Francesco Delfini

Le discipline a tutela del consumatore e il coordinamento con la proposta di Regolamento MiCA

(doi: 10.4478/106711)

Osservatorio del diritto civile e commerciale (ISSN 2281-2628)
Fascicolo Speciale, settembre 2022

Ente di afferenza:
()

Le discipline a tutela del consumatore e il coordinamento con la proposta di Regolamento MiCA

Francesco Delfini

Consumer Protection Rules and their Coordination with the Proposed MiCA Regulation

The paper addresses – as was the lecture from which it stems, held on September 15, 2022 at the symposium «*La nuova disciplina europea dei mercati digitali: nuovi paradigmi dell'autonomia contrattuale*», hosted by the Milan School of Law at UNIMI – the recent proposal of MICA (Markets in Crypto-Assets) Regulation. It deals with the impact of the proposed regulation on the consumer protection provisions and with the legal issues raised, on the one hand, by the blockchain architecture, compared to the less energy requiring permissioned and semi permissioned ledgers and raised, on the other hand, by Smart Contracts in respect to the common rules of the Contract law.

Keywords: Token, Consumer Protection, Smart Contracts, Crypto-Activities.

1. Gli obiettivi di tutela del consumatore evidenziati dalle Autorità europee di vigilanza

Nella «avvertenza» ESA 2022/15 delle Autorità Europee di Vigilanza (ESMA, EBA e EIOPA: le AEV)[1] sono evidenziati i rischi, per i consumatori, connessi alle cripto-attività (CA) e dunque gli obiettivi di un intervento regolatorio dell'Unione[2]:

[1] *European Securites and Markets Authority, European Banking Autority* e *European Insurance and Occupational Pensions Authority.*

[2] Si legge, infatti, nella «avvertenza»: «Le autorità di regolamentazione del settore finanziario dell'UE mettono in guardia i consumatori sui rischi delle cripto-attività. Le autorità europee di vigilanza (ABE, ESMA e EIOPA – le AEV) avvertono i consumatori che numerose cripto-attività sono altamente rischiose e speculative. Queste cripto-attività non sono adatte per la maggior parte dei consumatori al dettaglio come investimento o mezzo di pagamento o scambio. Qualora acquistino queste attività, i consumatori potrebbero esporsi alla possibilità molto concreta di perdere tutto il denaro investito. I consumatori dovrebbero prestare attenzione ai rischi di pubblicità ingannevole, anche attraverso i social media e gli influencer. I consumatori dovrebbero essere particolarmente cauti nei confronti dei rendimenti rapidi o elevati promessi, specialmente quelli che sembrano troppo allettanti per essere veri. I consumatori dovrebbero essere consapevoli della mancanza di ricorso o protezione a loro disposi-

1) volatilità e rischiosità delle CA anche in relazione alla possibile «perdita di tutto il capitale investito»;

2) scarsa adeguatezza rispetto agli obiettivi di risparmio del consumatore e scarsa attitudine delle CA all'impiego quali mezzi di pagamento;

3) possibile pubblicità ingannevole sulle caratteristiche delle CA, anche attraverso canali non ufficiali, come social media e c.d. «influencer»;

4) assenza di attuale protezione normativa europea, stante la mancata ricomprensione delle CA nell'ambito di applicazione delle attuali norme UE sui servizi finanziari;

5) mancata consapevolezza, nei consumatori, del rilevante impatto ambientale delle CA più diffuse.

Si tratta di profili di rischio che richiedono interventi regolatori che ben rientrano nei più ampi diritti fondamentali riconosciuti ai consumatori dal nostro codice del consumo (Decreto Legislativo. 6 settembre 2005, n. 206), come descritti in modo programmatico dall'art. 1, co. 2 del medesimo, ove sono «riconosciuti come fondamentali», fra gli altri:

– alla lett. *a*), quello «alla tutela della salute» – pregiudicato dall'enorme *carbon footprint* dei sistemi di *blockchain* basati sulla ormai ecologicamente insostenibile *proof of work*;

– alla lett. *b*), quello alla «sicurezza e alla qualità» dei *servizi*, che richiede una ponderazione di adeguatezza delle CA per il paniere del consumatore, vocato essenzialmente alla difesa del risparmio: quest'ultimo, obiettivo tutelato costituzionalmente (art. 47 co.1 Cost.);

– alla lett. *c*), quello ad una «adeguata informazione e a una corretta pubblicità» e alla lett. c-bis) quello all'«esercizio delle pratiche commerciali secondo principi di buona fede, correttezza e lealtà»: il che impone di contrastare ogni pubblicità ingannevole, specie se attuata con i più invasivi mezzi di comunicazione;

– alla lett. *d*), quello alla «educazione al consumo» che, ancorché con formulazione paternalistica, impone al legislatore di rendere consapevoli, al di là delle declamazioni miracolistiche della vulgata sulla *blockchain*, dei gravi rischi di compromissione climatica e di sperpero di energia che tale tecnologia, specie se basata sulla *proof of work*, comporta.

zione, in quanto le cripto-attività e i prodotti e servizi correlati in genere non rientrano nella protezione esistente ai sensi delle attuali norme UE sui servizi finanziari. [...] Alla data di questa avvertenza, esistono più di 17 000 cripto-attività distinte, alcune delle quali sono a volte indicate come le cosiddette "valute virtuali" o "monete" o "token" digitali. Le cripto-attività più importanti fino ad oggi includono bitcoin ed ether, che insieme rappresentano circa il 60% della capitalizzazione di mercato totale delle cripto-attività. Il consumo di energia di alcune cripto-attività è elevato, ad esempio è legato ai processi di mining e convalida, e i consumatori dovrebbero essere consapevoli del loro impatto ambientale».

2. La tutela del consumatore nella proposta di Regolamento MiCA

Quanto segnalato nella predetta «avvertenza» ben sintetizzava, dunque, l'agenda per il legislatore europeo, nelle sue varie articolazioni istituzionali, secondo gli art. 289 e 294 del TFUE.

La risposta dell'Unione, a tali potenziali rischi, per il consumatore, portati dalle nuove tecnologie si è tradotta nella proposta di Regolamento MiCA (MICA o Reg.)[3] concepita dalla Commissione, proposta che muove dalla tradizionale definizione del consumatore come «qualsiasi persona fisica che agisca per scopi che non rientrano nella sua attività commerciale, imprenditoriale, artigianale o professionale» (art. 3, co.1, n. 28) e il cui ambito di applicazione, secondo l'art. 1 lett. d), annovera anche la armonizzazione, con norme uniformi, delle «disposizioni a tutela dei consumatori per quanto riguarda l'emissione, la negoziazione, lo scambio e la custodia delle cripto-attività» (art. 1 lett. d) MICA).

L'ambito di applicazione del Reg. va poi ricostruito alla luce della definizione di «cripto-attività» (CA) data dall'art. 3 co.1, n. 2: «Una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tec-

[3] Il 30 giugno 2022 il Consiglio e il Parlamento hanno raggiunto un accordo provvisorio sulla proposta di regolamento relativo ai mercati delle cripto-attività (come previsto dalla procedura legislativa ordinaria, tale proposta era stata presentata dalla Commissione il 24 settembre 2020): il relativo comunicato stampa si legge su: https://www.consilium.europa.eu/it/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/#:~:text=Il%20regolamento%20MiCA%20protegger%C3%A0%20i,al%20di%20fuori%20dall'UE. Il raggiungimento di tale accordo provvisorio attraverso il c.d. sistema dei triloghi (i.e. riunioni informali tripartite sulle proposte legislative con rappresentanti di Parlamento, Consiglio e Commissione) segna la conclusione della prima fase della procedura legislativa ordinaria di cui all'art. 294 TFUE. Come noto, perché un atto normativo sia approvato secondo la procedura legislativa ordinaria, i co-legislatori – Consiglio e Parlamento – devono concordare un testo comune, avviando un negoziato politico in sede di c.d. triloghi (che, nel caso di specie, erano iniziati il 31 marzo 2022). L'accordo raggiunto in sede di trilogo (proposta di regolamento qui in oggetto) è provvisorio e deve essere approvato secondo le procedure formali applicabili in forza dei regolamenti interni di ciascuna Istituzione. Più in dettaglio, nel caso del Parlamento, ai sensi del 4° comma dell'art. 69 *septies*, l'accordo provvisorio deve essere presentato alla commissione competente, che deciderà se approvarlo con votazione unica, a maggioranza dei voti espressi; se approvato, l'Accordo verrà sottoposto all'esame in aula dopo la messa a punto giuridico-linguistica. Una volta che tale accordo sia stato formalmente approvato dal Consiglio e dal Parlamento, il Presidente del Parlamento firmerà l'atto insieme a un rappresentante della Presidenza di turno del Consiglio, conformemente all'art. 297 TFUE. Dopo la firma, il testo sarà pubblicato in G.U. e, salvo diversa previsione, entrerà in vigore e diverrà direttamente applicabile il 20° giorno successivo alla pubblicazione.

nologia analoga», completata da quella di «tecnologia di registro distribuito (DLT)»: un tipo di *tecnologia che supporta la registrazione distribuita di dati cifrati* (dall'art. 3 co.1, n. 1).

In negativo, poi, l'ambito di applicazione va ricostruito con le esenzioni *oggettive* di cui all'art. 2, co. 2 – che esclude le cripto-attività che rientrano nella definizione di: *(a)* strumenti finanziari ai sensi dell'articolo 4, paragrafo 1, punto 15, della direttiva 2014/65/UE; *(b)* moneta elettronica quale definita all'articolo 2, punto 2, della direttiva 2009/110/CE, tranne quando rientrano nella definizione di token di moneta elettronica ai sensi del presente regolamento; *(c)* depositi ai sensi dell'articolo 2, paragrafo 1, punto 3, della direttiva 2014/49/UE del Parlamento europeo e del Consiglio[4]; *(d)* depositi strutturati ai sensi dell'articolo 4, paragrafo 1, punto 43, della direttiva 2014/65/UE; *(e)* cartolarizzazione ai sensi dell'articolo 2, punto 1, del regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio[5] – e *soggettive*, di cui al medesimo art. 2 co. 3.

Il Reg. detta una disciplina ripartendo in tre categorie le CA e distinguendo tra: 1) «token collegato ad attività» (i c.d. *stable coins*); 2) «token di moneta elettronica» e 3) «Cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica», tra le quali, per taluni aspetti, possono rientrare i c.d. *non fungible tokens*[6]: NFT, che non sono specificamente definiti nella MICAr e su cui si torneà *infra*[7].

[4] Direttiva 2014/49/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativa ai sistemi di garanzia dei depositi (GU L 173 del 12.6.2014, p. 149).

[5] Regolamento (UE) 2017/2402 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, che stabilisce un quadro generale per la cartolarizzazione, instaura un quadro specifico per cartolarizzazioni semplici, trasparenti e standardizzate e modifica le direttive 2009/65/CE, 2009/138/CE e 2011/61/UE e i regolamenti (CE) n. 1060/2009 e (UE) n. 648/2012 (GU L 347 del 28.12.2017, pag. 35).

[6] Ad es. l'art. 4.2. lett. c) eccettua dalla disciplina del primo comma – tra cui l'obbligo di redazione del white paper – tra le altre, le cripto-attività che «sono uniche e non fungibili con altre cripto-attività», tra cui rientrano i c.d. NFT.

[7] Articolo 3: Definizioni: 1. Ai fini del presente regolamento si applicano le definizioni seguenti: (1) «tecnologia di registro distribuito (DLT)»: un tipo di tecnologia che supporta la registrazione distribuita di dati cifrati; (2) «cripto-attività»: una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga; (3) «token collegato ad attività»: un tipo di cripto-attività che intende mantenere un valore stabile facendo riferimento al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività; [c.d. STABLE COIN]; (4) «token di moneta elettronica»: un tipo di cripto-attività il cui scopo principale è quello di essere utilizzato come mezzo di scambio e che mira a mantenere un valore stabile facendo riferimento al valore di una moneta fiduciaria avente corso legale; (5) «utility token»: un tipo di cripto-attività destinato a fornire l'accesso digitale a un bene o a un servizio, disponibile mediante DLT, e che è accettato solo dall'emittente di tale token».

2.1. La disciplina relativa alle «cripto-attività *diverse* dai token collegati ad attività o dai token di moneta elettronica»

Iniziando da quest'ultima categoria residuale, quella delle «cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica», va sottolineato che la disciplina è la più snella tra quelle dettate dal MICAr, non essendo previsto alcun regime di autorizzazione per le *offerte al pubblico o l'ammissione alla negoziazione su una piattaforma di negoziazione di cripto-attività.* La tutela del consumatore è infatti essenzialmente imperniata (art. 4) su di un obbligo di *informazione preventiva*, gravante sull emittente, da veicolarsi con la redazione di un *white paper*, con i contenuti di cui all'art. 5, e sul diritto di *recesso di pentimento* (art. 12), analogo a quello stabilito in via generale nel Codice del consumo (d.lg. 206/2005: cod. cons.) agli artt. 52 ss.

L'art. 14 completa infine la disciplina degli artt. 4 e 5, prevedendo una responsabilità risarcitoria dell'emittente per informazioni incomplete, non corrette o poco chiare, oppure fuorvianti contenute nel *white paper* sulle cripto-attività: responsabilità accostabile a quella di cui agli artt. 1337 e 1440 cod. civ., resi comunque applicabili anche in virtù della clausola di salvaguardia del comma 4 dell'art. 14 medesimo (e nella misura in cui si ritenga sanzionabile in base a tali norme, quale dolo civilistico, anche una condotta meramente colposa e finanche omissiva, argomentando estensivamente dalle norme di settore, previste per le informazioni inesatte e le reticenze nel contratto di assicurazione)[8].

2.2. La disciplina relativa ai «token collegati ad attività»

La disciplina relativa ai «token collegati ad attività» è più restrittiva, richiedendosi, oltre alla informativa di cui al *white paper* (in questo caso soggetto ad approvazione e con il contenuto di cui all'art. 17), una *previa autorizzazione* dello stato di origine per l'offerta al pubblico o la negoziazione su piattaforma nell'Unione.

Dispone infatti l'art. 15: «1. Nessun emittente di token collegati ad attività offre tali token al pubblico nell'Unione o chiede l'ammissione di tali attività alla negoziazione su una piattaforma di negoziazione di cripto-attività nell'Unione, a meno che detto emittente non abbia ricevuto l'apposita autorizzazione dall'autorità competente del suo Stato membro d'origine conformemente all'articolo 19…».

Anche per tale categoria, la diciplina è poi completata (art. 22) dalla responsabilià risarcitoria per omesse, infedeli o fuorvianti informazioni ai

[8] Cfr. artt. 1892-1893 cod. civ.

consumataori, che pregiudichino la valutazione di opportunità dell'investimento.

Per gli emittenti tali categorie di CA è poi ribadito e dettagliato, nell'art. 23, un obbligo di *correttezza* che in via generale è previsto dall'art. 1337 cod. civ., per la fase precontrattuale, e dagli artt. 1175 e 1375 cod. civ., durante il rapporto contrattuale. È inoltre esplicitato un obbligo di *non discriminazione*, che in via generale non si trova nella parte generale del codice civile.

Gli artt. 32, 33 e 34 prevedono, poi, regole di impiego prudenziale in attività di riserva – esclusivamente in attività sicure e a basso rischio – a garanzia dei token collegati ad attività.

Il titolo III, capo 5, artt. 39 ss. Reg. prevede, infine, un regime aggiuntivo ed aggravato, qualora il token collegato ad attività sia qualificabile, dalla EBA o su richiesta dell'emittente, come token «significativo». I parametri indicati nel Reg. per tale qualificazione sono: le dimensioni della clientela dei promotori dei token collegati ad attività, il valore dei token collegati ad attività o la loro capitalizzazione di mercato, il numero e il valore delle operazioni, l'entità della riserva di attività, la rilevanza delle attività transfrontaliere degli emittenti e l'interconnessione con il sistema finanziario.

2.3. La disciplina relativa ai «token di moneta elettronica»

Anche per i Token di moneta elettronica – CA utilizzabili come mezzo di scambio e facenti riferimento al valore di una moneta fiduciaria avente corso legale – il Reg. prevede un regime *autorizzatorio*, che involge anche lo *status* dell'emittente quale «ente creditizio o "istituto di moneta elettronica" ai sensi dell'articolo 2, punto 1, della direttiva 2009/110/CE» (art. 43) ed indica dettagliatamente i contenuti del relativo *white paper* all'art. 46. Per tale categoria di token, poi, è prevista espressamente la rimborsabilità in qualsiasi momento (art. 44).

L'art. 47 della proposta di Reg. reca poi, come per le altre categorie, una specifica disciplina di responsabilità per le informazioni contenute nel *white paper*.

Infine, il titolo IV, capo 2, artt. 50 ss. prevede un regime aggiuntivo ed aggravato (tra cui l'applicabilità dell'art. 33 sulla custodia delle attività di riserva e dell'art. 34 sull'investimento di tali attività), qualora il token di moneta elettronica sia qualificabile, dalla EBA o su richiesta dell'emittente, come token «*significativo*», secondo i medesimi criteri indicati all'art. 39 per i token significativi *collegati ad attività*.

3. Gli obiettivi di tutela del consumatore *non accolti* e i profili *non trattati* nella versione attuale della Proposta MICA

Nella versione definitiva della proposta di regolamento risultano trattati numerosi tra i profili di necessaria tutela del consumatore evidenziati dalle Autorità europee di vigilanza, *ma non tutti*.

Inoltre, la disciplina di tutela recata dalla proposta si incentra su un limitato numero di strumenti, quali quello della informazione veicolata dal *white paper* (e della correlativa responsabilità precontrattuale), e quello del recesso.

Anche la tripartizione delle cripto-attività è in qualche misura arbitraria e delinea in positivo solo alcuni dei token presenti nella prassi, relegando alla categoria residuale definita in negativo (quella «cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica») il ruolo di contenitore di altre ben note figure di token presenti sul mercato, quali i NFT.

Per essi, una definizione stipulativa, dotata di qualche autorevolezza, può leggersi nel documento di Borsa Italiana che li descrive come segue: «Gli NFT sono dei "certificati digitali" basati sulla tecnologia blockchain volti a identificare in modo univoco, insostituibile e non replicabile la proprietà di un prodotto digitale. Acronimo di *Non-Fungible Token* (token non fungibili), gli NFT sono una delle applicazioni della finanza decentralizzata: un insieme di servizi e processi che vengono automatizzati grazie all'ausilio di contratti intelligenti (*smart contract*) e senza la presenza di intermediari. Si tratta dunque di un nuovo paradigma nella gestione del diritto di proprietà. Acquistare un NFT non comporta l'ottenimento della proprietà dell'opera bensì la possibilità di dimostrare un diritto su quell'opera, attraverso uno *smart contract* che esegue automaticamente un contratto che viene registrato in modo indelebile sulla blockchain»[9].

[9] Il necessario legame tra crypto attività e *blockchain*, che ne costituisce la impalcatura tecnica, è ben evidenziato nel *Report* del marzo 2018, dell'*US Senate Joint Economic Committee*, che così si esprime: «What are cryptocurrencies and blockchain? Blockchain is the distributed ledger technology that underlies digital currencies such as Bitcoin. A ledger is the accounting tool that tracks the movement of money from one person or account to another. Conventionally, such records are stored in central locations like banks, headquarters, and Paypal servers. Blockchain revolutionizes ledger technology with a network of distributed ledgers. Instead of one central, authoritative record of all transactions or information, blockchain creates potentially thousands of identical ledgers in computers and servers all over the world. In "permissionless" proof-of-work blockchain, people compete to validate each transaction in return for a reward. The protocol rewards users for creating and validating entries into the ledger. This reward creates an incentive for competition and gives these validators new tokens to use in the system. Users who do not earn tokens by performing verifications, i.e., not "miners", must buy the tokens. This interplay between miners and purchasers creates an

Il fenomeno economico che la proposta mira a regolare – soprattutto per colmare un vuoto di tutela dei consumatori che investano in token – presuppone una tecnologia alla quale il regolamento fa sintetico riferimento all'art. 1, n. 1 delle definizioni – quella dei cosiddetti *Distributed Ledgers* (DLT) – cui comunemente ci si riferisce con il termine di *blockchain*[10], e implicitamente e necessariamente richiama – con il sintetico riferimento sopramenzionato ai

ecosystem where people have clear incentives and rewards to maintain the distributed ledger for everyone. Bitcoin was the first blockchain. Bitcoin's network creates a new record of verified transactions approximately every ten minutes and packages the records into a so-called "block". Ethereum is the second-largest cryptocurrency in the world, and though it uses the same blockchain technology as Bitcoin, it serves different purposes. While Bitcoin's blockchain records each transaction in its currency, Ethereum records results from the programs users upload to its network. It allows programmers to create applications and "smart contracts" that utilize computing power from Ethereum's network to execute them. This brings the decentralized security of blockchain to computing power, while allowing developers to build applications, smart contracts, and other digital coins on top of Ethereum. Additionally, it uses the same proof-of-work mining that Bitcoin does, but its network produces a block every 12 to 15 seconds and rewards its miners three ethers per block, with additional rewards for solutions found but not included».

[10] Secondo la descrizione datane dal documento di Borsa italiana (FTA Online News, Milano, 15 maggio 2022, 11: 30): «Blockchain, letteralmente "catena di blocchi", è un paradigma tecnologico che permette di sviluppare applicazioni basate su un sistema decentralizzato di condivisione e validazione delle informazioni dalle numerose applicazioni. Una delle prime è stata il protocollo Bitcoin e il mondo delle criptovalute, ma si moltiplicano sempre più spesso gli impieghi delle applicazioni blockchain o registro condiviso (Distributed Ledger Tecnology – DLT) ai settori più diversi. Il nome deriva dalla sua natura distribuita: ogni nodo del network svolge un ruolo nella verifica delle informazioni, inviandole al successivo e fissando le informazioni e transazioni su cui tutti i nodi concordano in una catena composta da blocchi, blockchain appunto, condivisa ed immutabile. Il modello si basa sulla combinazione tra firma digitale e marca temporale (*time stamp*). La prima garantisce che mittente e destinatario (o meglio i loro indirizzi digitali ID) di un qualsiasi tipo di messaggio, compresa una transazione monetaria, siano identificati in modo certo. Il secondo permette che un insieme di messaggi, validato con la marca temporale da parte di un nodo scelto casualmente da un robusto modello matematico, venga comunicato e scritto nel registro di tutti gli altri nodi della rete e reso irreversibile. Si tratta di un vero e proprio un registro pubblico e condiviso, un libro contabile che si aggiorna automaticamente ed identicamente su ciascuno dei nodi che partecipano alla rete. Tutte le operazioni effettuate sono confermate dai singoli nodi attraverso software di crittografia che verificano un pacchetto di dati siglati con chiave privata, utilizzato per firmare le transazioni e per poterle controllare in qualsiasi momento. Tutto il sistema garantisce l'identità digitale di chi ha autorizzato gli scambi, intesa principalmente come ID, ossia come indirizzo digitale di un conto non necessariamente ricollegabile a un individuo o a una società. La caratteristica principale del processo è che il funzionamento non è garantito da un ente centrale, bensì ogni singola transazione viene validata ed approvata dall'interazione di tutti i nodi. Le transazioni che avvengono all'interno della rete vengono così registrate e validate eliminando in definitiva la necessità di terze parti "fidate". La conferma da parte di tutti i nodi della rete, necessaria affinché qualunque nuovo elemento venga inserito nella blockchain, crea una garanzia condivisa».

NFT – una ormai ben nota categoria di contratti, quella degli *smart contracts*, frutto della ibridazione tra l'autonomia privata e gli strumenti di intelligenza artificiale.

4. (*Segue*). L'insostenibile voracità energetica della *blockchain* basata sulla *proof of work*, evidenziata nei *recitals* 5a) e 5aa) poi caduti nella versione attuale del MiCAR

Il primo tema, quello della *blockchain* e della sua connotazione altamente energivora, qualora la ricerca del consenso tra i nodi sia basata sulla c.d. *proof of work*, era stato oggetto di una delle preoccupazioni evidenziate nella «avvertenza» ESA 2022/15», di cui si è detto *supra.*

Esso aveva trovato ingresso nei *Recitals* 5a) e 5aa), indicati dal Parlamento Europeo, ma poi caduti nell'attuale testo della MICA.

I *Recitals* denunciavano il problema come segue: «(5a) The consensus mechanisms used for the validation of transactions have a *substantial environmental impact.* That is particularly the case for the consensus mechanism known as *proof-of-work*, which requires participating miners to solve computational puzzles and compensates them in proportion to their computational effort. Rising prices of the associated cryptoasset, as well as the frequent replacement of mining hardware, create incentives for increases in computational power. As a result, *proof-of-work is today often associated with high energy consumption, a material carbon footprint and significant generation of electronic waste. Those characteristics might undermine Union and global efforts to achieve climate and sustainability goals, until other more climate friendly and non-energy intensive solutions emerge.* The best-known application of the proof-of-work consensus mechanism is Bitcoin. *According to many estimates, the energy consumption of the Bitcoin network equals that of entire countries.* Moreover, *during the period 1 January 2016 to 30 June 2018, the Bitcoin network was responsible for up to 13 million metric tons of CO2 emissions.* It has been estimated that each Bitcoin transaction deploys 707 kWh of electricity power. *The increasing energy consumption is accompanied by a growth in mining equipment and the generation of significant electronic waste.* It is therefore necessary to highlight the need for consensus mechanisms *to deploy more environmentally friendly solutions* and for the Commission to identify those consensus mechanisms that could pose a threat to the environment having regard to energy consumption, carbon emissions, depletion of real resources, electronic waste and the specific incentive structures. *Unsustainable consensus mechanisms should only be applied on a*

small scale»; «(5aa) *Crypto-assets relying on the proof-of-work consensus mechanism in order to validate transactions indirectly cause considerable carbon emissions and affect the climate and the environment negatively. That is due to proof-of-work's intensive and inefficient use of electricity*, often generated from fossil energy sources located outside the Union. *The deployment of the proof-ofwork method, as it presently stands, is unsustainable and undermines the achievement of the climate objectives under the Paris Agreement.* However, as other industries (such as the video games and entertainment industry, data centres, certain tools deployed in the financial and banking industry and beyond) also consume energy resources which are not climate friendly, it is an important issue for the Union to tackle in its environmental legislation, as well as in its relationships and agreements with third countries on a global scale. In that context, the Commission should work towards a holistic legislative approach, which is better placed to address such issues in a horizontal manner. *A crypto-asset white paper relying on the proof-of-work method should include an independent assessment of the crypto-asset's likely energy consumption*»...[11]

Il tema della *blockchain*[12] è connesso al sistema di cifratura a doppia chiave asimmetrica, su cui è basata l'architettura di firma digitale con cui hanno ormai familiarizzato numerose categorie professionali e gruppi di cittadini.

Ma non tutti coloro che oggi discettano di *blockchain* – e per certo non i consumatori interessati ai token, che le avvertenze delle Autorità economiche europee miravano a rendere consapevoli – sanno che la *blockchain* richiede, per la cifratura di ogni blocco (costituito da una ingentissima massa

[11] *Recitals* 5a) e 5aa) (mie sottolin.).

[12] Una definizione comune e descrittivamente corretta del fenomeno si legge su https://it.wikipedia.org/wiki/Blockchain: «Una blockchain è fondamentalmente un registro aperto e distribuito che può memorizzare le transazioni tra due parti in modo sicuro, verificabile e permanente. Una volta scritti, i dati in un blocco non possono essere retroattivamente alterati senza che vengano modificati tutti i blocchi successivi ad esso e ciò, per la natura del protocollo e dello schema di validazione, necessiterebbe il consenso della maggioranza della rete. La blockchain è una lista in continua crescita di record, chiamati *block*, che sono collegati tra loro e resi sicuri mediante l'uso della crittografia. Ogni blocco della catena contiene un puntatore hash come collegamento al blocco precedente, un *time stamp* e i dati della transazione. La natura distribuita e il modello cooperativo rende robusto e sicuro il processo di validazione, ma presenta tempi e costi non trascurabili, dovuti in gran parte al prezzo dell'energia elettrica necessaria per effettuare la validazione dei blocchi. L'autenticazione avviene tramite la collaborazione di massa ed è alimentata da interessi collettivi. Il risultato di tutto ciò è un flusso di lavoro robusto dove non è necessaria la competenza dei partecipanti in materia di sicurezza dei dati. L'utilizzo di questa tecnologia consente anche di superare il problema dell'infinita riproducibilità di un bene digitale e della doppia spesa senza l'utilizzo di un server centrale o di un'autorità».

di dati[13]) e la necessaria estrazione, con funzioni di *hash*[14], di *digest* della serie di blocchi via via succedutisi, consumi di energia elettrica massivi, come è testimoniato dall'esodo dei centri computazionali dei *bitcoin miners* verso il *far East,* dove il costo per KW elettrico – magari prodotto bruciando carbone – è minore (e vi è meno sensibilità per i problemi climatici[15]).

Né tutti tutti coloro, che oggi invocano un impiego della *blockchain* quasi fosse una panacea per ogni tipo di transazione telematica, sono consapevoli della connessa perenne necessità di allungamento delle chiavi di cifratura, per considerarle probabilisticamente sicure, e della frequente impostazione, negli attuali sistemi di *blockchain* (specie in quelli di cripto valute, come *bitcoin),* del problema informatico della ricerca del «consenso»[16] sul

[13] Nell'agosto del 2014 la dimensione del blockchain del bitcoin era di circa 20 gigabyte, nel marzo 2018 è arrivato alla dimensione di 162,4 gigabyte (fonte https://it.wikipedia.org/wiki/Blockchain, consultato il 9 agosto 2018).

[14] Con vari tipo di algoritmo può essere ricavato da ogni serie di dati, della più varia dimensione, un estratto (*digest*) informatico di lunghezza predefinita e con la proprietà di essere unico per la massa di dati di partenza e senza possibilità che una massa di dati anche di poco diversa dalla prima possa dare un *hash digest* identico (c.d. resistenza alle collisioni). Così è descritta tale tecnologia informatica in una delle opere più recenti e complete, pur di carattere divulgativo ma con adeguata precisione scientifica (I. Bashir, *Mastering Blockchain*, Birmingham-Mumbai, 2017, p. 87): «Cryptographic hashes. Hash functions are basically used to compress a message to a fixed length digest. In this mode, block ciphers are used as a compression function to produce a hash of plain text» (p. 60); «Hash functions. Hash functions are used to create fixed length digests of arbitrarily long input strings. Hash functions are keyless and provide the data integrity service. They are usually built using iterated and dedicated hash function construction techniques. Various families of hash functions are available, such as MD, SHA1, SHA-2, SHA-3, RIPEMD, and Whirlpool. Hash functions are commonly used in digital signatures and message authentication codes, such as HMACs. They have three security properties, namely pre-image resistance, second preimage resistance, and collision resistance».

[15] Per una sensibilità in questo senso, cfr. *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))* che al punto 47 «osserva che lo sviluppo della robotica e dell'intelligenza artificiale dovrebbe essere condotto *in modo tale da limitare l'impatto ambientale mediante un consumo energetico efficiente*, l'efficienza energetica mediante la promozione dell'uso delle energie rinnovabili e dei materiali di difficile reperibilità, nonché la riduzione al minimo dei rifiuti – ad esempio quelli elettrici ed elettronici – come pure la riparabilità».

[16] Nell'accezione informatica, il termine «consenso» indica il risultato di procedimenti di concordanza, relativi al calcolo distribuito in sistemi multi-agente, volti ad ottenere una affidabilità generale pur in presenza di processi potenzialmente difettosi o scorretti. Il problema informatico è noto, in informatica, come «Problema dei generali bizantini», dal titolo del saggio scritto nel 1982 dall'informatico statunitense Leslie Lamport insieme a Robert Shostak e Marshall Pease (L. Lamport, R. Shostak, M. Pease, *The Byzantine Generals Problem*, in *ACM Transactions on Programming Languages and Systems*, 1982, 4(3), pp. 382-401), problema così sunteggiato nell'*abstract* del saggio: «Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstract-

c.d. metodo della *Proof of Work*[17], con conseguente incrementale richiesta di investimento di capacità di calcolo e dunque di correlativa crescita di fabbisogno energetico.

Nei sistemi *tradizionali* (analogici) di tenuta dei dati giuridicamente rilevanti – ad esempio la pubblicità immobiliare – che i cultori informatici qualificherebbero come *Permissioned Ledger* (PL), 1) la garanzia di *provenienza* e *autenticità* del dato registrato è frutto dei meccanismi tradizionali di imputabilità del documento (tra cui centrale è la sottoscrizione) e 2) la *immodificabilità* dei dati è garantita dalla autorità del custode del registro e di coloro che possono avervi accesso per modificarlo: continuando nell'esempio, il Ministero delle Finanze o l'Agenzia del Territorio, che tengono i Registri Immobi-

ly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed».

[17] Secondo Bashir, I., *Mastering Blockchain*, cit., pp. 28-29: «Consensus is basically a distributed computing concept that has been used in blockchain in order to provide a means of agreeing to a single version of truth by all peers on the blockchain network. Roughly, the following two categories of consensus mechanism exist: 1. Proof-based, leader-based, or the Nakamoto consensus whereby a leader is elected and proposes a final value; 2. Byzantine fault tolerance-based, which is a more traditional approach based on rounds of votes. Proof of Work. This type of consensus mechanism relies on proof that enough computational resources have been spent before proposing a value for acceptance by the network. This is used in bitcoin and other cryptocurrencies. Currently, this is the only algorithm that has proven astonishingly successful against Sybil attacks. Proof of Stake. This algorithm works on the idea that a node or user has enough stake in the system; for example the user has invested enough in the system so that any malicious attempt would outweigh the benefits of performing an attack on the system. This idea was first introduced by Peercoin and is going to be used in the Ethereum blockchain. Another important concept in Proof of Stake (PoS) is coin age, which is a derived from the amount of time and the number of coins that have not been spent. In this model, the chances of proposing and signing the next block increase with the coin age». Il sistema della *proof of work* è intrinsecamente e altamente energivoro: «Per avere un'idea, il mining dei Bitcoin attualmente (maggio 2018) consuma circa 64 TeraWattora su base annuale, più o meno quanto la Svizzera. Il consumo energetico per valutare una singola transazione è di circa 850 KiloWattora, superiore al consumo medio annuale di una famiglia italiana. Le emissioni di CO2 dovute ad una singola transazione corrispondono circa a quelle di un veicolo medio che percorre 1600 km di strada. Il metodo sopra descritto per remunerare i *miners* è detto eufemisticamente *proof of work*, ma sarebbe forse più corretto chiamarlo *proof of waste*» (così Alberto Berretti, professore nel Dipartimento di Ingegneria Civile e Ingegneria informatica dell'Università di Roma Tor Vergata, in un assai chiaro articolo divulgativo: A. Berretti, *Blockchain e mining, ecco come funziona: dietro le quinte della tecnologia*: https://www.agendadigitale.eu/cittadinanza-digitale/pagamenti-digitali/.

liari e i notai o gli altri pubblici ufficiali che possono trascrivervi ed iscrivervi dati. Qui l'impatto energetico ed ambientale è pressoché irrilevante.

Nei corrispondenti sistemi *informatici*, i c.d. *Permissioned Ledger*, 1) la garanzia di *provenienza* e *autenticità* del dato registrato è basata sull'apposizione di firma digitale o elettronica qualificata (o comunque sulla identificazione elettronica dell'autore del dato) e 2) la *immodificabilità* dei dati è garantita dalla posizione di autorità del custode del registro e di coloro che possono avervi accesso per modificarlo. L'esempio dei Registri Immobiliari può anche qui essere riproposto perché, come noto, da tempo essi sono tenuti informaticamente e le registrazioni dei dati avvengono con accessi telematici da parte dei notai che rogano atti muniti di firma digitale; l'esemplificazione può poi arricchirsi con il sistema del processo civile telematico, ove il *Ledger* (composto dai vari fascicoli informatici) è tenuto dal Ministero della Giustizia e l'inserimento dei dati, costituiti da documenti informatici con firma digitale, avviene ad opera di soggetti selezionati (avvocati, giudici, cancellieri, ufficiali giudiziari). Anche in tali casi, di tenuta in via informatica di *Permissioned Ledgers*, l'impatto energetico e ambientale risulta contenuto.

Qualora invece – per scelta ideologica – si preferisca un sistema non gerarchizzato e in larga misura anarchico (quale la *blockchain*), non volendosi riconoscere alcuna autorità deputata alla tenuta e all'accesso del registro – i problemi di immodificabilità e concordanza dei dati, secondo ciò che in informatica viene indicato come «ricerca del consenso»[18] vengono risolti, ad oggi, sostanzialmente con la già menzionata *proof of work* oppure con la c.d. *proof of stake*, cui si aggiunge l'ulteriore metodo, meno collaudato ma più promettente in termini di risparmio energetico, della c.d. *proof of authority*[19] (ove i blocchi di

[18] Ove per «consenso» si intende il risultato di «procedimenti di concordanza», per ottenere una affidabilità generale del sistema di calcolo distribuito in sistemi multi-agente anche in presenza di processi di calcolo potenzialmente difettosi o scorretti.

[19] Dal sito https://academy.binance.com/en/articles/proof-of-authority-explained: «Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially the private ones). The term was proposed in 2017 by Ethereum co-founder and former CTO Gavin Wood. The PoA consensus algorithm leverages the value of identities, which means that block validators are not staking coins but their own reputation instead. Therefore, PoA blockchains are secured by the validating nodes that are arbitrarily selected as trustworthy entities. The Proof of Authority model relies on a limited number of block validators and this is what makes it a highly scalable system. Blocks and transactions are verified by pre-approved participants, who act as moderators of the system.PoA consensus algorithm may be applied in a variety of scenarios and is deemed a high-value option for logistical applications. When it comes to supply chains, for example, PoA is considered an effective and reasonable solution». Per un'analisi di tipo scientifico computazionale, O. Hasan, L. Brunie, E. Bertino, *Privacy Preserving Reputation Systems based on Blockchain and other Cryptographic Building Blocks: A Survey*, 2022: https://dl.acm.org/doi/10.1145/3490236.

dati vengono «chiusi», cioè resi immutabili, da un gruppo di soggetti selezionati come *validators*, la cui reputazione nella rete li rende affidabili)[20].

Nell'architettura *Bitcoin blockchain*, basata sulla *proof of work*, lo sviluppo della serie di blocchi è affidato ai c.d. *miners*[21] che sono incentivati alla «chiusura» di ciascun blocco dalla connesse ricompensa in Bitcoin.

Il sistema della *proof of work* non è tuttavia sicuro in modo assoluto e può fallire, se si creano concentrazioni di capacità computazionali superiori al 51%:[22]; inoltre, esso è instenibilmente energivoro, come si è detto, perchè la prova del possesso delle superiori capacità di calcolo, che i *miners* devono offrire, è quella di avere risolto enigmi computazionali che, in buona sostan-

[20] Cfr. I. Bashir, *Mastering Blockchain*, cit., pp. 132-133: «The proof of Work [...] relies on proof that enough computational resources have been spent before proposing a value for acceptance by the network. This is used in bitcoin and other cryptocurrencies», quanto alla «Proof of Stake. This algorithm works on the idea that a node or user has enough stake in the system; for example the user has invested enough in the system so that any malicious attempt would outweigh the benefits of performing an attack on the system. This idea was first introduced by Peercoin and is going to be used in the Ethereum blockchain».

[21] «Once a new node joins the bitcoin network, it downloads the blockchain by requesting historical blocks from other nodes. This is mentioned here in the context of the bitcoin miner; however, this not necessarily a task only for a miner. Transaction validation: Transactions broadcasted on the network are validated by full nodes by verifying and validating signatures and outputs. Block validation: Miners and full nodes can start validating blocks received by them by evaluating them against certain rules. This includes the verification of each transaction in the block along with verification of the nonce value. Create a new block: Miners propose a new block by combining transactions broadcasted on the network after validating them. Perform Proof of Work: This task is the core of the mining process and this is where miners find a valid block by solving a computational puzzle. The block header contains a 32-bit nonce field and miners are required to repeatedly vary the nonce until the resultant hash is less than a predetermined target. Fetch reward: Once a node solves the hash puzzle, it immediately broadcasts the results, and other nodes verify it and accept the block. There is a slight chance that the newly minted block will not be accepted by other miners due to a clash with another block found at roughly the same time, but once accepted, the miner is rewarded with 12.5 bitcoins (as of 2016) and any associated transaction fees... This is a proof that *enough computational resources have been spent in order to build a valid block*. Proof of Work (PoW) is based on the idea that a random node is selected every time to create a new block» (I. Bashir, *op. cit.*, pp. 132-133).

[22] «Mining centralization is a major concern that can occur if a pool manages to control more than 51% of the network by generating more than 51% hash rate of the bitcoin network. As discussed earlier in the introduction section, 51% attack can result in double spending attacks, and it can impact consensus and in fact impose another version of transaction history on the bitcoin network. This has happened once in the bitcoin history, when GHash.IO, a large mining pool, managed to acquire more than 51% of the network capacity. Theoretical solutions, such as two-phase Proof of Work, have been proposed in academia to disincentivize large mining pools. This scheme introduces a second cryptographic puzzle that results in mining pools to reveal their private keys or providing a considerable portion of the hashrate of their mining pool, thus reducing the overall hashrate of the pool» (Bashir, *op. cit.*, pp. 137-138).

za e a fini descrittivi, possono accostarsi al decifrare funzioni *hash* mediante la c.d. «forza bruta» informatica[23] e cioè provando innumerevoli volte combinazioni causali con computer di potenza adeguata.

5. Anarchia *versus* gerarchia dei sistemi informatici (ieri, la crittografia a doppia chiave; oggi la *blockchain* e i NFT)

Riguardando la vicenda della *blockchain,* partita dai Bitcoin, pare potersi dire che si sta ripetendo quanto avvenuto per la cifratura a doppia chiave asimmetrica, su cui si è costruito, a cavallo del 2000, il sistema di firma digitale.

Negli anni Settanta del secolo scorso alcuni informatici statunitensi, con un chiaro disegno ideologico, realizzarono un sistema di cifratura (il software c.d. *Pretty Good Privacy*: PGP) per dialogare su Internet in modo segreto nel timore, forse infondato, di una possibile lesione della privacy da parte delle autorità governative.

Nella sua originaria versione, essenzialmente anarchica, tale sistema di cifratura non riconosceva alcuna autorità che garantisse la generazione, custodia e attribuzione soggettiva all'utente delle singole chiavi di cifratura.

Ma quando tale procedura informatica rivestì interesse per il commercio giuridico, non si ebbe difficoltà a prevedere una figura di autorità, quella del certificatore - inizialmente soggetta ad *autorizzazione* statuale (cfr. DPR 513/1997) e poi, con l'apertura del mercato europeo delle firme elettroniche (direttiva 1999/93/CE sulle firme elettroniche), quantomeno in possesso di particolari requisiti professionali – che garantisse l'attribuzione delle chiavi di firma e la identificabilità elettronica del soggetto.

In altre parole, e per quanto qui ci interessa, la originaria ideologia anarchica, sottostante alla tecnologia, fu abbandonata per adottare una fisionomia gerarchizzata e basata su di una autorità di controllo di tale architettura.

[23] Come si può leggere nel documento divulgativo del Dipartimento di Matematica dell'Università di Ferrara, dal titolo *Problemi risolti ed irrisolti in teoria dei numeri*, accessibile all'indirizzo http://dm.unife.it/philippe.ellia/Docs/PbiTeoNum.pdf, «la crittografia moderna ("a chiave pubblica") si basa su un'idea molto semplice: *è molto difficile, praticamente impossibile fattorizzare in numeri primi, in un tempo ragionevole, un numero molto molto grande; anche usando computers molto potenti!* Per convincervi di questo fatto visitate il sito www.mersenne.org dedicato alla ricerca dei primi di Mersenne. Viceversa, dato un numero molto grande se si conosce un suo fattore primo ("la chiave"), allora la fattorizzazione diventa possibile. In sostanza il messaggio (= il numero molto grande o meglio la sua fattorizzazione) può essere reso pubblico, tutti sanno cosa bisogna fare, ma solo chi ha la chiave può leggere il messaggio. Questa è l'idea di base, in realtà si complica un pochino la situazione usando, per esempio, la generalizzazione di Eulero del piccolo teorema di Fermat…».

Mi pare, allora, che la medesima attitudine anarchica sia stata alla base della originaria concezione delle criptovalute (e del Bitcoin come loro archetipo). Ed è qui maggiormente comprensibile l'insofferenza per ogni autorità di certificazione e di controllo nel sistema blockchain, se si riflette sul risultato ricercato, quello della disintermediazione nella emissione e circolazione di moneta.

Da sempre, il «battere moneta» è stato ed è espressione della sovranità e lo stesso valore della moneta si regge sulla autorità dell'emittente, di regola uno Stato. Non sono mancati, tuttavia, anche casi in cui la semplice autorevolezza ha supportato emissione di moneta: la mia generazione può ricordare che, negli anni Settanta del '900, la carenza di moneta metallica aveva portato all'emissione dei cosiddetti mini-assegni, surrogati del contante emessi da soggetti la cui autorevolezza era data dall'appartenenza al ceto bancario, con la connessa vigilata solvibilità.

A tale approccio ideologico della *blockchain*, si combina poi la possibilità di sfruttare l'anonimia e virtuale in-tracciabilità delle criptovalute, che le rendono idonee ad un utilizzo in attività illecite.

Ma, allora, mi pare sul tema della *blockchain* – come su quello della crittografia – ci si debbano porre le giuste domande, scevre da incrostazioni ideologiche.

La prima: le funzioni cui può assolvere la *blockchain* (e i connessi NFT) sono, o possono essere, assolte da *altre* architetture tecnologiche, senza gli inaccettabili effetti collaterali che la *proof of work causa*, in termini di consumo energetico e di pregiudizio climatico e ambientale?

Al quesito il giurista, che abbia dialogato con l'informatico, sa dare da tempo risposta positiva, anche sulla base della storia.

Il problema di impedire una doppia alienazione di un singolo bene e già stato da tempo risolto con i registri proprietari (catasto, registri immobiliari) nei quali volta volta sono stati allibrati i beni ritenuti più rilevanti economicamente, e per i quali fosse possibile un controllo della circolazione (e l'impiego di strumenti informatici ha reso via via praticabile il controllo della circolazione di sempre maggiori categorie di beni, che per il passato sfuggivano praticamente ad un accurato sistema di pubblicità: si pensi ai beni mobili, per i quali per lungo tempo solo il *possesso* ha costituito la più rudimentale ed effettiva forma di pubblicità).

Lo stesso sistema di controllo degli acquisti a titolo derivativo, secondo una corretta catena di legittimazione, è replicato e replicabile, appunto, con l'impiego, da un lato, dei meccanismi di firma elettronica e digitale, sia per la provenienza dei documenti, sia per la stessa identificazione dei beni immateriali, perché l'applicazione di una firma digitale può contrassegnare in modo immodificabile un documento informatico di qualunque genere, da una fotografia, a un'opera musicale, a un video; dall'altro, la funzione della *blockchain* è replicata e replicabile con la selezione di soggetti, dotati di

autorità in base a sistemi normativi, per la custodia e la gestione di registri qualificabili come *Permissioned* o *Semipermissioned Ledgers*.

Emerge allora evidente che l'unico elemento differenziatore della blockchain rispetto a tali *Permissioned* o *Semipermissioned Ledgers* non è funzionale, ma strutturale e consegue al rifiuto di riconoscimento di qualunque autorità di gestione del registro.

La ulteriore domanda da porsi è dunque: ha senso (e siamo disponibili a) sacrificare le compromissioni ambientali ed energetiche di cui si è detto sopra, per continuare a mantenere un sistema che offre come vantaggio, rispetto a quelli meno energivori, *esclusivamente l'anonimato o il ripudio di qualunque tipo di autorità*?

Anche per le criptovalute, come per i meccanismi di firma digitale, potrebbe essere ragionevole preconizzare un abbandono del carattere anarchico e anonimo che ideologicamente ne aveva caratterizzato l'origine, per giungere a un più tradizionale e non energivoro approdo che identifichi, sulla base di sistemi normativi (o forse anche volontaristici), quali siano le autorità di gestione del registro medesimo.

In altre parole, qual è il vantaggio, per la collettività, nel ripudiare ogni affidamento su di una autorità di registro, per privilegiare esclusivamente una architettura di registro distribuito?

Anche lo stesso dibattito sui benefici e vantaggi recati dai Non Fungibile Tokens al commercio giuridico è inquinato dalla medesima mancanza di consapevolezza che, *anche senza la blockchain*, le opere d'arte o le opere dell'ingegno, esistenti nella forma dei documenti o oggetti informatici, possono essere rese uniche non già esclusivamente tramite i NFT (che implicano la *blockchain*), ma anche tramite la ormai collaudata tecnologia della firma digitale, la cui affidabilità non è basata su alcuna prova di potere computazionale, ma sulla autorità del certificatore e sull'aggiornamento tecnologico delle chiavi di cifratura.

6. I problemi posti dagli *smart contracts*

Il secondo tema, quello degli *smart contracts* convolge profili di teoria generale del contratto.

6.1. Il c.d. «decreto semplificazioni» del 2019 e il requisito di forma scritta

Innanzitutto, il tema delle definizioni, che trova un riferimento in una norma dotata di scarsa portata applicativa, ma verosimilmente concepita a fini me-

ramente cosmetici e *lato sensu* politici, quale velleitario tentativo di veicolare una visione e capacità di ammodernamento del Paese, esistenti solo nelle intenzioni e sulla carta.

Il c.d. «decreto semplificazioni» del 2019[24], all'art. 8 *ter*, intitolato *Tecnologie basate su registri distribuiti e smart contract*, reca infatti, al primo comma, una definizione di DLT più analitica e descrittiva di quella di cui all'art. 3 co.1, n. 1) del MICA, ma non in contrasto con essa. 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».

I commi successivi di tale art. 8 *ter* definiscono poi gli *smart contracts*, e ne disciplinano alcuni limitati effetti, come segue: «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».

La normativa – cui non aveva fatto seguito la emanazione delle necessarie norme tecniche nel termine indicato dal 4 comma – appare inopportuna e di cattiva formulazione, è frutto di incompetenza e di una contingente improvvisazione.

In primo luogo, essa non si attiene al saggio principio della neutralità tecnologica nella normazione del c.d. diritto privato dell'informatica e dun-

[24] D.l. 14 dicembre 2018, n. 135 (in Gazzetta Ufficiale – Serie generale – n. 290 del 14 dicembre 2018), coordinato con la legge di conversione 11 febbraio 2019, n. 12 (in questa stessa Gazzetta Ufficiale alla p. 6), recante: «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione».

que fotografa una situazione tecnologica puntuale, destinata ad evoluzione nel tempo con conseguente prevedibile e celere obsolescenza della disciplina giuridica stessa.

Inoltre, essa demanda la sua completezza ad una integrazione normativa di secondo livello, oltretutto priva di copertura normativa primaria, pur incidendo su aspetti centrali della circolazione giuridica, quali quelli della forma del contratto: dimentica che l'art. 1350, n. 13, cod. civ., indica nella *legge* la fonte primaria della disciplina dei requisiti formali dei negozi e di quello, più solenne, della «forma scritta».

Ancora, la disciplina recata dall'estemporaneo provvedimento appare modesta sul piano applicativo, perché l'unica parte non descrittiva, ma dispositiva, della norma, cioè l'attribuzione degli effetti giuridici della validazione temporale elettronica al *documento informatico memorizzato su blockchain*, era ed è già ottenibile con l'utilizzo di una semplice marca temporale digitale, priva di significativo *carbon footprint* e di immediata applicazione: dunque *nihil novi sub sole*!

Infine, la disciplina di cui al co. 2, secondo cui «gli smart contract soddisfano il requisito della forma scritta» sconta una evidente incompetenza tecnica, ed introduce una aporia ed una schizofrenia nel sistema del diritto privato dell'informatica.

Infatti, come è noto, la disciplina sulle firme digitali e sulla documentazione informatica (ora raccolta nel Codice dell'amministrazione digitale, il c.d. CAD: D.lgs. 82/2005), nonché quella di settore sul processo civile telematico, escludono la possibilità di ottenere gli effetti giuridici conseguenti alla apposizione di firma digitale ai documenti che contengano c.d. «campi dinamici» e cioè macroistruzioni che consentano al documento di variare alcune parti o dati in esso incorporati al variare di funzioni esterne (es. la data) o rispetto ad *imput* esterni.

Ciò è intuitivamente comprensibile, perché uno dei principali effetti dell'apposizione della firma digitale è la garanzia di immodificabilità del documento, che evidentemente è vanificata dalla presenza, in esso, di istruzioni che ne consentono una adattabilità e modificabilità dopo la sua confezione.

Per converso è ontologicamente connaturata allo *smart contract* la possibilità, ed anzi la necessità, che esso adegui il contenuto e dia luogo ad istruzioni variabili durante il rapporto contrattuale, specie in relazione ad input esterni, tra cui i cosiddetti *Oracles*, che inseriscono nel contratto (o, meglio, nella relazione contrattuale che ne nasce) parametri e risultati di accadimenti esterni e successivi alla conclusione del medesimo.

Poiché il requisito della forma scritta è richiesto dal codice civile, e dalle norme di settore del diritto privato dell'informatica, allorché del documento debba essere garantita la immodificabilità, l'attribuzione agli *smart contracts*

del valore della forma scritta, di cui alla norma in questione, risulta dunque in palese contraddizione con il sistema.

6.2. *Smart contracts* e predisposizione unilaterale del contenuto del contratto

Ciò detto su tale episodico intervento di diritto positivo, e volgendoci agli obiettivi funzionali indicati dai giuristi che guardano a codesta tecnologia informatica, si può notare come taluno proponga lo *smart contract* come i) antidoto all'imprevedibilità del Giudice e come ii) garanzia di ineluttabile adempimento, al verificarsi di certi presupposti in fatto[25].

Si tratta di un appello – pur mosso dall'attuale novellata esigenza, espressa dall'economia, di certezza del diritto, non solo *positum* ma, soprattutto, *applicato* – all'estensione della *autotutela* in un campo, quello del diritto privato e dei contratti, nel quale, con saggezza, il codificatore la aveva relegata a casi eccezionali.

È per vero in atto un *trend* di risposta, ad una amministrazione della Giustizia percepita come incerta e certo spesso tardiva, che dai più sedimentati casi del «diritto di ritenzione» (quello del meccanico sulla motocicletta riparata: una delle prime nozioni di diritto che il sedicenne motociclista imparava!) – è giunto a prevedere la liceità della autotutela nelle opere intellettuali (con i c.d. strumenti di *Digital Right Mangement*: DRM, ammessi ed assistiti anche da sanzione penale contro i tentativi di loro manomissione dalla novellazione del 2003 alla legge sul diritto di autore)[26].

[25] In questo senso, si è detto: «Il vantaggio connesso all'utilizzazione di smart contract è rappresentato innanzitutto… dall'innumerevole quantità di variabili che un programma informatico può includere, il che determina sostanzialmente la possibilità di neutralizzare il rischio delle sopravvenienze. Un'altra prerogativa dell'esecuzione automatizzata consiste nell'inevitabilità dell'effetto al verificarsi di una condizione che è propria del meccanismo informatico if – then. Questa caratteristica potrebbe determinare una riduzione del contenzioso, quanto meno in una prima fase: il contraente sa che al verificarsi di un determinato evento si produce l'effetto: se la rata non è stata pagata il veicolo non va in moto; se il vettore è in ritardo il prezzo si riduce, ecc.» (D. Di Sabato, *Gli* smart contracts*: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2017, p. 398). Maugeri rileva condivisibilmente la circostanza che «l'oracolo (umano e non) potrebbe errare nel valutare il corretto adempimento, e che le parti, almeno in Italia, sono vincolate non solo a quello che è previsto nell'accordo ma anche a tutto quello che dallo stesso deriva secondo la legge o, in mancanza, secondo gli usi e l'equità (art. 1374 cod. civ.). Ciò significa che la corretta esecuzione del Code potrebbe non tradursi nella corretta esecuzione del contratto» (M. Maugeri, Smart contracts *e disciplina dei contratti*, in *ODCC*, 2020, p. 396).

[26] Sulla l. 633/1941 legge diritto aut. ha inciso il D.lg. 9 aprile 2003, n. 68, di attuazione della Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001,

Tuttavia, l'impiego degli *smart contracts* in modo massivo acuirebbe un problema, già oggi evidente e al quale il codificatore del 1942 non aveva dedicato norme espresse: quello della *determinazione unilaterale* del contenuto (e dell'oggetto) dei contratti *standard* ad opera del predisponente ed in danno dell'aderente, tema sul quale codificatori più recenti del nostro hanno preso posizione e sul quale anche una parte del *Common Law* nordamericano riflette oggi[27].

Infatti, un diffuso impiego degli *smart contracts* estremizzerebbe la predisposizione unilaterale del contenuto del contratto, incidendo non solo nella configurazione dei diritti ed obblighi delle parti, ma altresì nell'*enforcement* dei medesimi, sottraendo quest'ultimo al monopolio statale, cui l'impianto giuridico del nostro sistema di diritto privato e diritto processuale lo sottopone: ciò che quantomeno renderebbe più attuale l'esigenza di una parte ge-

sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione. Essa, ed il suo decreto attuativo, si occupano delle c.d. misure tecnologiche di protezione, destinate ad avere una rilevante incidenza sui beni oggetto dei contratti del commercio elettronico (tra i quali, in particolare, i brani musicali, ovvero i video, tutelati dal diritto di autore). La direttiva prende atto del duplice versante sul quale si articola la «autotutela» posta in essere dai titolari di diritti economici di sfruttamento di tali opere per evitarne la sistematica violazione nell'ambito dell'impiego di strumenti informatici e telematici: da un lato, l'apposizione sulle opere o sui materiali protetti dal diritto di autore di misure tecnologiche di protezione (DRM) e, dall'altro, l'inserimento su tali opere e materiali di informazioni elettroniche sul regime dei diritti ad essi connessi che diano immediata contezza all'utente o a chi ne è in possesso o ne viene in contatto della sfera delle condotte lecite ed illecite. Il legislatore europeo, con la direttiva, si è mosso dunque nel senso del riconoscimento della liceità di tali pratiche di «autotutela» e nel senso della richiesta a ciascuno Stato membro di approntare una ulteriore tutela, a monte, indirizzata contro la manomissione delle informazioni sul regime dei diritti delle opere intellettuali che possono essere associate o apposte ai dati in forma digitale di cui constano tali opere, con un capo autonomo, il terzo, intitolato *Tutela delle misure tecnologiche e delle informazioni sul regime dei diritti*, composto di due articoli, 6 e 7. Il d.lg. 68/2003 di attuazione interna ha poi provveduto ad inserire nella originaria l. 633/1941 un nuovo Titolo, il II-*ter*, composto da due articoli, il 102-*quater* e il 102 *quinquies*. Il primo prevede la liceità della «autotutela» costituita dalla apposizione di misure tecnologiche di protezione; il secondo richiama le «informazioni elettroniche» sul regime dei diritti, oggetto dell'art. 7 della direttiva, di cui riprende anche l'impreciso uso dell'attributo «elettronico» quale sinonimo di digitale. Coerentemente con l'impostazione della l. 633/1941 l'apparato sanzionatorio che presidia i due nuovi riportati articoli è stato poi inserito nella parte finale della legge, alla Sezione II dedicata alle «Difese e sanzioni penali», ove sono state aggiunte le nuove lettere *f-bis*) e *h*) nell'art. 171-*ter*, che contiene ipotesi delittuali ed è stato introdotto un nuovo art. 174-*ter*, contenente sanzioni amministrative.

[27] Mi riferisco alla codificazione argentina del 2015 e alla *doctrine of unconscionability* sviluppata dalla Supreme Court of Canada. Su questi temi, mi permetto di rinviare ai miei due saggi: F. Delfini, *Unnegotiated Contracts of Adhesion in American Common and Civil Law Jurisdictions: The Canadian and Argentinian Cases*, in *Milan Law Review*, 2021, 1; Id., *Norme dispositive e determinazione del contenuto del contratto*, in *Riv. Trim. Dir. Proc. Civ.*, 2020, 2, pp. 547-574.

nerale del diritto dei contratti, relativa al controllo della predisposizione del contenuto dei contratti *standard,* a prescindere dallo *status* di professionista o consumatore dell'aderente.

6.3. *Smart contracts* e contratti dei consumatori

La struttura nella tecnologia *blockchain,* su cui si appoggiano gli *smart contracts* presenta criticità nel caso dei contratti dei consumatori, per i quali, come noto, la disciplina di derivazione europea prevede, quale centrale tutela, il recesso di pentimento a favore del consumatore aderente.

In primo luogo, pare condivisibile ritenere che gli *Smart Contracts* non possano giovarsi della esclusione di applicazione della disciplina del consumatore prevista all'articolo 47, lett. n) del Cod. Cons. (D.lg. 206/2005) – che esenta dall'applicazione delle sezioni 1- 4 del capo I Titolo III (tra cui quelle sulle informazioni precontrattuali ed il recesso) – per i contratti «conclusi tramite distributori automatici o locali commerciali automatizzati»[28]: e ciò non solo perché gli *smart contracts* sono necessariamente contratti a distanza, ma altresì per la circostanza che l'esclusione sopra menzionata è giustificata dalla circostanza che, nel caso dei distributori automatici, si è di fronte a un contratto di fatto e quindi non vi è alcun problema di percezione di un regolamento contrattuale espresso da un linguaggio (naturale o matematico); inoltre si tratta di contratti aventi ad oggetto beni tangibili e dunque alla comprensione della portata dell'operazione economica, peraltro di regola di modesta entità, soccorre la percezione naturalistica tramite alcuni dei cinque sensi (vista, tatto, talvolta l'udito, se reso possibile dal distributore automatico).

Né agli *smart contracts* può applicarsi la specifica eccezione al diritto di recesso di cui all'art. 59 comma 1 lett. a) cod. cons., riferita ai «contratti di servizi, dopo la completa prestazione del servizio, se l'esecuzione è iniziata con l'accordo espresso del consumatore e con l'accettazione della perdita del diritto di recesso a seguito della piena esecuzione del contratto da parte del professionista»: ciò, da un lato, qualora lo *smart contract* non abbia ad oggetto servizi e comunque, dall'altro, anche qualora si tratti di servizi, perché è discutibile che tramite l'architettura della *blockchain* si possa avere un accordo *espresso* del consumatore avente ad oggetto la perdita di tale diritto[29].

[28] In questo senso, Maugeri, Smart contracts *e disciplina dei contratti*, cit., p. 400 e Id., *Mercato finanziario, criptoattività, proposta di Regolamento MICA* (Markets in Crypto – Assets) *e tutela del consumatore*, in *Contratto e impresa*, 2022, p. 5.

[29] Concorde anche, con diverse sfumature, Maugeri, Smart contracts *e disciplina dei contratti*, cit., p. 403.

Ulteriori problemi pone, poi, la compatibilità con gli *Smart Contracts* della previsione, di cui all'articolo 51 comma 2 cod. cons.[30], che prevede una forma assai dettagliata – anche nella grafica dell'interfaccia con l'aderente e nelle parole da usarsi da parte del predisponente – per rendere consapevole il consumatore del trapasso dalla fase informativa sulla transazione economica alla conclusione del contratto con obbligo di pagamento[31].

Infine, ulteriori problemi di compatibilità sorgono con l'articolo 51, co. 7 cod. cons., laddove prevede un obbligo di *conferma* del contratto da parte del professionista al consumatore su un mezzo *durevole*: il che è ovviamente pensato per una tecnologia di contrattazione a distanza diversa dalla *blockchain*.

6.4. *Smart contracts* e conoscibilità del contenuto del contratto

Lo *smart contract* è tipicamente contratto *standard*.

L'art. 1341 co.1., come è noto, contiene una norma, di favore per il predisponente, che rende le condizioni generali di contratto predisposte «efficaci nei confronti dell'altro, se al momento della conclusione del contratto … *avrebbe dovuto conoscerle* usando l'ordinaria diligenza». L'art. 1374 cod. civ. ricomprende poi nel contenuto obbligatorio del contratto, anzitutto, «quanto è nel medesimo espresso».

[30] L'art. 51, co. 2 del codice del consumo, introdotto dal D.lgs. 21/2014 in attuazione dell'art. 8, co. 2, della direttiva 2011/83/UE, ha riconosciuto espressamente la validità del contratto concluso con il *point and click*, prevedendo tuttavia che il professionista debba garantire la consapevolezza, in capo al consumatore ed al momento di inoltrare l'ordine, che l'ordine stesso implica l'obbligo di pagare ed imponendo che «se l'inoltro dell'ordine implica di azionare *un pulsante o una funzione analoga*, il pulsante o la funzione analoga riportano in modo facilmente leggibile soltanto le parole "ordine con obbligo di pagare" o una formulazione corrispondente inequivocabile indicante che l'inoltro dell'ordine implica l'obbligo di pagare il professionista». Se tali prescrizioni non sono rispettate, e dunque se il consumatore non è messo nella condizione di comprendere che da una fase *informativa* sul bene o servizio offerti sta passando alla *conclusione* del contratto, la norma prevede che il consumatore non sia vincolato dal contratto o dall'ordine. Tale più recente tutela del consumatore completa quella già prevista dall'art. 12 D. Lgs. 70/2003 sul commercio elettronico, che impone al predisponente il sito *internet* di fornire informazioni sui «mezzi tecnici messi a disposizione del destinatario per individuare e correggere gli errori di inserimento dei dati prima di inoltrare l'ordine al prestatore», così implicitamente imponendo al professionista di predisporre idonei strumenti di revisione dell'ordine prima dell'invio e di correzione di eventuali errori nella manifestazione della volontà.

[31] Ne è consapevole Maugeri (Maugeri, Smart contracts *e disciplina dei contratti*, cit., p. 403, nota 84; Id., *Mercato finanziario, criptoattività, proposta di Regolamento MICA* (Markets in Crypto – Assets) *e tutela del consumatore*, cit., p. 8.

Va allora considerato che la redazione di un contratto in codice binario, o comunque come un «listato» di istruzioni in linguaggio macchina farebbe emergere, nel breve periodo, un *gap tecnologico* tra il contraente normale e quello tecnologicamente esperto[32] che farebbe impallidire chi, negli anni Sessanta negli Stati Uniti e in Australia, si lamentava dell'incomprensibile linguaggio giuridico da iniziati usato nei contratti, ed invocava, per porvi rimedio, la sostituzione del *Legal English* in *Plain Language*.

Anche ammesso che, in base alle norme del codice sopra ricordate, per la contrattazione *standard* la mera *conoscibilità* del contenuto predisposto lo renda vincolante ed opponibile all'aderente, sorge allora il forte dubbio che per lo *smart contract* si possa predicare una effettiva *conoscibilità,* con l'ordinaria diligenza, del contenuto del contratto da parte dell'aderente (non necessariamente «consumatore»).

Inoltre, in larga parte le istruzioni di (auto)esecuzione), connaturate allo *smart contract,* ricadono nelle materie menzionate nel secondo comma dell'art. 1341 cod. civ. (si pensi alla sospensione della esecuzione da parte del predisponente o alla limitazione alla possibilità di opporre eccezioni da parte dell'aderente), con i conseguenti problemi in punto di *specifica approvazione per iscritto,* richiesta dalla norma.

Infine, e astraendo dal dato domestico, si può rilevare che lo *smart contract,* per dare il meglio di sé, in termini di governo delle sopravvenienze, deve prevedere tutto e comprendere istruzioni per ogni evenienza fattuale: saremmo così al trionfo del contratto *non etero integrabile,* cioè connotato da un'analiticità estrema, tipica della redazione dei contratti anglosassoni (perché privi di un referente codicistico per colmare le eventuali lacune), che ha portato ad inconvenienti che, con autoironia, gli stessi *common lawyers* indicano come *redundancy and repetition*[33].

6.5. *Smart contracts* ed esercizio della giurisdizione

Ulteriori problemi si pongono sul versante della giurisdizione.

Anche scontato l'auspicio di un più ridotto coinvolgimento del Giudice nell'*enforcement,* nei casi in cui questi sia chiamato comunque a conoscere del contratto ci troveremmo di fronte, con gli attuali strumenti culturali del processo, alla pratica impossibilità di decisione su di uno *smart contract* in senso stretto, perché si tratta di oggetto informatico in linguaggio binario nativo, in-

[32] Lo rileva, analiticamente e condivisibilmente, P. Cuccuru, *Blockchain ed automazione contrattuale. Riflessioni sugli Smart contract*, in *Nuove leggi civ. comm.*, 2017, 2, p. 113.

[33] Sul tema, C. Felsenfeld, *The Plain English in the United States*, in *Can. Bus. L. J.*, 1981-1982, 6, p. 408.

comprensibile all'operatore medio del diritto: ciò che potrebbe portare, di fatto, ad una rinuncia alla giurisdizione, in contrasto con l'art. 24 Cost.

E anche il prevedibile massivo ricorso a CTU informatiche costituirebbe, di fatto, una denegata giustizia; inoltre non rispetterebbe, neppure per finzione, il precetto costituzionale secondo cui la giustizia è amministrata «in nome del popolo» (art. 101 Cost.), perché la decisione e la cognizione su tali contratti verrebbe di fatto demandata a tecnici (CTU informatici), la cui scelta non potrebbe in alcun modo ritenersi *precostituita* per legge (come nel caso del giudice naturale: art. 25 Cost.), né soggetta a controllo basato su norme di legge (come avviene per l'accesso alla Magistratura).

6.6. *Smart contracts* e imputabilità dell'*Artificial Intelligence*

Se lo *smart contract* integra un «agente informatico» dotato di intelligenza artificiale (AI: *Artificial Intelligence*), capace di governare le sopravvenienze nei contratti di durata, dovremo poi misuraci con l'art. 1349 cod. civ. ed eventualmente con i limiti nel c.d. *arbitraggio della parte*, se tale *software* è concepito unilateralmente o viene introdotto in una contrattazione *standard* unilateralmente predisposta.

Allo *smart contract,* quale agente informatico di *AI*, può poi essere demandata non solo la gestione o esecuzione di contratti (tradizionali), ma anche la stessa conclusione di futuri contratti (ne è già diffusa l'applicazione nel mercato finanziario: si pensi all'*High frequency trading*, impraticabile con efficienza dagli esseri umani).

Si dirà che l'oggetto dei futuri contratti è in questo caso determinabile *per relationem* all'opera dello *smart contract*, ma esso potrebbe essere *imprevedibile* a priori[34].

Ci si chiede allora se ne venga pregiudicata l'imputabilità giuridica del futuro contratto al patrimonio dell'essere umano o della persona giuridica, che si avvale dello *smart contract.*

[34] Cfr. G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, p. 456, che osserva condivisibilmente: «Il contenuto del contratto è dunque determinabile, ma secondo modalità che non sempre consentono una pre-comprensione. Occorre dunque chiedersi se di volontà in senso stretto si tratta, anticipatamente dichiarata, rispetto all'effettivo formarsi delle condizioni contrattuali e quindi del contenuto negoziale, almeno in parte, oppure se non sia invece più aderente rappresentare tutto ciò nei termini di un sistema di assunzione del rischio. In altri termini, la narrazione giuridica può declinarsi affermando che il contraente ha accettato il rischio di concludere il contratto attraverso un dato sistema informatico che utilizza un programma di intelligenza artificiale, o affermando che lo stesso contraente ha concluso un contratto con oggetto determinabile attraverso un sistema di intelligenza artificiale».

La risposta mi pare debba essere negativa, perché l'ordinamento già prevede casi in cui la *suitas* dell'atto o negozio giuridico è legata alla logica del *rischio* di avvalimento di strumenti tecnologici: così è, sia nelle norme di settore sulla custodia del meccanismo di firma digitale (art. 20 co. 1 *bis* CAD), sia nella disciplina codicistica della responsabilità civile per custodia di cose (art. 2051 cod. civ.), che potrebbe essere qui richiamata per analogia[35].

7. Spunti di riflessione conclusivi

Gli *smart contracts* promettono di rimuovere dalle transazioni commerciali la stessa possibilità di inadempimento, perché lo scambio avverrebbe *solo e quando* le due prestazioni siano contestualmente eseguite.

Non è questo, forse, un ritorno ad una *realità* convenzionale del contratto?

E non segna, di fatto, una fuga dal concetto stesso di *obbligazione* quale *iuris vinculum* con il quale si programma ed impegna il futuro?

Il pendolo storico si sposta dunque dalla *promessa* di fare o dare, al *fare* o *dare* contestuale.

E non è questa una patente sfiducia nell'effettività del sistema giuridico?

Sotto altro profilo, le nuove tecnologie devono indurre il giurista a mutamenti di prospettiva anche riguardo agli stessi tradizionali istituti giuridici.

Può ricordarsi qui come è stato modificato e vivificato il concetto, di teoria generale del contratto, di forma scritta e scrittura privata.

Grazie alle norme speciali (artt. 1, co. 1, lett. *p*) e *p-bis*) e 20 CAD), di definizione del documento informatico e di equiparazione del medesimo, se munito di firma digitale, alla scrittura privata «analogica» (artt. 1350 e 2702

[35] Ciò non esclude la opportunità di concepire nuove regole di settore. Il tema è affrontato nella Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), di cui si è fatto cenno *supra*, che indica, nel considerando «AG» «che sono palesi le carenze dell'attuale quadro normativo anche in materia di responsabilità contrattuale, dal momento che le macchine progettate per scegliere le loro controparti, negoziare termini contrattuali, concludere contratti e decidere se e come attuarli rendono inapplicabili le norme tradizionali; [...] che ciò pone in evidenza la necessità di norme nuove, efficaci e al passo con i tempi che corrispondano alle innovazioni e agli sviluppi tecnologici che sono stati di recente introdotti e che sono attualmente utilizzati sul mercato» e prospetta (punto 59, lett. f) «l'istituzione di uno status giuridico specifico per i robot nel lungo 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».

cod. civ.), si sono infatti aperti nuovi spazi nella forma documentale: si pensi alla documentazione digitale della conclusione di un contratto, laddove la riproduzione delle immagini dei soggetti fisici che emettono oralmente le dichiarazioni costituenti l'accordo contrattuale può semplificare l'attività di interpretazione del contratto che, firmato digitalmente, rispetterà altresì i requisiti formali dello scritto, pur potendo constare di una rappresentazione multimediale di persone dichiaranti, di cose contrattate, ecc.

Il «nuovo», portato dell'informatica in campo contrattuale, non deve dunque sconcertare, ma non può portare in modo idiosincratico al ripudio delle attuali regole, perché, come bene è stato detto, «il giurista è interprete e non mero contabile del diritto»[36], né – spesso per scarsa conoscenza delle tecnologie o delle branche dello scibile diverse dalla propria – può portare il giurista a coonestare o ipostatizzare, per un malinteso «modernismo», ogni novità tecnologica che gli si ponga sotto gli occhi.

Francesco Delfini
Università degli Studi di Milano
via Festa del Perdono 7, 20122 Milano
francesco.delfini@unimi.it
Orcid: 0000-0001-6426-8602

[36] Finocchiaro, G., *ult. op. cit.*, p. 459.