] Ciò, tuttavia, desta qualche perplessità poiché tale tecnologia innovativa presenta, tra gli altri vantaggi, proprio quello della maggiore sicurezza.[18] L'approdo al mercato di veicoli autonomi certamente presuppone che abbiano dimostrato di essere più sicuri, in termini di numero di incidenti causati, rispetto a quelli guidati dall'uomo.

Più plausibile potrebbe essere il richiamo all'art. 2051 c.c. sulla responsabilità da cose in custodia,[19] che già si applica quando il danno non deriva da un fatto della circolazione, ma ad esempio dall'esplosione del serbatoio che causa un incendio quando l'auto è in garage.[20] Anche questa soluzione però non convince del tutto. La responsabilità da cose in custodia di regola concerne una cosa inerte, inanimata;[21] inoltre, l'imputazione della responsabilità al "custode" trova una giustificazione razionale nella sua posizione di controllo, ossia, è il soggetto capace di sorvegliare e compiere atti di manutenzione sulla cosa. La macchina

---

[17] R. Lobianco, *op. cit.*, 737; U. Ruffolo, E. Al Mureden, *op. cit.*, 1711.

[18] A. Davola, R. Pardolesi, *op. cit.,* 625.

[19] Favorevoli all'applicazione dell'art. 2051 c.c. ai danni causati da sistemi autonomi sono A. Albanese, *op. cit.*, 1007 ss.; U. Ruffolo, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Intelligenza Artificiale e diritto*, cit., 1700; Id., Self-driving car, cit., 46 s.

[20] P. Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2017, 397 s.; F. Mezzanotte, *op. cit.*, 1372.

[21] M. Costanza, *Impresa robotizzata e responsabilità*, in *Intelligenza artificiale e responsabilità*, cit., 113.

guidata da un'intelligenza artificiale, invece, causerà il danno in maniera diretta, per un problema intrinseco, sul quale non spiegano alcuna incidenza gli obblighi di controllo di chi ne fa uso.[22]

Anche per la sua collocazione topografica, sembra piuttosto da valorizzare il 4° comma dell'art. 2054, che del resto configura una particolare ipotesi di responsabilità per danno da cose, e condivide con la previsione appena menzionata sia il criterio (oggettivo) di imputazione della responsabilità sia l'identificazione del responsabile nel proprietario. Custode è infatti colui che ha la disponibilità materiale del bene, che perlopiù coinciderà con lo stesso proprietario; mentre non potrebbe essere il semplice trasportato, poiché la responsabilità da cose in custodia presuppone un potere di intervento sulla cosa a fini di manutenzione e conservazione. L'unica agevolazione per il danneggiato derivante dall'inquadramento nel contesto dell'art. 2051, anziché dell'art. 2054, 4° comma, potrebbe consistere nella necessità di provare nel primo caso soltanto il nesso di causa, mentre nel secondo anche il vizio di costruzione o di manutenzione.

Questa disposizione di fatto risponde in modo abbastanza efficiente ai problemi di allocazione dei rischi posti da tecnologie innovative: consente di identificare con facilità un soggetto cui la vittima possa rivolgere l'azione risarcitoria; lo chiama a rispondere secondo un criterio sostanzialmente oggettivo per danni causati da un vizio intrinseco al veicolo, senza che sia richiesto un coinvolgimento attivo del guidatore, che potrebbe non esserci o non essere rimproverabile per la condotta di guida; infine, grazie alla combinazione con il meccanismo assicurativo, non grava di costi insostenibili il proprietario. È anzi possibile aspettarsi che questo schema incentivi la diffusione di veicoli che abbiamo dimostrato una maggiore sicurezza, per i quali il premio assicurativo è meno elevato, con ciò assecondando anche un obiettivo di prevenzione.

La norma lascia inoltre aperta la possibilità che il proprietario, o in sua vece la compagnia assicurativa che ha risarcito il danno, possano rivalersi sull'effettivo responsabile, sia esso il conducente in colpa oppure il produttore del veicolo.

5. La responsabilità da prodotto difettoso

Tra i regimi potenzialmente applicabili agli incidenti che coinvolgono auto a guida autonoma, la fattispecie prevista dall'art. 2054, 4° comma, basandosi sulla presenza di un "vizio di costruzione", concorre con la disciplina della responsabilità del produttore.

---

[22] M. Costanza, *L'Intelligenza Artificiale e gli stilemi della responsabilità civile*, in *Intelligenza Artificiale e diritto*, cit., 1687 s.

Quest'ultima è considerata, più in generale, l'insieme normativo di rilevanza centrale rispetto ai danni causati da sistemi intelligenti, poiché, in mancanza di un operatore umano, è naturale ricondurre l'azione dannosa a una difettosità intrinseca del dispositivo, e dunque al soggetto che lo ha progettato e messo in commercio. Nella pratica, tuttavia, è difficile immaginare che la vittima di un incidente della circolazione agisca in base alla responsabilità da prodotto a fronte della disponibilità dell'art. 2054, comma 4. L'onere probatorio da soddisfare sarebbe infatti non meno gravoso, e si dovrebbe inoltre rinunciare alla procedura sostanzialmente amministrativa garantita dall'azione diretta contro la compagnia assicurativa.[23]

Nondimeno, la disciplina della responsabilità da prodotto merita di essere esaminata sia perché astrattamente applicabile in via diretta ai danni causati dalla circolazione di un veicolo – ad esempio, per un malfunzionamento del software o per una sensoristica difettosa –, sia in quanto potrebbe definire le condizioni del regresso del proprietario del veicolo o dell'impresa assicurativa chiamati a risarcire i danni causati da un vizio di costruzione. Inoltre, non è da sottovalutare il suo ruolo di leva rispetto alla messa in circolazione di macchine sicure: essa, infatti, pone l'incentivo ad adottare misure di sicurezza sul soggetto che meglio è in grado di prevenire gli incidenti.

Infine, un'ultima circostanza la rende interessante nella prospettiva della ricerca di un sistema efficiente di distribuzione dei costi associati alla guida autonoma: essa garantirebbe un rimedio al proprietario che sia rimasto vittima di un incidente senza altri veicoli corresponsabili.[24] L'unica alternativa sarebbe infatti ricorrere allo schema generale dell'art. 2043 c.c., in assenza di una soluzione come quella accolta dalla recente legge inglese di *first party insurance* obbligatoria.

La responsabilità da prodotto difettoso serve dunque a completare l'assetto del quadro regolatorio applicabile alla circolazione di veicoli autonomi. Al riguardo, è in corso da tempo in corso un'operazione di *fitness check* della attuale disciplina per verificare se sia adeguata a prodotti tecnologici avanzati, come quelli che incorporano moduli di intelligenza artificiale. Essa è culminata in una proposta di direttiva diretta a riformare la disciplina precedente e a eliminare le principali asperità applicative.[25]

---

[23] F.P. Patti, *Machine Learning and European Product Liability*, in *Researches in European Private Law and Beyond: Contribution in Honour of Reiner Schulze's Seventieth Birthday*, a cura di A. Janssen, H. Schulte-Nölke, Baden-Baden, 2020, 111.

[24] S. Pellegatta, *op. cit.*, 1429.

[25] Proposal for a directive of the European Parliament and of the Council on liability for defective products COM (2022) 495 final, 28.9.2022.

Guardando alla intensa discussione che si è svolta in materia dall'angolo visuale dei veicoli autonomi, tra i principali profili problematici vi è anzitutto la nozione di difettosità del prodotto.[26] Come intendere la difettosità algoritmica? È da considerare difettoso il prodotto che causa un incidente che un guidatore umano avrebbe evitato, come accaduto in Florida con una Tesla il cui autopilota non ha distinto la sagoma di un camion bianco contro lo sfondo del cielo?[27] Oppure si deve adoperare un diverso test che si allontani dallo standard antropocentrico di sicurezza e diligenza? Ad esempio, è stato proposto di confrontare la sicurezza di quel veicolo contro il benchmark dato dal comportamento dei veicoli appartenenti alla stessa tipologia, a prescindere dalle circostanze concrete del singolo incidente.[28] E per converso, non si esclude di far corrispondere al rispetto degli standard tecnici e di sicurezza l'assenza di difetti, superando l'attuale disallineamento tra conformità ed (eventuale) difettosità.[29]

Altro tema controverso, ancora a proposito della nozione di difetto, riguarda la previsione secondo cui un prodotto non può essere considerato difettoso per il solo fatto che un prodotto più perfezionato sia stato successivamente messo in commercio (art. 117, comma 2, cod. cons.). In relazione a dispositivi digitali e connessi, che possono essere monitorati nel loro comportamento ed, eventualmente, aggiornati nella componente software anche da remoto, ci si chiede se sia ancora ragionevole una simile prescrizione. Essa è legata agli alti costi che il monitoraggio post vendita, il richiamo o la sostituzione porrebbero rispetto a beni tradizionali; la tecnologia digitale, tuttavia, li abbatte notevolmente, rendendo plausibile configurare, se non un dovere di intervenire, almeno quello di informare su alcune condizioni in cui l'uso del veicolo non è sicuro.[30]

---

[26] F. Mezzanotte, *Risk Allocation and Liability Regimes in the IoT*, in *Digital Revolution*, cit., 179 s.; F.P. Patti, *Autonomous Vehicles' Liability*, cit., 205 ss.; R. Lobianco, *op. cit.*, 1083 s. In termini più generali, U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, 2020, 1260 ss.

[27] L'incidente è classificato in un database sugli incidenti occorsi nella guida autonoma: AI Incident Database, <incidentdatabase.ai/cite/52/>.

[28] Diffusamente su questa ipotesi, anche con rilievi critici, F.P. Patti, *The European Road to Autonomous Vehicles*, cit., 143 ss.

[29] Sul punto v. A. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm.*, 2020, 1348 ss.; con specifico riguardo ai veicoli autonomi, U. Ruffolo, E. Al Mureden, Autonomous vehicles, cit., 1708 ss. Rispetto al sistema nord-americano di responsabilità del produttore, K.S. Abraham, R.L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, in *Virginia Law Review,* vol. 105, 2019, 139 ss.

[30] F.P. Patti, *Autonomous Vehicles' Liability*, cit., 208 s.

Ancora con riferimento alle caratteristiche della difettosità rilevante, è previsto che il difetto debba essere presente nel momento in cui il prodotto viene messo in circolazione (art. 118, lett. b), cod. cons.). Di tale condizione si evidenzia anzitutto la potenziale contraddizione con la complessità dell'architettura dei sistemi e con il loro evolversi in maniera impredicibile qualora basati su tecniche di *machine learning*, grazie alla capacità di automodificarsi e di migliorare la loro *performance* apprendendo dai nuovi scenari in cui sono inseriti e dai dati aggiuntivi che raccolgono. In secondo luogo, il difetto potrebbe essere originato proprio da un aggiornamento successivo alla fornitura del bene: occorre capire se la responsabilità si estende a questa ipotesi ed, eventualmente, chi sia tenuto a dimostrarlo.

La distribuzione dell'onere probatorio è ugualmente un tema sofferto, data la natura sofisticata dei prodotti basati sull'intelligenza artificiale e, talvolta, l'indecifrabilità del loro comportamento, da cui conseguono notevoli difficoltà, e costi elevati, per munirsi delle evidenze necessarie a sostanziare la prova del difetto e del nesso di causalità con l'evento di danno.[31] I possibili rimedi individuati in dottrina andavano nella direzione di un'inversione dell'onere probatorio, oppure verso la soluzione più radicale di eliminare il concetto di difettosità, introducendo una forma di responsabilità oggettiva. Nessuno di essi, peraltro, sembra essere stato accolto nella proposta di direttiva menzionata.

Certamente, un modo per facilitare la prova del difetto e del nesso di causa è sotteso alla proposta di equipaggiare i veicoli autonomi con un sistema di *event data recorder* (EDR). Dapprima prevista in numerosi documenti di policy,[32] è stata accolta dalla disciplina tedesca (§Via, Straßeverkehrsgesetz) e francese (art. 11, Décret n. 2018-211) proprio per facilitare la tracciabilità delle operazioni della macchina e consentire l'acquisizione delle relative informazioni anche per fini di accesso alla giustizia.[33]

Altri aspetti critici, ampiamente segnalati dalla dottrina, riguardano l'esenzione per rischi da sviluppo (art. 118, lett. e), cod. cons.), che troppo spesso potrebbe esonerare dalla responsabilità il produttore date le dinamiche evolutive della

---

[31] A. Davola, R. Pardolesi, *op. cit.*, 624 s., R. Lobianco, *op. cit.*, 1083; R. de Bruin, *op. cit.*, 491.

[32] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, On the road to automated mobility: An EU strategy for mobility of the future COM(2018) 283 final, 10; European Parliament Resolution of 15 January 2019 on autonomous driving in European transport (2018/2089 (INI) §13.

[33] A prescindere dalle caratteristiche di autonomia della macchina, una simile regola è ora posta dal Regolamento UE 2019/2144, sul quale v. E. Al Mureden, Event Data Recorder *e* Advanced Driver Assistance Systems*: la spinta gentile verso la mobilità del futuro*, in *Contr. e Impr.*, 2022, 390 ss., che ne apprezza l'utilità soprattutto con riguardo alle azioni di rivalsa e di regresso (400 s.).

tecnologia,[34] e lo spettro delle perdite risarcibili, limitate ai danni alle cose e alle persone, dal cui novero resterebbe peraltro escluso il danno al veicolo stesso in quanto rappresenta il prodotto difettoso.

6. Considerazioni di sintesi e traiettorie future

Un bilancio, all'esito di questa breve rassegna, sembra indicare nella responsabilità civile per gli incidenti della circolazione tuttora il regime più adatto, o il meno inadatto, a regolare i danni causati dalle auto a guida autonoma.

L'applicazione di questa disciplina sembra adeguata, almeno a una prima fase di immissione sul mercato della tecnologia, perché risponde in modo efficiente all'esigenza di tutelare le vittime, che possono facilmente identificare il responsabile grazie al sistema di registrazione dei motoveicoli ed essere risarcite più agevolmente per la combinazione con il meccanismo dell'assicurazione obbligatoria e le facilitazioni, anche procedurali, che esso garantisce.

Ugualmente semplice è individuare i presupposti di applicazione del regime all'illecito in cui sia coinvolto un sistema intelligente: è sufficiente che sia avvenuto nel contesto della circolazione stradale. Il valore di questa constatazione, in sé ovvia, si lega alla probabile traiettoria di diffusione della tecnologia: che non sarà introdotta *ex abrupto*, sostituendo i mezzi di trasporto preesistenti, ma attraverserà una fase, verosimilmente piuttosto lunga, di convivenza con le auto tradizionali, oltre che con tutti gli altri utenti della strada. In uno scenario di circolazione mista, potrebbe essere particolarmente diseconomico impegnare le vittime di incidenti nella ricerca della disciplina applicabile e, di seguito, nell'identificazione del diverso responsabile a seconda che il veicolo coinvolto sia del tipo tradizionale, ovvero autonomo o semiautonomo, dovendosi anche stabilire, in quest'ultimo caso, in quale modalità fosse guidato al momento dell'incidente.

Questo accertamento potrà semmai essere svolto in sede di rivalsa da parte della compagnia assicurativa, che ha i mezzi e le competenze per determinare l'opportunità, in base a un rapporto costi-benefici, di individuare e agire contro l'effettivo responsabile dell'incidente.

Anche la preoccupazione circa la scarsa propensione a investire maggiormente in sicurezza da parte del produttore di veicoli innovativi, qualora schermato dalla responsabilità immediata del proprietario, può essere ridimensionata. La maggiore sicurezza di una marca di veicolo rispetto ad un'altra, infatti, oltre a operare, com'è noto, quale incentivo reputazionale, può indirettamente con-

[34] In tema, F.P. Patti, *Autonomous Vehicles' Liability*, cit., 204 s.

tribuire al suo successo e alla sua diffusione anche perché comporta rischi di incidente meno elevati e, dunque, un premio assicurativo più leggero. Si realizza in tal modo un buon equilibrio tra gli scopi di compensazione delle vittime e di prevenzione dei danni, il che permette di considerare tuttora valido e *future-proof* il sistema di allocazione dei danni che questo schema giuridico assicura.

Sulla base di queste conclusioni, è possibile esprimere qualche dubbio circa alcune proposte, emergenti a livello europeo, che sembrano andare nella direzione di una soluzione armonizzata, applicabile orizzontalmente a tutti i sistemi basati sull'intelligenza artificiale.

In particolare, la strategia europea per la regolazione dell'IA si compone di una disciplina rivolta ad assicurare standard elevati di sicurezza per i prodotti c.d. ad alto rischio e di una legislazione complementare che investe il versante della responsabilità per i danni. La prima, costituita dal c.d. Artificial Intelligence Act,[35] definisce i requisiti per la progettazione, lo sviluppo e la messa in circolazione di sistemi ad alto rischio che i fornitori e gli utenti devono rispettare; nella nozione di sistemi ad alto rischio data dall'art. 6, comma 1, rientrano i veicoli a guida autonoma.

La seconda, che si occupa dell'aspetto della responsabilità extracontrattuale, non presenta al momento tratti particolarmente nitidi. Secondo una prima formulazione,[36] la disciplina della responsabilità per danni causati dall'intelligenza artificiale sarebbe stata radicalmente ripensata: ricalcando la categoria dei sistemi ad alto rischio propria dell'Artificial Intelligence Act, si proponeva per questi l'introduzione di un regime di responsabilità oggettiva, mentre per i prodotti con un coefficiente di rischio inferiore a questa soglia si prevedeva una responsabilità per colpa presunta. Ad essere gravati dagli obblighi risarcitori sarebbero stati sia l'operatore *front-end* sia l'operatore *back-end*, secondo una distribuzione di responsabilità non facile da sceverare in concreto. Il più recente intervento legislativo – una proposta di direttiva –[37] mitiga notevolmente la portata innovativa dei precedenti documenti, e si limita a introdurre una presunzione circa il nesso di

---

[35] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM (2021) 206 final, 21.4.2021.

[36] Il riferimento è alla proposta del Parlamento europeo, contenuta nella Risoluzione su Civil liability regime for artificial intelligence (2020/2014(INL)), 20 October 2020. Per un'analisi v. A. Bertolini, *Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies*, in *Europa e diritto privato*, 2022, 384 ss.

[37] Proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM (2022) 496 final, 28.9.2022.

causa, lasciando intatte le regole, nazionali o europee, relative al criterio di imputazione della responsabilità. Una soluzione simile non sarebbe capace di alterare in modo significativo le regole sulla responsabilità da circolazione stradale per come si configurano nella maggior parte degli ordinamenti europei. Si aggiunga che una norma, piuttosto sibillina, stabilisce che la direttiva lascia impregiudicate le prescrizioni dell'Unione che regolano le condizioni della responsabilità "nel campo dei trasporti" (art. 1, comma 3, lett. a)). Dall'ambito di applicazione delle nuove regole potrebbero dunque essere esclusi i danni da circolazione stradale, anche se un simile esito avrebbe richiesto una formulazione meno equivoca. La discussione precedente, infatti, includeva sempre i veicoli autonomi, che anzi rappresentavano il prototipo del sistema ad alto rischio.

Ad essere opinabile non è tanto il livello europeo dell'intervento legislativo. Quello dei veicoli autonomi è infatti un tema transnazionale per eccellenza sia in rapporto al mercato unico dei beni e dei servizi sia in considerazione dell'uso transfrontaliero della tecnologia. Approcci normativi frammentari potrebbero in effetti ostacolare lo sviluppo di sistemi di trasporto autonomi e frenare la competitività europea; in particolare, sarà certamente necessaria un'opera di adattamento e uniformazione delle discipline in ordine alla conformità del veicolo, alle regole stesse della circolazione stradale, alle competenze del guidatore, alla connettività del veicolo e ai dispositivi di registrazione automatica.[38] È discutibile, tuttavia, che non sia riconosciuta la specialità di questo comparto tecnologico, anche con riferimento al tema della responsabilità, in favore di un approccio che si concentra sulla presenza nel sistema di un modulo di intelligenza artificiale.

Con i limiti derivanti dall'incertezza del quadro normativo, tuttora *in fieri* e per certi versi di difficile lettura, è possibile comunque proporre una considerazione generale: un regime uniforme che regoli trasversalmente gli illeciti derivanti dall'uso di intelligenza artificiale, senza tenere conto dei diversi contesti di impiego della tecnologia, rischia di disperdere gli elementi di specificità delle legislazioni settoriali, che già presentavano caratteristiche di efficienza e un buon grado di adattamento all'evoluzione tecnologica.

In questo momento, e per le ragioni già viste, un radicale ripensamento della disciplina sembra prematuro,[39] fermo restando che di fronte a scenari più avanzati, quando la circolazione di veicoli autonomi avrà raggiunto un'ampia

[38] Cfr. E. Al Mureden, Autonomous cars, cit., 907.

[39] Predilige un approccio che esplori tutte le potenzialità interpretative del sistema, piuttosto che la suggestione dell'immediato ricorso a nuove regole, G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contr. e Impr.*, 2020, 715 ss. Nello stesso senso, con specifico riferimento alle auto a guida autonoma, U. Ruffolo, Self-driving car, cit., 34 s.

diffusione, le regole attuali andranno riviste. Ciò tuttavia, dipenderà non soltanto dalle caratteristiche tecnologiche inedite dei mezzi di trasporto, ma anche da una trasformazione che investirà tutta la mobilità. È ragionevole immaginare che, anche per ragioni di tutela ambientale, tramonti l'idea dell'automobile come oggetto di proprietà individuale e si prospetti un uso condiviso dei veicoli, almeno nel contesto urbano.[40]

In una prospettazione verosimile, la mobilità diventerà un servizio, ed includerà anche il versante assicurativo senza che sia l'utilizzatore a doversene munire; scomparirà quindi non solo il conducente, com'è intrinseco alla tecnologia della guida autonoma, ma anche il modello proprietario finora dominante. Pertanto, la soluzione che lascia questa responsabilità soltanto su chi ha la disponibilità materiale del veicolo diventa sempre meno razionale.

Ad una rivisitazione delle regole condurrà anche la maggiore complessità dell'attività di circolazione stradale, alla quale cooperano numerosi attori, dal *provider* del network che abilita la comunicazione tra veicoli e tra veicoli e infrastrutture, al fornitore del servizio di rilevazione geosatellitare che serve per tracciare gli itinerari, agli incaricati della manutenzione delle infrastrutture sulle quali i veicoli si muoveranno. La mobilità sarà garantita da una rete organizzata in cui molte persone assumono compiti di gestione, di supervisione e di controllo, e possono essere responsabili o corresponsabili del danno. Il fallimento del software che guida la macchina, insomma, non sarà necessariamente la causa efficiente esclusiva dell'evento di danno, e occorre capire come governare la presenza contemporanea di più soggetti – dal produttore al programmatore all'utente finale, ma non solo – sulla catena causale, e verosimilmente arrivare a una regolazione contrattuale della distribuzione dei rischi tra le imprese che offrono servizi di mobilità e prestazioni a essi correlati.

[40] F.P. Patti, *Autonomous Vehicles' Liability*, cit., 201 s.

Valentina Di Gregorio

Robotica e AI in campo sanitario: profili di responsabilità civile

Sommario: 1. Tecnologia e medicina. – 2. Il profilo diagnostico e terapeutico. – 3. I dispositivi medici e la riabilitazione del paziente. – 4. I rischi sul piano della sicurezza: safety e security. – 5. Il sistema di responsabilità proposto in ambito europeo.

1. Tecnologia e medicina

L'innovazione tecnologica avviata con l'industria 4.0 ha lanciato agli studiosi del diritto una sfida che ha investito anche il sistema della responsabilità civile, ponendo interrogativi sulla classificazione di nuovi prodotti, servizi e rapporti non facilmente catalogabili all'interno delle categorie tradizionali e sui relativi effetti, sia in un'ottica di prevenzione dei danni, sia in una prospettiva risarcitoria[1].

[1] Senza pretesa di fornire in questa sede il significato scientifico ed epistemologico dell'espressione "intelligenza artificiale", con essa s'intende, sotto un profilo di carattere generale, la scienza che studia i fondamenti, le metodologie e le tecniche che consentono di progettare sistemi *hardware* e *software* atti a dotare l'elaboratore elettronico di prestazioni che appaiono di pertinenza esclusiva dell'intelligenza umana. Si devono a Turing, considerato il padre dell'informatica, i primi studi sul tema (A. Turing, *Computing machinery and Intelligence*, in *Mind*, New Series, 1950, 59) e a Searle (J.R. Searle, *Minds, brains and programs, in Behavioral and Brain Sciences*, 1980, p. 417 ss.), la distinzione tra AI forte, relativa a capacità cognitive e di pensiero autonomo e AI "debole", dotata di elaborate e rafforzate capacità di calcolo.
Sul piano normativo, la necessità di individuare una definizione di robot e di *Artificial Intelligence* è stata avvertita, soprattutto in tempi più recenti, dalle istituzioni europee che ne hanno dato evidenza nella risoluzione del 16.2.2017 (2015/2103 (INL)) del Parlamento che contiene raccomandazioni alla Commissione sulle norme di diritto civile sulla Robotica, cui ha fatto seguito la risoluzione del 12.2.2019 sulla politica industriale europea in materia di robotica e intelligenza artificiale (2018/2088 (INI), la risoluzione del 20.10.2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale (2020/2015 (INI) e la risoluzione sulla responsabilità civile per l'intelligenza artificiale del 20.10.2020 (2020/2014 (INL). In quest'ultimo atto viene offerta, nell'art. 3 dell'allegato, che contiene la proposta di regolamento, la seguente definizione di sistema di intelligenza artificiale: *"un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di*

L'impiego della robotica e dell'AI in campo medico (c.d. medicina 4.0), in particolare, a fronte di indubbi benefici, ha imposto di ricercare soluzioni omogenee in tema di responsabilità civile nell'ottica del contemperamento tra sviluppo tecnologico e rischi associati al suo utilizzo nel settore della salute delle persone, oltre ad aver promosso un dibattito anche sul piano etico[2].

In questo specifico ambito, infatti, il fenomeno dell'interazione uomo-macchina presenta una serie di criticità connesse alla necessità di rendere compatibile l'innovazione tecnologica – strumento potenzialmente idoneo a promuovere il benessere, la prevenzione, la diagnosi delle patologie e la ricerca – con il diritto alla salute che potrebbe subire un pregiudizio dall'azione del robot o dall'utilizzo del sistema di intelligenza artificiale.

---

autonomia, per raggiungere obiettivi specifici" e viene evidenziata, in particolare, l'opacità di taluni sistemi che "*potrebbe rendere estremamente oneroso o addirittura impossibile identificare chi avesse il controllo del rischio associato al sistema di IA o quale codice, input o dati abbiano causato, in definitiva, l'attività pregiudizievole; che tale fattore potrebbe rendere più difficile individuare il legame tra il danno o il pregiudizio e il comportamento che lo ha causato, con il risultato che le vittime potrebbero non ricevere un adeguato risarcimento"* (cons. H). Nella proposta di regolamento del Parlamento europeo e del Consiglio in materia di armonizzazione delle regole sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 21.4.2021 (COM/2021/206 final), l'art. 3 descrive il sistema di intelligenza artificiale come "*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono",* offrendo una definizione che è stata correttamente considerata *"estremamente generale"* (così, G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, p. 303 ss., spec. p. 311). Deve darsi atto anche della recente proposta di Direttiva del Parlamento e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità civile da intelligenza artificiale) (COM/2022/496). Il tema della robotica e dell'AI è oggi oggetto di un ampio numero di studi multidisciplinari nell'ambito dei quali, *ex aliis*, G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020; E. Gabrielli, U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, in *Giur. it.*,, numero monografico, 2019; U. Ruffolo, *Intelligenza artificiale e responsabilità*, Milano, 2017; C. Perlingieri, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rass. dir. civ.,* 2015, p. 1235 ss.; E. Palmerini, *The interplay between law and technology, or the Robolaw project in context*, in E. Palmerini, E. Stradella (a cura di), *Law and technology. The challenge of regulating technological development,* Pisa, 2013, p. 7 ss. Sotto il profilo dell'analisi economica del diritto, nell'ambito dei trasporti, E. Al Mureden – G. Calabresi, Driverless cars. *Intelligenza artificiale e futuro della mobilità*, Bologna, 2021. Su un piano più generale, v. G. Sartor, *L'intelligenza artificiale e il diritto*, Torino 2022; G. D'acquisto, *Intelligenza artificiale. Elementi*, Torino, 2021; L. Arnaudo e R. Pardolesi, Ecce robot. *Sulla responsabilità dei sistemi adulti di intelligenza artificiale,* in *Danno e resp.,* 2023, p. 409.

[2] Risoluzione del Parlamento europeo del 20.10.2020 sugli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012 (INL)).

I rischi attengono alla sicurezza intesa come *safety,* che può essere intaccata dal malfunzionamento o da errori derivanti da difetti di progettazione o di programmazione o da vizi delle componenti meccaniche o elettroniche *firmware* (quale microprogramma che controlla le schede elettroniche a più basso livello) e *software,* che si sottraggono al controllo o che influiscono sull'eventuale processo di apprendimento automatico della macchina, ma anche come *security*, possibile oggetto di *vulnus* per effetto dell'illiceità della raccolta, del trattamento e della divulgazione dei dati personali ricavati dall'uso dei *device* tecnologici e degli strumenti di AI anche tramite attacchi e minacce informatiche (*cyber security)*, cui si aggiungono le difficoltà connesse alla vulnerabilità della persona che si interfaccia con un robot intelligente nei confronti del quale possono scaturire forme di dipendenza psicologica, soprattutto quando l'aspetto esteriore della macchina evochi la fisionomia umana.

Sul piano legislativo europeo – come anche su quello interno – l'attenzione per il tema della robotica e dell'intelligenza artificiale è concentrata sul regime di responsabilità per danni, al quale sono dedicate alcune risoluzioni emanate dall'Unione Europea, la proposta di regolamento del 2021 sulle regole armonizzate in tema di intelligenza artificiale che tengono conto dei risvolti anche di natura etica delle nuove tecnologie e la proposta di direttiva del Parlamento e del Consiglio *relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale* (direttiva sulla responsabilità civile da intelligenza artificiale) (COM/2022/496)[3].

Nell'ambito della sanità, le implicazioni si avvertono soprattutto nell'uso di robot intelligenti che operano per mezzo di algoritmi di intelligenza artificiale sul piano diagnostico, terapeutico (ove rientrano anche le tecniche chirurgiche) e riabilitativo; nondimeno il tema riveste un'importanza peculiare nel settore

[3] Complementare alla proposta di direttiva di cui al testo è anche la proposta di direttiva del parlamento europeo e del consiglio sulla responsabilità per danno da prodotti difettosi (COM/2022/495 final).

Emerge dalla proposta di Regolamento del 21.4.2021 come l'Unione Europea aspiri ad "*essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica*" (1, §1.1). Il tema si incrocia con quello della soggettività delle macchine, per il quale si rinvia alle puntuali considerazioni di G. Finocchiaro, *Intelligenza artificiale e responsabilità*, in *Contr. e impr.*, 2020, p. 713 e ID., *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, cit., p. 303 ss. Sul versante etico: F. Lazzini, *Etica digitale e intelligenza artificiale,* Torino, 2022, p. 111, secondo cui un sistema di AI affidabile, nel rispetto di principi di legalità eticità e robustezza, deve garantire, in armonia con gli atti dell'UE emanati sul tema, la tutela del diritti fondamentali degli individui, l'autonomia umana, assicurare la prevenzione dei danni, l'equità delle procedure, la resistenza agli attacchi, la riservatezza, la qualità e l'integrità dei dati, la protezione del principio di non discriminazione, la sostenibilità dell'ambiente.

dell'assistenza personale a soggetti che necessitano di un supporto nelle attività quotidiane a causa delle loro condizioni personali di ordine patologico o per ragioni di disabilità o motivi di invecchiamento.

2. Il profilo diagnostico e terapeutico

L'intelligenza artificiale in campo medico mira alla riduzione dell'errore diagnostico e all'individuazione precoce dei segnali di una malattia e degli strumenti di personalizzazione della cura, anche con funzioni predittive.

Tra le prestazioni basate su metodi di AI e di robotica in campo sanitario rientra la c.d. diagnostica computerizzata, tecnica che opera nutrendosi di un grande numero di dati (c.d. *Data science*) per l'addestramento di modelli, attuati anche con tecniche di *imaging processing* (su cui si basano già le diagnosi tratte da metodi di indagine come la TAC), sviluppati sulla base della ricorrenza statistica. Una delle questioni più discusse, sotto questo profilo, è quella del rischio di errore (e dell'individuazione della responsabilità) in cui incorre il medico che assume come decisivo ai fini della diagnosi il risultato dell'indagine svolta dal sistema senza l'apporto di una valutazione personale, soprattutto quando questa presenti profili di divergenza da quanto emerso dal processo algoritmico.

In ambito terapeutico, e in particolare nel campo della chirurgia, i vantaggi dell'impiego della robotica sono ravvisabili nell'ampliamento delle capacità dell'operatore.

La chirurgia robotica ha cambiato la modalità di approccio al paziente rispetto alla chirurgia tradizionale con benefici sul piano del più elevato livello di precisione dei movimenti meccanici programmati con il *software*, dell'invasività ridotta sul corpo del paziente e dell'operabilità da remoto; il comando degli strumenti con semplici movimenti del polso consente al chirurgo di superare i limiti delle tecniche chirurgiche "*open*" e laparoscopiche, adattando tecniche mini-invasive ad una vasta gamma di procedure complesse, determinando contemporaneamente l'eliminazione del tremore fisiologico delle mani del chirurgo grazie all'uso di arti robotici collegati alla *console* di comando, con una maggior velocità nelle procedure e diminuzione dei rischi per il paziente. Inoltre, la visualizzazione 3D in alta definizione, unita ad una migliore interfaccia utente – come l'interfaccia *touch screen* del monitor – consente al personale sanitario di accelerare la predisposizione della sala operatoria per i diversi interventi, con un'ottimizzazione dei tempi necessari.

Tra le tecniche utilizzate si possono richiamare gli esempi del robot con azioni governate da un mero supporto esterno (ad es., il robot endoscopico o il robot chirurgico Da Vinci utilizzato in urologia) che è situato ad un livello "zero" di automazione, il caso dell'assistente chirurgico robotico (co-robot) che,

in una versione più evoluta della precedente compie in autonomia alcuni limitati movimenti con un livello 1 di automazione[4] o del robot che svolge manovre di ausilio necessarie per movimentare una strumentazione pesante, come nel caso del braccio meccanico *Cyberknife*, usato in radioterapia e capace di eseguire prestazioni di alta precisione per evitare il danneggiamento dei tessuti circostanti la parte del corpo oggetto delle radiazioni.

Questi robot sono principalmente utilizzati per lo svolgimento di attività di "assistenza chirurgica", definita genericamente telechirurgia o cyberchirurgia, con tecniche basate sulla *digital vision* per la navigazione verso aree specifiche del corpo, con un grado di complessità variabile in considerazione delle apparecchiature, generalmente utilizzabili nel caso di interventi chirurgici minimamente invasivi del torso e nella chirurgia ortopedica, ove il sistema sfrutta una combinazione di parti robotiche intelligenti e di immagini 3D, compiendo contestualmente un'analisi dei dati.

All'utilità conseguita per effetto di strumentazioni robotiche o fondate sull'intelligenza artificiale si contrappongono svantaggi generati dai costi del sistema e dall'esigenza di un'adeguata formazione del medico chirurgo e del personale di sala, nonché dalla carenza, in campo chirurgico, di un riscontro tattile che è proprio del contatto diretto tra il paziente e la mano del medico.

Il problema è noto agli organismi dell'Unione Europea che negli ultimi anni hanno dedicato particolare attenzione al tema, esigendo che i sistemi robotici o gli strumenti di intelligenza artificiale, utilizzati anche sotto forma di servizi e non solo di beni, garantiscano "procedure eque" in materia di risarcimento del danno alla persona o al patrimonio cagionato da sistemi di intelligenza artificiale e il medesimo livello di protezione previsto per i casi in cui non sia coinvolto un sistema di intelligenza artificiale, attraverso adeguamenti specifici e coordinati dei regimi di responsabilità contro pregiudizi provocati alle persone o danni al patrimonio, escludendo una revisione completa dei regimi già vigenti nei vari Paesi e nel quadro della promozione dell'innovazione tecnologica e dello sviluppo delle imprese[5].

Le preoccupazioni riguardo ai rischi di perdita del controllo della macchina sono compensate, nei principi contenuti negli atti dell'Unione europea, dal divieto di assunzione di decisioni autonome in capo ai robot, i quali, in un quadro

[4] Si tratta di un processo ancora in via di sperimentazione in Italia.

[5] Ris. UE del 20.10.2020, sul regime di responsabilità civile per l'intelligenza artificiale (cons. H e K) e *Responsabilità e intelligenza artificiale*, §6. Già la ris. 16.2.2017 sulle norme civili sulla robotica aveva posto in rilievo l'insufficienza della regolamentazione vigente a risolvere le questioni inerenti la responsabilità dei robot per danni a terzi (*Responsabilità,* cons. AD) e gli altri atti emanati in forma di proposta dagli organi dell'Unione europea, già citati.

generale di tutela dei diritti fondamentali, possono solo costituire, secondo il livello attuale di sviluppo tecnologico con le sue caratteristiche specifiche di opacità, complessità, dipendenza dai dati, comportamento autonomo, un supporto all'azione umana, senza tuttavia sostituirsi ad essa[6].

In campo medico tale autonomia decisionale delle macchine non è considerata un obiettivo cui tendere.

Un punto fermo fissato negli atti delle istituzioni europee in ambito sanitario è infatti il principio dell'*"autonomia supervisionata"* da parte dell'operatore che preclude un'azione completamente automatizzata del robot, come può trarsi dalla risoluzione UE del 2017 in tema di norme di diritto civile sulla robotica (cons. 33), secondo cui "*la programmazione iniziale di cura e la scelta finale sull'esecuzione spetteranno sempre a un chirurgo umano*" e che richiama l'attenzione sulla funzione di assistenza svolta dal robot rispetto al rapporto diretto medico-paziente, prevedendo un'adeguata formazione del personale sanitario (medici e assistenti).

L'indirizzo è coerente con l'obiettivo europeo della promozione di un processo di innovazione indispensabile allo sviluppo della società affidabile e sicuro, da attuarsi nel rispetto della Carta dei diritti fondamentali dell'Unione Europea (art. 1, dignità umana, artt. 7 e 8, rispetto della vita privata e protezione dei dati di carattere personale) e delle libertà e dei diritti fondamentali degli individui, protetti nel diritto interno dai principi costituzionali di dignità, uguaglianza, autodeterminazione, di tutela della segretezza della vita privata, di tutela della salute (artt. 2, 3, 14, 24 e 35 Cost.)

Nel quadro della sicurezza e della tutela dei diritti fondamentali deve analogamente pervenirsi all'affermazione dell'assenza di una valenza decisionale autonoma dei sistemi di elaborazione robotici o di intelligenza artificiale in campo diagnostico quando gli esiti siano fondati unicamente sui risultati da essi emergenti.

All'esigenza di rispetto del principio della supervisione umana è ispirata anche la risoluzione UE del 2020 sul regime di responsabilità civile per l'intelligenza artificiale che propugna una responsabilità dell'operatore per "*tutte le attività dei sistemi di IA*", "*giustificata dal fatto che la persona sta controllando un rischio*

---

[6] I sistemi di AI immessi sul mercato, secondo la proposta di regolamento UE 21.4.2021 e la proposta di direttiva UE *sull'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale* del 2022, devono rispettare i diritti fondamentali, i valori dell'Unione e garantire l'applicazione della normativa esistente anche in materia di requisiti di sicurezza (cosi, il regolamento: 1. *Contesto della proposta*. 1.1. *Motivi e obiettivi della proposta;* 3. *Risultati delle valutazioni ex post, delle consultazioni dei portatori di interessi e delle valutazioni di impatto* 3.5. *Diritti fondamentali*).

associato al sistema di IA" ai fini dell'individuazione del soggetto responsabile per i danni eventualmente arrecati dal robot, esortando ad adottare un concetto ampio di "*operatore di un sistema di AI*".

L'operatore è definito come il soggetto che esercita un controllo inteso come "*azione capace di influenzare il funzionamento del sistema* di AI *e quindi il grado di esposizione di terzi ai suoi potenziali rischi"* e che racchiude tutti i soggetti *che esercitano un controllo diretto o indiretto sul rischio connesso al sistema di AI*, come l'operatore di *front-end* (il soggetto che esercita un *controllo su un rischio connesso all'operatività e al funzionamento del sistema di AI e che beneficia del suo funzionamento*) che, in campo sanitario, coincide con il medico o la struttura sanitaria, e l'operatore di *back-end* (il soggetto che *su base continuativa definisce le caratteristiche della tecnologia, fornisce i dati e il servizio di supporto di back-end essenziale e pertanto esercita anche un elevato grado di controllo su un rischio connesso)* che è rappresentato dal fornitore, dal produttore del sistema robotico, ma anche dall'elaboratore del programma e dall'editore del *software*.

Il principio della "*sorveglianza umana*" è oggetto di specifica prescrizione nella proposta di regolamento del 2021 (art. 14) per i sistemi appartenenti alla categoria di sistemi di AI "*ad alto rischio*" (art. 6) che viene elaborata nella relazione introduttiva della risoluzione del 2020 (cons. 13, 14) e nel testo della proposta (art. 3, 4), allo scopo di individuare i sistemi immessi sul mercato caratterizzati da un elevato potenziale di danno connesso all'ambito specifico in cui essi sono utilizzati e del grado di autonomia decisionale ad essi ascritto, per i quali sono previste specifiche prescrizioni da parte dei soggetti che li immettono nel mercato ed una valutazione della conformità *ex ante*.

La risoluzione, considerato che la partecipazione di più soggetti al processo produttivo, ciascuno dotato di una propria funzione (produzione, programmazione, edizione, configurazione del *software),* contribuisce a rendere particolarmente difficile l'identificazione del soggetto che ha il controllo del rischio associato al sistema o l'accertamento di quale *input* o quale dato erroneo abbia provocato il malfuzionamento e il danno, suggerisce l'adozione di un sistema di responsabilità solidale degli operatori coinvolti, graduata sul rischio assunto per ciascuna attività (con la specifica identificazione e definizione, come si è detto, di un sistema ad "alto rischio") e la previsione della risarcibilità del danno alla persona, alla salute, all'integrità fisica, sia sotto il profilo patrimoniale che non patrimoniale[7].

[7] Ris. 16.2.2017, sulle norme di diritto civile sulla Robotica (2015/2103 (INL)), *Robot medici* §33; Risoluzione del Parlamento europeo del 20.10.2020 sul regime di responsabilità civile per l'intelligenza artificiale (2020/2014 (INL), *Responsabilità e intelligenza artificiale*, §10, *Responsabilità dell'operatore* §§11,12,13; All., cons. nn. 13,14, art. 3.

Nell'ambito dei rischi inerenti l'impiego delle nuove tecnologie di robotica ed intelligenza artificiale è esplicitamente menzionato, nelle risoluzioni, anche il pericolo di interferenze illecite di terzi o di violazione delle regole su accesso ai dati personali, che pur dovendo essere incentivato, considerato l'elevato livello di circolazione dei dati e di comunicazione posto in essere da applicazioni e apparecchi informatici, deve mostrarsi coerente con la legislazione vigente sul versante europeo ed interno[8].

In campo sanitario a tali problematiche si sovrappongono, quando si tratta di un robot azionato dal medico, altre e più articolate questioni inerenti la ripartizione della responsabilità civile tra l'utilizzatore (medico o altro professionista sanitario), il produttore della soluzione tecnologica e la struttura sanitaria presso la quale è eseguito l'attività diagnostica o il trattamento terapeutico.

Nella relazione alla proposta di direttiva del 2022 si specifica che per alleviare i problemi riscontrati dai danneggiati è opportuno adottare una strategia che "*alleggerisce l'onere della prova per le azioni connesse all'IA e con la previsione di un meccanismo di revisione e prevede la revisione mirata in materia di responsabilità oggettiva, eventualmente abbinata alla copertura assicurativa obbligatoria*".

L'ambito di applicazione, secondo la direttiva, concerne "*le domande di risarcimento del danno causato da un sistema di IA nel quadro di azioni civili di responsabilità extracontrattuale, qualora tali azioni siano intentate nell'ambito di regimi di responsabilità per colpa, ossia, in particolare, regimi che prevedono la responsabilità legale di risarcire i danni causati da un'azione o un'omissione intenzionalmente lesiva o colposa*" (art. 1). Riguardo all'elemento soggettivo dato dalla colpa, identificabile nella non conformità a un obbligo di diligenza a norma del diritto dell'Unione o nazionale, viene stabilita, nella norma dedicata alla presunzione del nesso di causalità, sempre per agevolare l'onere della prova del danneggiato – a favore del quale non è prevista una forma di responsabilità oggettiva – una "*presunzione relativa mirata di causalità*" in relazione al "*nesso di causalità tra la non conformità e l'output prodotto dal sistema di IA o la mancata produzione di un output da parte del sistema di IA che ha cagionato il danno*" (art. 4, 1° e 2° comma), con l'effetto di suscitare perplessità sul regime proposto rispetto al diritto interno.

---

[8] F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018. Sui problemi della *cyber security* e della *cyber defense*, attuati con sistemi di *Machine learning* e *Deep Learning* v. G. D'acquisto, *Etica digitale e intelligenza artificiale*, cit., p. 110.

3. I dispositivi medici e la riabilitazione del paziente

Gli impieghi della robotica in medicina riguardano anche il settore delle protesi e dei dispositivi impiantabili che appartengono alla categoria dei dispositivi medici, sottoposti alla disciplina contenuta nel regolamento UE/2017/745, entrato in vigore nel maggio 2021, mirato a garantire il buon funzionamento del mercato interno, un livello elevato di protezione della salute dei pazienti e degli utilizzatori e la fissazione di standard elevati di qualità e sicurezza[9], comprendendo esplicitamente anche il *software* tra i possibili componenti di un dispositivo medicale (art. 2)[10].

Tali dispositivi, quando siano componenti di un sistema di AI, possono essere compresi tra i c.d. "*sistemi di AI ad alto rischio*", che la risoluzione del 2020 sulla responsabilità civile per l'AI definisce come sistemi che presentano "*un potenziale significativo di AI che opera in modo autonomo, capaci di causare danni o pregiudizi a una o più persone in modo casuale e che va oltre quanto ci si possa ragionevolmente aspettare",* in cui deve tenersi conto dell'interazione tra la gravità dei possibili danni o pregiudizi, del grado di autonomia decisionale, della probabilità che il rischio si concretizzi e della modalità e dal contesto di utilizzo del sistema di intelligenza artificiale[11].

---

[9] L'atto normativo, noto anche come *Medical Device Regulation*, entrato in vigore il 25.5.2017 e applicabile dal 26.5.2020, è reso operativo, quanto all'adeguamento alla normativa nazionale, dal d. lgs. n. 137/2022. Contestualmente è stato emanato il Reg. UE 2017/746 sui dispositivi medico-diagnostici *in vitro* cui ha fatto seguito il d. lgs. n° 138/2022.

[10] Altre norme in materia sono costituite dalla direttiva macchine 2006/42/CE (recepita con d. lgs. 27.1.2010, n° 17 (e per la quale è in atto una revisione a livello europeo contenuta nella proposta COM/2021/202 final 2021/0105 COD presentata il 21.4.2021), nel cui ambito possono farsi rientrare i robot impiegati anche in medicina, in quanto costituiti dalle componenti soggette alla normativa e, se si conviene di qualificare le attrezzature robotiche come prodotti, il codice del consumo, come modificato a seguito della direttiva 771/2019/UE sulla vendita dei beni di consumo recepita nel d. lgs. n. 170/2021. In precedenza già la Corte di giustizia aveva ricompreso tra i "dispositivi medici" alcune forme di *software*, finalizzate a raccogliere dati per rilevare controindicazioni, interazioni tra medicinali, anche se non si tratta di dispositivi che agiscono direttamente sul corpo umano: così, CGUE, 7.12.2017, C-329/16, caso *Snitem e Philips France c. Francia*, in *Rass. dir. farm*., 2017, p. 138; CGUE, 15.1.2009, C-140/07, caso *Hecht-Pharma c. Germania,* in *Rass. dir. farm*., 2009, 427. V. anche CGUE, 22.11.2012, C-219/11, caso *Brain Products c. BioSemi VOF*, *ivi*, 2013, p. 939, in cui la Corte ha specificato che la nozione di dispositivo medico comprende un oggetto concepito dal fabbricante per essere utilizzato sull'uomo a fini di studio di un processo fisiologico solo se destinato a scopo medico.

[11] Risoluzione del 20.10.2020 sul regime di responsabilità civile per l'intelligenza artificiale (2020/2014 (INL), *Norme in materia di responsabilità diverse per i diversi tipi di rischi,* §15, all. art. 3, lett. c) e art. 4, ove si fa rinvio alla necessità di elaborare un elenco di sistemi ad alto rischio che è stato inserito nella proposta di regolamento sulle regole armonizzate in tema di intelligenza artificiale del 21.4.2021 (art. 6).

La proposta di regolamento dell'Unione Europea del 2021, finalizzata all'emanazione di regole armonizzate per l'immissione sul mercato di sistemi di intelligenza artificiale, inserisce i vari sistemi in una "piramide di rischio" ascendente che si snoda dal rischio basso/medio a quello elevato, fino al rischio inaccettabile e quindi vietato (le pratiche vietate sono indicate nell'art. 5), rinviando, nell'art. 6, 1° par., lett. a) e b), ad un elenco contenuto nell'allegato II al documento, dove compaiono i dispositivi medici indicati nel regolamento UE/2017/745. La proposta prevede al contempo regole particolarmente rigorose di gestione dei rischi e di conformità dirette a garantire l'eliminazione dei rischi, la riduzione, l'attuazione di misure di attenuazione (artt. 8, 9), il mantenimento del controllo umano (art. 14), il rispetto dei requisiti di conformità, l'istituzione di organismi di controllo e valutazione (artt. 19 e 43), adottando un modello basato sul rischio[12].

Anche la chirurgia assistita rientra nelle pratiche di AI di cui all'art. 6, par. 1, lett. a) e b) della proposta di regolamento del 2021 che rinvia all'allegato II e quindi è catalogata tra i sistemi ad alto rischio, sia che l'attività si fondi su una strumentazione che assume la natura di "prodotto", sia di "componente di prodotto"[13].

---

[12] Nella proposta sono dettati obblighi per i soggetti coinvolti nella creazione e nell'utilizzo dei sistemi, come il *provider* che deve garantire la conformità attestata mediante una procedura di valutazione e istituire un sistema di gestione della qualità e per gli altri soggetti coinvolti. V. sul punto G. Finocchiaro, *La proposta di regolamento*, cit., p. 317; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ.*, 2020, p. 1246. Per un'ampia disamina dei profili più rilevanti del regolamento e delle possibili ripercussioni in campo sanitario v. A. D'Adda, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema della responsabilità civile ed iniziative di diritto europeo,* in *Riv. dir. civ.,* 2022, p. 805.

[13] L'art. 2 del Reg. UE/2017/745 definisce nel par. 1 come dispositivo medico "*qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie; diagnosi, monitoraggio, trattamento, attenuazione o compensa zione di una lesione o di una disabilità; studio, sostituzione o modifica dell'anatomia oppure di un pro cesso o stato fisiologico o patologico; fornire informazioni attraverso l'esame in vitro di campioni pro venienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi*". Considera tra i dispositivi medici anche i "*dispositivi per il controllo del concepimento o il supporto al concepimento; i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, paragrafo 4, e di quelli di cui al primo comma del presente punto*", specificando al par. 2 che per «accessorio di un dispositivo medico» si intende "*un prodotto che, pur non essendo esso stesso un dispositivo medico, è destinato dal fabbricante a essere utilizzato con uno o più dispositivi medici specifici, per permettere in particolare che questi ultimi siano impiegati conformemente alla loro destinazione d'uso, oppure per assistere specificamente e diretta-*

Il campo della robotica riabilitativa, da un'impostazione propria degli anni '90 in cui la macchina in fisioterapia aveva un ruolo meramente passivo, è stato attraversato, all'inizio del nuovo millennio, da una nuova fase in cui il robot ha assunto una funzione di assistenza alla persona, nell'ambito di un'attività destinata ad una riabilitazione neurologica e cognitiva, di particolare importanza in un'ottica di gestione del fenomeno dell'invecchiamento della popolazione. È il caso degli esoscheletrici terapeutici e gli arti robotici utilizzati per contribuire alla riabilitazione, ad esempio, in seguito a *ictus*, paralisi, lesioni cerebrali traumatiche o sclerosi multipla; alcuni di essi, basati su algoritmi e dotati telecamere di profondità, agiscono in versione *assistance needed,* vale a dire "quanto basta" per soddisfare l'esigenza del paziente e sono dotati di una certa autonomia nell'adattare il proprio intervento a sostegno della persona, modulando, ad esempio, la forza necessaria per sostenere un movimento in funzione dei progressi del paziente.

Per questi sistemi cyberfisici (CPS) e per i dispositivi impiantabili regolati da *software* (come il *pace-maker*), anch'essi considerati sistemi di AI ad alto rischio, le situazioni problematiche riguardano piuttosto l'accesso continuo alla manutenzione e all'aggiornamento del *software*, nel quadro della gestione del rischio di sottrazione dei dati, cancellazione o disattivazione della memoria del dispositivo[14].

Un ulteriore passaggio dell'innovazione scientifica e tecnologica in questo campo è quello che oggi ha trasferito il robot riabilitativo dalla struttura all'a-

---

mente la funzionalità sul piano medico del dispositivo o dei dispositivi medici in relazione alla loro destinazione d'uso" e, al par. 3 per «dispositivo su misura» "*qualsiasi dispositivo fabbricato apposita mente sulla base di una prescrizione scritta di qualsiasi persona autorizzata dal diritto nazionale in virtù della sua qualifica professionale, che indichi, sotto la responsabilità di tale persona, le caratteristiche specifiche di progettazione, e che è destinato a essere utilizzato solo per un determinato paziente esclusivamente al fine di rispondere alle sue condizioni ed esigenze individuali*". Tra i dispositivi "attivi" di cui al par. 4, vale a dire "*qualsiasi dispositivo il cui funzionamento di pende da una fonte di energia diversa da quella generata dal corpo umano per tale scopo o dalla gravità e che agisce modificando la densità di tale energia o convertendola. I dispositivi destinati a trasmettere, senza modifiche di rilievo, l'energia, le sostanze o altri elementi tra un dispositivo attivo e il paziente non sono considerati dispositivi attivi*" è esplicitamente compreso anche il *software*.

[14] V., sul punto, il noto caso della difettosità di un dispositivo medico accertata sulla base di un esemplare – e non di una serie – deciso dalla CGUE, 5.3.2015, C-503/13 e C-504/13, caso *Boston Scientific Medizintechnik c. AOK Sachsen-Anhalt -Die Gesundheitskasse* e altri, in *Dejure*. Il caso riguardava l'accertamento di un guasto di un componente utilizzato per la produzione di un *pace-maker* che aveva indotto la ditta produttrice a segnalare la necessità della sostituzione anticipata del dispositivo impiantato nei pazienti a causa di un possibile malfunzionamento in un componente, benché tale difetto non fosse ancora manifestato.

bitazione del paziente, il quale può indossare *wearable robots* (quindi oltre il concetto di *wearable* device) che consistono in oggetti la cui tecnologia è di derivazione militare, in grado di supportare la persona nei movimenti; anche per tali dispositivi il *focus* dell'attenzione è diretto sul livello di flessibilità necessaria per garantire la sicurezza del prodotto ed evitare eventuali danni, considerato che essi si trovano a stretto contatto con il corpo umano.

Su un versante non lontano, benché distinte sotto il profilo della sicurezza, si pongono le questioni connesse all'utilizzo del robot "assistente personale" che, pur non essendo a diretto contatto con il corpo del paziente, svolge funzioni di monitoraggio delle funzioni vitali e di accompagnamento di persone anziane o con disabilità. Anche in questo caso – e restando ferme le implicazioni che ne possono derivare sul piano etico ed emotivo – il robot, nonostante sia programmato per apprendere dall'esperienza, resta soggetto al controllo dell'uomo, cui è riservato sempre un potere di intervento laddove si presenti la necessità di evitare danni alla persona o alle cose; laddove non sia applicabile la disciplina sulla responsabilità da prodotto, l'utilizzo di sistemi appartenenti all'elenco inserito nell'allegato II della proposta di regolamento del 2021, in questo settore, comporta l'applicazione delle prescrizioni previste per i sistemi di AI ad alto rischio sopra enunciati.

4. I rischi sul piano della sicurezza: *safety* e *security*

Si è detto che i rischi di danno derivanti dal ricorso alla robotica o ai sistemi di AI riguardano sia la sicurezza materiale contro i pericoli di *vulnus* alla persona (c.d. *safety)* o alle cose, sia la sicurezza dei dati personali acquisiti mediante tramite robot e *device* che immagazzinano, controllano ed elaborano le informazioni (c.d. *security*).

Quest'ultimo profilo, nel campo dell'intelligenza artificiale, assume peculiare rilievo per la natura dei sistemi, alimentati attraverso dati e informazioni che devono essere sfruttabili e possedere requisiti di qualità ed esattezza senza dare origine contestualmente a rischi di violazione dei diritti della persona e, in particolare, del diritto alla riservatezza dei dati che, in campo sanitario, è soggetto a regole rigorose dettate nell'art. 9 del GDPR n. 679/2016, dedicato al trattamento di categorie particolari di dati personali, tra cui rientrano, insieme ai dati genetici e biometrici, i dati relativi alla salute, soggetti a specifiche garanzie e stringenti limiti di trattamento[15].

[15] Nel quadro della sanità digitale, la telemedicina consente ai medici e agli operatori sanitari di assistere a distanza i pazienti e di migliorare la capacità di diagnosi a mezzo della condivisione del FSE (fascicolo sanitario elettronico), permettendo di rendere inclusivi e accessibili i servizi sanitari,

Alla tutela prevista dal GDPR riguardo alla liceità della raccolta, del trattamento, della trasmissione dei dati, si accompagna la necessità del controllo dell'accuratezza e della qualità del dato raccolto e, in particolare, dei c.d. *Big Data,* i quali sono necessari per la creazione dell'algoritmo sulla cui base, in medicina, è proposta la diagnosi di supporto al medico, costruita non più e non solo su una *evidence based medicine*, bensì anche sulla scorta di algoritmi che usano tecniche di *deep learning* capaci di compiere anche diagnosi predittive[16].

Sul piano del diritto europeo, riguardo alla sicurezza dei dati, una specifica disposizione della proposta di regolamento del 2021 (art. 10) contiene regole di *governance* per i sistemi ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli, allo scopo di evitare manipolazioni, l'emersione di *bias* o di collegamenti ottenuti statisticamente, ma non connessi strettamente ad un rapporto causa-effetto che possono inquinare l'*output* e quindi l'individuazione della cura.

La norma ha destato alcune perplessità sotto due profili: il primo riguarda la parte in cui si richiede che i set di dati per l'addestramento di modelli, convalida e prova, soggetti ad adeguate pratiche di *governance* e di gestione dei dati siano pertinenti, rappresentativi, esenti da errori e completi, imponendo in tal modo un controllo rigoroso, difficilmente raggiungibile e impegnativo sotto il profilo della responsabilità del soggetto deputato a compierlo (art. 10, par. 3). Il secondo attiene all'eccezione fissata rispetto alla previsione dell'art. 9 del GDPR che consente il trattamento in deroga di categorie particolari di dati (par. 5) che sembra ampliare la griglia protettiva imposta dal regolamento europeo sulla protezione dei dati, innestandosi sulla linea impressa già nell'art. 22 che prevede eccezioni al divieto di trattamento tramite decisioni automatizzate. Di qui alcuni dubbi sulle modalità di controllo, non solo della raccolta e del trattamento dei dati, ma anche delle procedure algoritmiche rispetto ai principi che reggono la normativa europea anche sotto il profilo dell'affidabilità del dato la cui carenza può costituire fonte di danno[17].

---

con innegabili vantaggi sul piano delle liste di attesa di visite e ospedalizzazioni e risparmio dei costi, pur presentando il pericolo della perdita, sottrazione o divulgazione di dati personali riservati in spregio dei diritti garantiti nella normativa europea e interna. V. le osservazioni di M. Gigola, *Evoluzione tecnologica e tutela della riservatezza dei dati sanitari,* in *Resp. medica*, 2023, p. 71.

[16] Il tema del controllo dei dati personali trattati con sistemi di AI è all'attenzione del legislatore europeo nella proposta di *Data Governance Act* del 25.11.2020 COM/2020 767 final e nella proposta di *Data Act* del 23.2.2022 COM/2022 68 final. V. per il profilo della riferibilità del concetto di *Data* non solo ai dati personali, ma anche alle informazioni intese come beni C. Perlingieri, *Data as the object of a contract and contract epistemology*, in *Italian law journal,* 2019, p. 613 ss.

[17] G. Resta, C*osa c'è di "europeo" nella proposta di Regolamento UE sull'intelligenza artificiale?* in *Dir. inf.,* 2022, p.323 ss.

Per quanto riguarda la sicurezza materiale dell'uso di strumentazioni robotiche o di AI, i profili più critici attengono all'individuazione di una disciplina della responsabilità che sfugge ad un chiaro inquadramento all'interno della trama legislativa vigente soprattutto quando l'elevato grado di sofisticazione del prodotto, del *software* o del servizio rende difficile ricostruire la catena causale degli eventi, complicando l'operazione interpretativa per i danni prodotti da comportamenti imprevedibili delle macchine dotate di capacità di autoapprendimento.

Nel diritto interno, quando si tratta di tecnologie robotiche o di AI in medicina, la materia è presidiata dalle norme del codice civile in tema di responsabilità contrattuale, extracontrattuale, responsabilità oggettiva (artt. 1218, 1223, 1225, 1226, 1227, 2043, 2050, 2051, 2055 e 2056), dal codice del consumo, relativamente alla parte sulla sicurezza dei prodotti e alla responsabilità del produttore (quando ne ricorrano i presupposti) e dalla legge sulla responsabilità medica n. 24/2017[18].

Le questioni relative ai danni provocati dai sistemi di robotica e AI guidati dal personale adeguatamente istruito all'interno di una struttura sanitaria, sia sul piano diagnostico che terapeutico, devono essere valutate dunque nel quadro del rapporto tra medico e paziente regolato dalla l. n. 24/2017 che, come è noto, impone al medico il rispetto delle raccomandazioni previste nelle linee guida e delle buone pratiche clinico-assistenziali nell'art. 5 e descrive un regime binario di responsabilità della struttura sanitaria o sociosanitaria pubblica o privata ex art. 1218 e del medico ex art. 2043 c.c. (salvo che l'obbligazione tra medico e paziente sia sorta da un incarico professionale al di fuori della struttura), con una diversa ripartizione dell'onere della prova tra le parti (art. 7) in funzione della natura della responsabilità su di esse gravante e una gradazione in diminuzione del risarcimento del danno a carico del medico quando la colpa lieve sia dovuta a imperizia, ma siano state rispettate le buone pratiche (art. 7, 3° comma)[19].

---

[18] Tra le norme applicabili devono considerarsi i già citati regolamenti UE/2017/745 e UE/2017/746, quest'ultimo recentemente modificato con regolamento UE/2022/112.

[19] La circostanza di cui al testo rappresenta una specifica causa di esclusione della punibilità in sede penale (art. 590 *sexies,* 2° comma c.p.) nel caso di responsabilità colposa derivante da morte o lesioni personali provocata dagli esercenti la professione sanitaria, introdotta dall'art. 6 della l. n. 24/2017 con riferimento agli eventi verificatisi a causa di imperizia, sul presupposto che siano state rispettate le raccomandazioni previste dalle linee-guida come definite e pubblicate ai sensi di legge ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali, sempre che le raccomandazioni previste dalle predette linee-guida risultino adeguate alle specificità del caso concreto. Sul punto Cass., sez. un., 22.2.2018, n. 8770, in *Dejure*, ha escluso la responsabilità di un medico che aveva seguito correttamente le linee guida, ma aveva al contempo agito erro-

Il ricorso ad una strumentazione meccanica, robotica, di AI da parte della struttura sanitaria o del medico che in essa opera determina l'applicazione degli artt. 1218, 2043 e, in particolare, dell'art. 2051 c.c. sul danno da cose in custodia, posto che il soggetto che manovra il robot o il dispositivo chirurgico o che si basa su di esso per compiere la diagnosi è il medico o altro personale sanitario[20]. Il ricorso ad un regime di responsabilità di tipo oggettivo (come quello dettato nell'art. 2051) che prescinde dalla violazione di un dovere di custodia, derivando unicamente dal dinamismo della cosa custodita, può alleggerire il paziente dall'onere probatorio[21].

Qualora invece si tratti di situazioni in cui non ricorrono i presupposti per affermare la responsabilità della struttura sanitaria e/o del medico perché il *device* è utilizzato direttamente dal paziente, la soluzione delle questioni di imputazione della responsabilità del danno generato da malfunzionamento può essere rinvenuta anche nella disciplina del danno da prodotto difettoso, con i limiti che derivano dalle difficoltà di ordine probatorio gravanti sul soggetto (il paziente) tenuto a provare il difetto del prodotto (art. 120), benché la giurisprudenza consideri assolto tale onere anche tramite presunzioni e assuma quali requisiti di si-

---

neamente nell'attuarle per imperizia dovuta a colpa lieve. La funzione premiale, che costituisce la *ratio* dell'art. 7, 3° comma, è coerente con quella complessiva della legge, volta a ridurre il ricorso alla c.d. medicina difensiva senza sacrificare la tutela del diritto alla salute. In quest'ottica, la disposizione, nel prevedere una deroga alla finalità riparatoria della responsabilità civile, appare coerente con il parametro della ragionevolezza imposto dai principi costituzionali essendo la riduzione del risarcimento ex art. 7, 3° comma, applicabile esclusivamente in caso di azione rivolta dal danneggiato contro il medico, e non, nel giudizio contro la struttura sanitaria (art. 7, 1° comma). La previsione della responsabilità della struttura, di natura contrattuale, veicola su quest'ultima le domande di risarcimento, limitando le tecniche di medicina difensiva ogniqualvolta risultino rispettate le linee guida.

[20] M. Costanza, *L'intelligenza artificiale* e gli stilemi della responsabilità civile, in *Giur. it.*, 2019, p. 1687 ss. Sul profilo probatorio, che la giurisprudenza affronta anche con il richiamo al principio della "vicinanza della prova", attribuendo all'espressione diversi significati, v. le puntuali osservazioni critiche di M. Franzoni, *La "vicinanza della prova*", quindi..., in *Contr. e impr.*, 2016, p. 360 ss.

[21] Segnala U. Ruffolo "*Le mobili frontiere della responsabilità medica*", in *Giur. it.*, 2021, pp. 456, 457, come in riferimento alla responsabilità oggettiva della struttura sanitaria, il diffondersi di azioni civili per *malpractice*, abbia reso più complesso l'onere probatorio gravante su colui che lamenta il danno, mentre con l'avvento dilagante dell'AI all'interno delle strutture sanitarie, si registra l'aumento direttamente proporzionale della responsabilità da custodia delle apparecchiature mediche dotate di AI e da addestramento di *AI-powered* (frutto della combinazione di due tecnologie: a*nalytics* e intelligenza artificiale), anziché da prodotto difettoso.
V. sull'evoluzione del regime di responsabilità sanitaria R. De Matteis, *Le responsabilità in ambito sanitario. Il regime binario: dal modello teorico ai risvolti applicativi*, Milano, 2017.

curezza le circostanze tipizzate nell'elenco contenuto nell'art. 117 c. cons. o altri elementi valutabili dal giudice, nell'ambito dei quali rientrano anche gli standard di sicurezza eventualmente imposti da normative di settore[22].

Sotto questo profilo, la risoluzione sulla responsabilità civile per l'AI sembra condividere la *ratio* della norma dell'art. 2051 c.c. laddove estende la responsabilità per danni all'operatore di *front-end;* nel caso di divergenza dal compito originariamente affidato, tuttavia, viene in luce la fragilità del confine con la responsabilità prevista dalla clausola generale dell'art. 2043 che impone al medico o all'operatore di rispondere dei danni per condotta negligente nell'esecuzione della prestazione[23].

Le perplessità sul ricorso alla responsabilità da prodotto riguardano i problemi di sicurezza che potrebbero scaturire dall'uso di prodotti la cui funzionalità possa essere alterata dai sistemi di intelligenza artificiale o in cui i sistemi di AI si modificano nel corso del tempo (in campo medico tale ultima condizione non può essere ammessa)[24].

Più discutibile è, invece, concepire un'applicazione dell'art. 2050 sull'attività pericolosa – norma considerata espressiva di un principio "intermedio" tra quello della colpa e del rischio[25] – in quanto apparentemente incompatibile con l'uso di sistemi di intelligenza artificiale e robot il cui impiego in medicina è finalizzato ad accrescere il livello di sicurezza e non ad introdurre un fattore di pericolo[26], benché gli atti normativi europei propendano per un regime di *strict liability* nella valutazione del grado di rischio del prodotto che comprende anche l'errore nell'algoritmo, in un'ottica di bilanciamento tra promozione delle iniziative di ricerca, degli investimenti, della diffusione sul mercato delle

---

[22] A partire da Cass. 29.5.2013, n. 13458, in *Dejure*, confermata di recente da Cass., 10.5.2021, *ivi*. La nuova proposta di direttiva in tema di danno da prodotto.

[23] M. Costanza, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giur. it.*, cit., p. 1687.

[24] G. Alpa, *Quale modello normativo europeo per l'intelligenza artificiale?* in *Contr. e impr.*, 2021, p. 1016.

[25] P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 2, 9.

[26] Di contrario avviso C. Leanza: *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp. civ. prev.* 2021, p. 1011, secondo cui "laddove sia consentito ad un automa munito di capacità adattative e di apprendimento di interagire con un uomo, non esiste sicurezza alcuna che lo stesso non possa assumere comportamenti lesivi dei diritti dei terzi. Attualmente, pertanto, non vi è ragione per escludere dal novero delle «attività pericolose», per come definite dall'art. 2050 c.c., l'impiego di robot in attività relazionali con esseri umani". Per una riflessione di più ampio respiro v. F. Di lella, *Le attività pericolose nel settore bio-medico. Spunti per una rilettura dell'art. 2050 c.c.*, Pisa, 2020, p. 115 e ss.

nuove tecnologie e tutela dei diritti fondamentali dell'individuo, *ivi* compreso, come in questo caso, il diritto alla salute[27].

5. Il sistema di responsabilità proposto in ambito europeo

Nello scenario sopra descritto, e non solo in campo medico, le risoluzioni europee (sulla robotica del 2017, sull'intelligenza artificiale del 2020), anticipando i problemi che verranno a porsi con l'evoluzione dei sistemi, configurano un nuovo sistema binario di regole diversificato in funzione del livello di rischio del sistema utilizzato che dovrebbe integrarsi con quello preesistente, interpretato alla luce dell'innovazione, non esautorando il controllo umano in vista di un'adeguata tutela alla persona.

Una prima forma di responsabilità, più severa, di tipo oggettivo, *risk based approach,* è applicabile agli operatori di dispositivi medici o di processi guidati da sistemi definiti "ad alto rischio" e concentra la responsabilità sul soggetto che è in grado di minimizzare i rischi e affrontarne l'impatto negativo: come si è avuto modo di anticipare, per quanto riguarda l'attività medica, ove sono in gioco la salute (e relative diagnosi e terapie) e i diritti fondamentali della persona, i sistemi di AI sono considerati sempre ad alto rischio, con la sola clausola di esclusione della forza maggiore e sono classificati attraverso il richiamo all'elenco contenuto nell'allegato II, nonché accompagnati da un obbligo assicurativo[28].

Un secondo modello di allocazione della responsabilità, meno rigoroso, è costruito, nella risoluzione UE del 2020, su una presunzione di colpa dalla quale l'operatore può liberarsi ricorrendo alle seguenti cause di esclusione: a) il sistema di AI si è attivato senza che ne fosse a conoscenza e sono state adottate tutte le misure

---

[27] Sul tema la letteratura è amplissima. V. spec. P. Trimarchi, *Rischio e responsabilità oggettiva*, cit., p. 9 ss.; ID.; *Atti illeciti, rischio, danno*, Milano, 2017, p. 275 ss.; S. Rodotà, *Il problema della responsabilità civile*, Milano, 1964, p. 128, G. Alpa, *Il problema dell'atipicità dell'illecito*, Napoli, 1979; M. Franzoni, *L'illecito*, in *Trattato della responsabilità civile,* Milano, 2010, p. 395 ss.; P. Monateri, *Le fonti delle obbligazioni, 3, La responsabilità civile*, in *Trattato di diritto civile* Sacco, Torino, 1998, p. 1036 ss.; M. Comporti, *Fatti illeciti: le responsabilità oggettive,* cit., 54 ss. Sull'errore dell'algoritmo L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Pol. dir.*, 2018, p. 728.

[28] In particolare, tali sistemi sono previsti negli allegati II e III della proposta di regolamento del 2021 e nel cons. 56 della ris. sulla robotica del 2017, e nel cons. 14 della risoluzione sull'AI del 2020. L'allegato III prevede i sistemi ad altro rischio c.d. "indipendenti" che non rappresentano prodotti o componenti di prodotti di cui all'all. II, ma che sono ritenuti ad alto rischio per il loro impatto sulla salute, la sicurezza, i diritti fondamentali. Un'analisi di tali sistemi sotto un profilo di carattere generale è compiuta da A. Amidei, *La proposta di Regolamento UE per un Artificial Intelligence Act: prime riflessioni sulle ricadute in tema di responsabilità da Intelligenza Artificiale*, in *Tecn. e dir.*, 2022, p. 1 ss.

ragionevoli e necessarie per evitare l'attivazione al di fuori del suo controllo; b) l'operatore ha tenuto una condotta diligente consistente nello svolgimento di una serie di operazioni (come la selezione di un sistema di AI idoneo al compito, il corretto avvio al funzionamento, il monitoraggio e la manutenzione con aggiornamenti).

Quest'ultimo criterio non è applicabile all'intelligenza artificiale e alla robotica impiegati in medicina perché nel campo della salute il ricorso alle nuove tecnologie, seguendo la proposta di regolamento, è assoggettato ad un regime di responsabilità più rigoroso in un'ottica di protezione della posizione del paziente, sia sotto il profilo dell'imputazione della responsabilità, sia sotto quello della prova del danno.

Il modello di allocazione del rischio approntato nella proposta di regolamento dell'UE delinea un regime di responsabilità oggettiva per i sistemi di AI ad alto rischio, di responsabilità presunta per i sistemi di AI non ad alto rischio che si dovrebbe aggiungere al regime di responsabilità presunta "speciale" disciplinata dalle norme sull'onere della prova (art. 120 c. cons.) e sulle cause di esclusione (art. 118 c. cons.) per tutti gli altri prodotti che può essere adattato alle nuove tecnologie.

Le disposizioni sulla responsabilità da prodotto, tuttavia, non offrono margini di tutela sufficienti di tutela nel settore sanitario, considerato l'onere probatorio del difetto gravante sul danneggiato e la possibilità di ricorrere, tra le clausole di esonero dalla responsabilità, al c.d. rischio di sviluppo (art. 118, lett. e) che in questo campo è invocabile con maggiore facilità a causa del rapido progresso delle conoscenze scientifiche[29].

È certo che una distinzione ordinata in base al grado di sofisticazione dei sistemi, del loro livello di autoapprendimento, nonché del rischio generato dall'immissione nel mercato del prodotto o dall'utilizzo dell'algoritmo, rischio accettato e compatibile con l'utilità sociale della condotta – ancorché pericolosa – cui ine-

[29] Ai fini di tutela del paziente danneggiato, la giurisprudenza della Corte di giustizia tende alleggerire l'onere probatorio riguardo al difetto del singolo esemplare, quando si tratti di prodotti in serie, in contrapposizione all'orientamento della Cassazione che, nel definire "presunta" la responsabilità da prodotto, richiede la prova del collegamento causale tra il difetto del prodotto (non tra prodotto) e il danno subito. Così, ad esempio, nel noto caso della difettosità di un dispositivo medico accertata sulla base di un esemplare e non di una serie, deciso dalla CGUE 5.3.2015, C-503/13 e C-504/13, cit. Ammette il ricorso a metodi anche indiziari per ricavare la difettosità del prodotto CGUE, 21.6.2017, C-621/15, caso *Sanofi Pasteur MSD SNC*, in *Dejure*, riguardante i danni da vaccino contro l'epatite B. Adotta un criterio più rigoroso nel senso della natura presunta della responsabilità del produttore che impone la prova del collegamento tra difetto e danno e non tra prodotto e danno: Cass., 24.9.2018, n. 23447, in *Dejure;* Cass., 29.5.2013, n. 13458, in *Giust. civ.*, 2013, I, p. 1979. *Contra:* Cass. 8.10.2007, n. 20985, in *Foro it.*, 2008, I, 1, c. 143, che, in un caso di protesi mammaria difettosa, aveva ritenuto la responsabilità dell'azienda produttrice sulla base della constatazione che la protesi aveva dato luogo ad un "risultato anomalo".

risce, soprattutto in medicina, è in linea con il riconoscimento del diritto del danneggiato di "raggiungere" facilmente il responsabile anche quando la decisione, nell'ambito di un processo automatizzato, venga delegata ad un sistema (*software* o servizio ad esso collegato) che svolge l'azione, anche per conto di altri soggetti (talora il livello di sofisticazione del sistema e l'articolazione del processo tecnologico non consentono un'agevole individuazione del soggetto responsabile, come, ad esempio, nei sistemi di *deep learning*). Quando il processo evolutivo della tecnologia è rapido, il rischio è difficilmente calcolabile *ex ante*, sicché al legislatore spetta il compito di dettare una disciplina che permetta di coinvolgere tutti i soggetti del processo causale in grado di esercitare un controllo.

Il livello di rischio e delle sue conseguenze, che costituisce già un fattore di valutazione dell'ammissibilità di vari processi industriali, della gestione dei dati riservati e della sicurezza sul lavoro, rappresenta nelle risoluzioni e nella proposta di regolamento europeo un elemento necessario per pervenire alla determinazione del regime di responsabilità in materia di *AI* e robotica, operando anche come parametro di gradazione della responsabilità.

Diverso il regime proposto dalla direttiva UE sulla responsabilità per danno da prodotti difettosi del 28.9.2022 che, secondo regole analoghe a quelle fissate nella contestuale proposta di direttiva sull'intelligenza artificiale, descrive un sistema fondato sulla responsabilità per colpa corredato da presunzioni che alleggeriscono l'onere probatorio del danneggiato, scegliendo una soluzione di compromesso, con l'intento di contemperare il diritto al risarcimento del danneggiato con le esigenze di produzione e l'evoluzione tecnologica.

Se applicata in materia sanitaria la direttiva confermerebbe l'adozione di un criterio di imputazione della responsabilità ricalcato sulla normativa in tema di responsabilità del produttore vigente, richiedendo al danneggiato di provare il carattere difettoso del prodotto, il danno subito e il nesso di causalità tra il difetto e il danno (art.9), ma con il favore di una serie di presunzioni che consentono di accertare la difettosità del prodotto se è data prova: b) della mancanza dei requisiti obbligatori di sicurezza stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno verificatosi o c) di un malfunzionamento evidente del prodotto durante l'utilizzo normale o in circostanze ordinarie (analogamente a quanto prescritto nelle risoluzioni già citata). Inoltre, il meccanismo di presunzioni delineato nella proposta, nella finalità di facilitare il danneggiato nell'estrema difficoltà o impossibilità di individuare dare la prova in presenza di particolari meccanismi di funzionamento e caratteristiche tecnologiche, permette di pervenire all'affermazione della responsabilità sulla base della presunzione del nesso di causalità tra il carattere difettoso del prodotto e il danno "*nel caso in cui sia stato provato che il prodotto è difettoso e che la natura del danno cagionato è generalmente coerente con il difetto in questione*".

A mitigare il criterio della colpa, infine, nel 4° comma dell'art. 9, il legislatore europeo, in presenza di "difficoltà eccessive" nella dimostrazione del carattere difettoso del prodotto, del nesso di causalità tra difetto e del danno o di entrambi gli elementi per la complessità tecnica o scientifica, traccia una disciplina secondo cui "*si presumono il carattere difettoso del prodotto, il nesso di causalità tra difetto e danno o entrambi tali elementi se l'attore ha dimostrato, sulla base di elementi di prova sufficientemente pertinenti, che: a) il prodotto ha contribuito a cagionare il danno; b) è probabile che il prodotto fosse difettoso, oppure che il carattere difettoso dello stesso è una causa probabile del danno, o entrambi tali elementi*"[30].

L'effetto cui tendono le proposte più recenti, a parte la complessità dell'apparato meccanismo probatorio, non è tuttavia dissimile da quello disegnato dall'Unione Europea negli atti che propendono per l'adozione di un regime di responsabilità per rischio, idoneo ad assolvere adeguatamente alla sua funzione soprattutto nelle situazioni in cui il meccanismo automatizzato non può essere manomesso dall'intervento umano e l'identificazione dei fattori soggettivi (l'agente) e oggettivi (il difetto e l'onere probatorio) della fattispecie concreta è complessa per il grado di specializzazione tecnologica del dispositivo o del processo di AI.

La soluzione della sulla base dedistinzione tra diverse scale tipologie di rischio – che in medicina si assestano sempre su un l livello "alto", soggetto ad un maggiore rigoreconsiderata l'importanza del diritto alla salute del paziente sul quale incidono in medicina i sistemi di AI – può essere percorsa, ma determina una duplicazione di regime; l'alternativa basata sulla colpa evoca il dubbio che il sistema probatorio articolato e complesso basato sulle presunzioni, di non agevole lettura, promosso nel testo sia idoneo a realizzare l'obiettivo di offrire, in un settore popolato da soggetti fragili (i pazienti), un rapporto equilibrato tra incentivo allo sviluppo del settore tecnologico e protezione dei diritti delle persone.

Un nuovo paradigma in campo sanitario dovrebbe forse tenere conto della necessità di una valutazione del rischio di danno in rapporto al livello di automazione e al grado di sofisticazione dei sistemi/prodotti/processi/servizi ad oggi conosciuti, considerandone le diverse gradazioni, calibrate secondo tabelle istitutive dei presupposti di conformità e indicative della tipologia e delle caratteristiche tecnologiche del sistema e accreditare una disciplina che, anche basata su un sistema di presunzioni, preservi la fiducia del paziente nella tecnologia, fornendo al contempo tutti gli strumenti necessari a garantire un'adeguata tutela in caso di violazione dei suoi diritti.

---

[30] Le cause di esclusione di responsabilità del produttore sono indicate nell'art. 10 della proposta in esame. Il tema è oggetto di approfondimenti nello scritto di M. Faccioli, *Intelligenza artificiale e responsabilità sanitaria,* in *Nuova giur. civ. comm.,* 2023, p. 732.

I QUADERNI DELLA SSM

nella stessa collana

Quaderno 1 – Bioetica e biodiritto

Quaderno 2 – Raccolta delle fonti e delle principali delibere della Scuola superiore della magistratura

Quaderno 3 – Comunione e condominio

Quaderno 4 – Diritti e obblighi del lavoratore all'epoca COVID

Quaderno 5 – Il trattamento dei dati personali in ambito giudiziario

Quaderno 6 – Storia della magistratura

Quaderno 7 – I metodi di risoluzione alternativa delle controversie: Focus su mediazione, negoziazione assistita e conciliazione giudiziale

Quaderno 8 – Il procedimento disciplinare dei magistrati

Quaderno 9 – L'ordinamento giudiziario

Quaderno 10 – L'evoluzione della responsabilità civile

Quaderno 11 – I diritti fondamentali fra Carte e Costituzioni europee

Quaderno 12 – Dieci anni di Scuola superiore della magistratura (2011-2021)

Quaderno 13 – Il diritto dei contratti e l'emergenza sanitaria

Quaderno 14 – Il diritto tributario nella prospettiva penale e civile

Quaderno 15 – Giustizia digitale

SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

I QUADERNI DELLA SSM

nella stessa collana

Quaderno 16 – Il nuovo diritto di famiglia

Quaderno 17 – L'etica giudiziaria

Quaderno 18 – Gli assetti organizzativi dell'impresa

Quaderno 19 – Intercettazioni di comunicazioni e tabulati

Quaderno 20 – Il giudizio civile di cassazione

Quaderno 21 – Scienza e diritto penale

Quaderno 22 – Il diritto dell'immigrazione

Quaderno 23 – Composizione negoziata della crisi di impresa e concordato semplificato

Quaderno 24 – Contratto, contratti e mercati

Quaderno 25 – Le criticità del sistema giustizia: dall'irragionevole durata del processo all'ingiusta detenzione

Quaderno 26 – Le fonti del diritto, il ruolo della giurisprudenza e il principio di legalità

Quaderno 27 – Il nesso di causalità nel diritto civile e nel diritto penale

Quaderno 28 – Rapporto di ricerca - La valutazione di medio-lungo periodo dei corsi di formazione iniziale e dei corsi di formazione permanente organizzati dalla Scuola superiore della magistratura

Quaderno 29 – Le sanzioni amministrative

Quaderno 30 – I reati concernenti gli stupefacenti

SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

Finito di stampare nel mese di febbraio 2024
a cura dell'Istituto Poligrafico e Zecca dello Stato S.p.A.