Guida pratica digitalizzazione per l'estero.

TECH LAW: blockchain, smart contract, token, big data e cryptovalute.

Regione Lombardia e Unioncamere Lombardia hanno ritenuto opportuno sviluppare la redazione di tale Guida che mira all'analisi del profilo normativo ed alla connessione funzionale che intercorre fra Big Data, Blockchain, Cryptovalute e Smart Contract come strumenti sempre più utilizzati nella vita delle imprese e dei singoli individui. La presente Guida è realizzata nell'ambito del programma internazionalizzazione 2021 di Regione Lombardia e Unioncamere Lombardia.

unioncamerelombardia
camere di commercio lombarde

Regione Lombardia

DIGITALIZZAZIONE PER L'ESTERO

TECH LAW: *BLOCKCHAIN, SMART CONTRACT, TOKEN, BIG DATA E CRYPTOVALUTE*.

La Guida è stata curata da Marco Tupponi – Studio Tupponi, De Marinis, Russo & Partners, su commissione di Regione Lombardia ed Unioncamere Lombardia.

Aggiornata a novembre 2021.

Pubblicazione fuori commercio.

È consentita la riproduzione con citazione della fonte.

TUPPONI, DE MARINIS, RUSSO & PARTNERS
INTERNATIONAL BUSINESS LAW FIRM

INDICAZIONI PER LA LETTURA DELLA GUIDA

Per una migliore comprensione si suggerisce di leggere il commento al testo fatto dall'Autore e le norme ad esso collegate.

INDICE

Capitolo 1) *Blockchain* ed eIDAS

1.1) Definizione di *Blockchain*

1.2) Come funziona la *Blockchain*

1.3) Le caratteristiche della *Blockchain*

1.4) Regolazione e *Governance*

1.5) La regolamentazione che governa l'utilizzo della *Blockchain*.

1.6) *Blockchain* e GDPR

1.7) Alcune tipologie applicative di *Blockchain*

1.7.a) *Blockchain* come strumento di lotta alla Contraffazione

1.7.b) Operazioni con l'estero e *Blockchain*

1.8) eIDAS e *Blockchain*

1.9) Utilizzo della tecnologia *Blockchain* nella governance delle Imprese e le implicazioni nei mercati finanziari.

1.10) Il Regolamento eIDAS (UE) n. 910/2014 in particolare

1.10.a) Le caratteristiche della firma elettronica

1.10.b) Caratteristiche dell'utilizzazione della firma digitale

1.11) Identità Auto Sovrana e Progetto eIDAS *Bridge*

1.12) …. Continua: il ruolo della tecnologia dei registri distribuiti

2) Capitolo 2) Le ICO – *Initial Coin Offering* ed i *Token*

2.1) Le ICO - *Initial Coin Offering* storia e finalità

2.2) Le ICO come raccolta pubblica di capitale

2.3) I *Token*: definizione

2.4) La *tokenizzazione*

2.5) Le "proprietà" *smart*

2.6) Classificazione dei *Token*

2.7) Natura giuridica *dell'investiment* token come "prodotto/strumento finanziario"

3) *SMART CONTRACT*

3.1) Gli antecedenti degli *Smart Contracts*

3.2) Caratteristiche tecniche e tecnologiche degli *Smart Contracts*

3.3.a) DLT *Digital Ledger Technologies*.

3.3.b) Automaticità dell'adempimento.

3.4) La natura giuridica di uno *Smart contract.*

3.5) Le maggiori differenze tra gli *Smart contracts* ed i contratti disciplinati dal codice civile.

3.5.a) La Fiducia

3.5.b) L'Accordo delle parti

3.5.c) La Responsabilità civile

3.5.d) Le Clausole vessatorie

3.5.e) La Lingua dello *Smart contract*

3.5.f) The DAO – *Decentralized Autonomous Organizations*: un caso emblematico

3.6) Vizi nella formazione dello *Smart Contract*

3.7) Gli Oracoli

3.8) Il Momento di passaggio della proprietà e momento di passaggio dei rischi

3.9) Interpretazione dello *Smart contract*

3.10) La Forma dello Sma*rt Contract*

3.11) L'Adempimento del contratto e Buona Fede

3.12) L'Integrazione e l'Esecuzione forzata del contratto

3.13) La Legge applicabile ed il Foro competente

3.15.a) La Legge applicabile

3.15b) Il Foro competente e l'Arbitrato

3.16) La Risoluzione delle controversie in tema di *Smart contract* - un esempio nell'UE: la piattaforma ODR (*On Line Dispute Resolution*)

3.17) Gli *Smart contracts* e gli *Incoterms ICC* 2020

3.18) Cenni di normativa internazionale e comparata

4) LE CRYPTOVALUTE: PROFILI GIURIDICI

4.1) Storia ed inquadramento

4.2) Natura giuridica delle *cryptovalute*

4.2.1) Moneta: origini e funzioni

4.2.2) Sistema dei pagamenti

4.2.3) Le monete alternative

4.2.4) La rivoluzione informatica

4.2.5) *Bitcoin*/*cryptovalute* e moneta

4.2.6) *Cryptovalute* e moneta elettronica

4.2.7) *Cryptovalute* e moneta complementare

4.2.8) *Cryptovalute* come bene?

4.3) *Cryptovalute* e documento informatico

4.4) *Cryptovalute* e strumento finanziario/prodotto finanziario?

4.5) I vantaggi di *bitcoin* e delle *cryptovalute*

4.6) Il funzionamento del Sistema delle *cryptovalute*

4.7) Il prezzo del *bitcoin*

4.8) I principali rischi connessi all'uso di *bitcoin*/*cryptovalute*

4.9) La regolamentazione normativa in Italia ed all'Estero

4.9.a) Italia

4.9.b) Paesi Esteri

5) I *BIG DATA*

5.1) Nozione e funzione dei *Big Data*

5.2) Le attività che conferiscono valore ai dati:

5.2.a) Raccolta dei dati

5.2.b) Archiviazione dei dati

5.2.c) Analisi ed Organizzazione dei dati

5.2.d) L'utilizzo dei dati inclusa la vendita dei dati

5.3) I Rischi derivanti dalle attività tipiche dei *Big Data Submarkets*.

5.4) I *Data Brokers*

5.5) I limiti giuridici all'accesso ai dati personali: trattamento e uso - diritto alla *privacy* (USA e UE).

5.5.a) Il modello statunitense e quello europeo

5.5.b) USA

5.5.c) Unione Europea

5.6) I limiti al trattamento dei dati personali.

5.6.a) Il Principio di minimizzazione.

5.6.b) Il diritto alla trasparenza, accesso e rettifica

5.6.c) Il diritto alla limitazione ed alla cancellazione dei dati

5.6.d) Il diritto alla Portabilità dei dati

5.7) La disciplina dell'accesso ai dati personali nella U.E.

5.8) La cosiddetta *group privacy*

5.9) Gli algoritmi utilizzati per elaborare i dati

5.10) La "proprietarizzazione" dei dati personali nel Regolamento U.E. 2016/679.

5.11) Paragone con il diritto d'autore ed il diritto di licenza

5.12) I limiti giuridici all'accesso ai dati non personali: proprietà e regolamentazione

5.12.a) Alle radici di un dibattito essenzialmente europeo

5.12.b) I *Big Data* e allocazione giuridica dei "nuovi" beni immateriali

5.12.b.1) Il diritto d'autore

5.12.b.2) La tutela giuridica delle banche dati: la Direttiva 96/9/CE

5.12.b.3) La tutela brevettuale

5.12.b.4) Il segreto commerciale: la Direttiva (UE) 2016/943 – TUTELA RESIDUALE

5.13) Gli accordi di esclusiva fra le intese restrittive della concorrenza e l'abuso di posizione dominante

5.14) Il diritto dei consumatori a tutela delle imprese: la Direttiva 93/13/CEE

5.15) Il diritto di portabilità dei dati non personali

CAPITOLO 1

BLOCKCHAIN ed eIDAS

1.1 Definizione di *Blockchain*

La *Blockchain* può essere considerata come una sequenza cronologicamente determinata di blocchi, contenente informazioni, che si sviluppa da un tempo passato (il primo blocco della catena) verso il presente (l'ultimo blocco della catena).
Ogni singolo blocco – nodo/*computer* è validato da tutti gli altri blocchi – nodi/*computers* della catena.

La forma più nota di *Blockchain* è quella di *Bitcoin* e delle *cryptovalute* che saranno esaminate al capitolo 4) della presente Guida,

Genericamente la *Blockchain* rappresenta una struttura di dati e quindi di informazioni condivisa e immutabile.

Da un punto di vista pratico, la *Blockchain* permette di gestire un *database* in modo distribuito, consiste quindi in un'alternativa agli archivi centralizzati e permette di controllare il continuo aggiornamento dei dati con la collaborazione di tutti gli utenti partecipanti alla rete e garantendo la possibilità di condividere tali dati rendendoli così accessibili ad ogni partecipante.

Questa lista di blocchi collegati tra loro è resa sicura tramite l'uso della crittografia.

In termini tecnici, questo sistema permette di gestire i dati, verificati e autorizzati, senza il bisogno di un'autorità centrale.

Alcuni esperti definiscono la *Blockchain* come la "nuova generazione di internet", in quanto potrebbe essere assimilata ad un *browser* che permette di effettuare delle "transazioni".

Cioè la *Blockchain* rappresenta un registro digitale – *ledger* - aperto e distribuito, all'interno del quale le voci sono raggruppare in blocchi, uniti l'uno all'altro in ordine cronologico, in modo da creare una catena digitale di informazioni ordinate digitalmente.

Qualsiasi genere d'informazione o dato può essere digitalmente rappresentato ed essere contenuto e conservato all'interno di una piattaforma *Blockchain*.

1.2 Come funziona la *Blockchain*

La *Blockchain* è formata da **due elementi principali**:

1) i nodi/*computers* e
2) i *miners*.

I nodi/*computers* sono tutti i *computers* della rete che hanno scaricato la *Blockchain* nella loro memoria; chiunque potrebbe diventare un nodo, attraverso l'apposito programma.

I *miners*, invece, sono coloro che effettuano il controllo delle "transazioni", grazie all'utilizzo di *computers* molto potenti ed energivori e attraverso un protocollo di validazione complesso.

Il protocollo di validazione rappresenta l'elemento vitale della *Blockchain*, perché è proprio da questo che dipendono sostanzialmente la velocità della catena e la sua sicurezza, inoltre, esso definisce gli algoritmi validanti e chi può essere un *miner*.

In questo ambito si caratterizzano le principali evoluzioni che vanno a diversificare le tipologie di *Blockchain*.

Non esiste un protocollo di validazione migliore di un altro, tutto dipende dal campo di applicazione nel quale deve essere usato.

Prendiamo brevemente in esame i tre principali **protocolli di validazione**:

1) *Proof of Work*

Questo è il protocollo di validazione primigenio, sul quale si è basata la prima e più famosa *Blockchain* che è quella utilizzata per "veicolare" i *Bitcoins*.

Il funzionamento è il seguente: ogni dieci minuti viene immesso un nuovo blocco nella *Blockchain*, il quale contiene migliaia di "transazioni".
La criticità di questo meccanismo è nella velocità, in quanto per controllare un blocco è richiesta una crescente potenza elaborativa da parte dei *computers* dei *miners*, poiché la *Blockchain* diventa sempre più grande.

2) *Proof of Stake*

Questa validazione nasce per fare fronte al problema della scalabilità del protocollo "*Proof of Work*", attraverso una semplificazione del processo di *mining* – validazione.
Il nuovo protocollo prevede che ogni volta che è aggiunto un nuovo blocco, viene automaticamente scelto anche il creatore del blocco successivo.
Per effettuare questa operazione di selezione è possibile utilizzare diversi metodi.

Questi due appena descritti sono i principali metodi di validazione utilizzati, in seguito ne sono stati creati altri, tra i quali troviamo di particolare interesse citare il:

3) *Federated Byzantine Agreeent* (FBA)

Questa metodologia è basata su unità di fiducia decise dai singoli *server* che insieme stabiliscono il livello di consenso del sistema.
E' stato sviluppato da *Stellar Development Foundation* ed è utilizzato dalla *Blockchain* chiamata *Stellar*.

Tutti i dati inseriti all'interno di una *Blockchain*, solitamente chiamati "**transazioni**", sono memorizzati in maniera:

- sicura,
- verificabile,
- permanente.

La *Blockchain* consiste quindi in un protocollo di comunicazione, che identifica una tecnologia basata sulla **logica del *database* distribuito.**

Si sottolinea che la *Blockchain* è costituita da una serie di blocchi che archiviano un insieme di transazioni e quindi informazioni validate e correlate da un **Marcatore Temporale che viene**

predisposto tramite un *hash* ogni blocco contiene il proprio marcatore temporale - *hash* e quello del blocco precedente.

Il Marcatore Temporale consiste nel processo di generazione e apposizione su un documento digitale di una sequenza di caratteri, attuati tramite *hash*, che rappresentano **una data e un orario**, per accertare l'effettivo avvenimento di un certo evento.

L'*hash*, è un'operazione che produce una serie di *bit* e che permette di mappare una stringa - *digest*, cioè una sequenza di caratteri di testo, di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata.

La lunghezza dei valori di *hash* varia a seconda degli algoritmi utilizzati.

La funzione di *hash* è quella di essere "l'impronta digitale" di un testo e quindi ad una caratteristica che lo identifica in maniera univoca.

L'*hash* identifica in modo univoco e sicuro ciascun blocco, permettendo il collegamento con il blocco precedente tramite identificazione.

La caratteristica fondamentale di queste funzioni è la loro pressoché impossibile invertibilità: in questo modo, dato un valore di *hash*, **è impossibile risalire al messaggio che l'ha generato**; è inoltre molto difficile produrre un messaggio che fornisca una stringa predeterminata.

Ogni minima modifica del *file* o del testo produrrà una diversa stringa in uscita (cosiddetto "effetto valanga").

Una delle maggiori applicazioni dell'*hash* si ha nell'utilizzo delle **firme digitali**

Le funzioni *hash* svolgono un ruolo essenziale nella crittografia in quanto sono utili per verificare l'integrità di un messaggio poiché l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un *message digest*, cioè un risultato, completamente differente rispetto a quello calcolato sul testo originale rivelando la tentata modifica.

UN ESEMPIO PRATICO è quello di una "transazione" tra due soggetti, da A a B, per la **vendita di un immobile.**

Per prima cosa viene creata una "transazione" con elementi quali l'indirizzo pubblico di B, le informazioni relative alla "transazione" e le *Cryptographic Key*.

In questo caso le informazioni comprenderebbero quelle relative all'immobile, la disponibilità economica di B, l'effettiva proprietà dell'immobile da parte di A ed eventuali altre informazioni necessarie a completare il quadro di riferimento per la vendita e l'acquisto.

Entrambe le parti avranno la propria Chiave Crittografata.

La "transazione" di un'unità di valore comincia con la firma digitale di A e la sua Chiave Crittografata, diretta verso B.

In questa maniera viene creato un nuovo blocco, contenente tutti i dati relativi alla "transazione" sopra elencati.

Il blocco, che comprende anche altre "transazioni" identiche a livello metodologico, viene preparato per essere sottoposto alla verifica e all'approvazione dei partecipanti alla *Blockchain*.

Per farlo, il blocco viene portato in Rete e, una volta verificato dai *miners*, viene aggiunto alla catena di blocchi che forma la *Blockchain*.

Questo significa che **il blocco** è ora accessibile a tutti i partecipanti, essendo **nell'archivio** e diventa un riferimento permanente, immutabile e immodificabile di quella "transazione" e di "transazioni" come quella.

La specifica "transazione" è completata ed il metodo, assieme alla specifica "transazione", è inglobato nella *Blockchain*.

1.3) Le caratteristiche della *Blockchain*

1) decentralizzazione
2) trasparenza

3) immodificabilità
4) affidabilità
5) sicurezza
6) Tracciabilità

Con "decentralizzazione" si intende lo sfruttamento di un ***networking* distribuito – "la catena"**, cioè un sistema di memorizzazione dei dati su tutta la rete, così da evitare che ci sia un punto centralizzato che potrebbe essere sfruttato da un *hacker* per abbattere l'intero sistema della *Blockchain*.

La *Blockchain* è definita **trasparente** perché le "transazioni" effettuate attraverso essa sono visibili a tutti i partecipanti.
In base a questi principi, la *Blockchain* riesce a generare un nuovo concetto di fiducia, tanto da riuscire a creare una nuova forma di rapporto sociale, dal momento in cui tutti gli archivi nei quali sono registrati i dati sono inalterabili e immodificabili, risultando così immuni alla corruzione.

1.4) Regolazione e *Governance*

Per poter esaminare in maniera esaustiva la regolamentazione riguardante la *Blockchain* e i suoi svariati utilizzi, è necessario fare una prima distinzione tra:

1) **il codice legale**, cioè l'insieme di regole costituite da obblighi di legge e

2) **il codice tecnico - informatico**, cioè quello riguardante *software* e protocolli informatici.

a) La differenza principale tra questi due codici riguarda il grado di influenza sulle attività, in quanto le regole del **codice legale** possono essere inadempiute seppur incorrendo in conseguenze giuridiche.

b) Al contrario, le regole del **codice tecnico – informatico** – *coding* - non possono essere inadempiute, poiché si genererebbe un errore tecnico/informatico e di conseguenza non verrebbe svolta l'attività richiesta e si bloccherebbe il funzionamento del meccanismo.

Ovviamente le regole che riguardano il **codice legale** prevalgono a livello di "fonte" rispetto al **codice tecnico – informatico** nel senso che le "regole giuridiche" a monte sono sempre alla base e prevalenti a qualsiasi attività umana anche se compiuta in modo automatico tramite meccanismi tecnico – informatici.

Facciamo l'esempio di *Bitcoin,* che evidenzia la possibilità di far esistere un sistema contabile finanziario senza alcuna regolamentazione. **(Si veda il capitolo 5 della presente guida)**

Tutti i partecipanti a *Bitcoin* devono seguire le regole del codice tecnico – informatico.
Tutti gli utenti utilizzano gli stessi *software* e sono obbligati tecnicamente ed informaticamente ad usare un certo tipo di "transazioni".

Non esistono delle leggi scritte all'interno di un codice tecnico - informatico che possano limitare o regolamentare queste "transazioni", ma gli utenti sono comunque "forzati" a seguire una certa condotta, obbligati a ciò dall'aspetto tecnico - informatico.
Tale vincolo obbligatorio si può ipotizzare che assuma la natura giuridica di un **uso normativo**

Il funzionamento di *Bitcoin* è concettualmente semplice: gli utenti possono spendere solo i *coins* che possono dimostrare di possedere tramite delle chiavi crittografate.
Inoltre, per evitare che gli utenti modifichino queste regole tecniche, la *Blockchain* richiede che ogni "transazione" sia approvata – *mining* - prima che diventi effettiva, garantendo così sicurezza all'intero sistema.

Con riguardo al **settore finanziario**, inoltre, possiamo suddividere due tipologie di **regolamentazioni**, quelle **private** e quelle **pubbliche**.

1) Mentre **le regolamentazioni private**, chiamate *governance*, servono a regolamentare le azioni di tutti i partecipanti aventi rapporti con un'organizzazione privata al fine di ottenere coordinamento e, di conseguenza, benefici, come **per esempio** quella del circuito Visa, emanate da Visa. Inc.

2) **Le regolamentazioni pubbliche**, invece, riguardano il sistema finanziario di ogni singolo Stato e devono tenere in considerazione il fatto che nell'economia moderna tutti gli Stati debbano interagire tramite atti finanziari.

1.5) La regolamentazione che governa l'utilizzo della *Blockchain*.

Questa tecnologia è regolata da un sistema tecnico - informatico.

Occorre notare però che, esattamente come il sistema legale, anche quello tecnico - informatico deve essere gestito alla base da persone fisiche in grado di definire le regole sulle quali si baserà il funzionamento della *Blockchain*.

Per ogni *software* che lavora sulla *Blockchain*, esiste **uno sviluppatore/programmatore** che ha il compito di gestirne il funzionamento, migliorarla e risolvere i malfunzionamenti.

Tramite degli aggiornamenti, lo sviluppatore/programmatore può modificare tutti gli aspetti del *software*.

Nel caso gli sviluppatori/programmatori siano molteplici, e questo è il caso più probabile vista la complessità e l'importanza del sistema, sarà presente un documento nel quale gli sviluppatori/programmatori attesteranno che ogni modifica rilevante al *software* dovrà essere approvata – *mining* - da tutti gli altri prima di renderla effettiva.

Il problema di questo tipo di *governance* sussiste nel momento in cui alcune decisioni finiscono per privilegiare alcuni soggetti e partecipanti alla *Blockchain* piuttosto che altri, dal momento in cui tutto il procedimento è strettamente connesso con i loro interessi.

I *softwares* di *Blockchain* sono basati su delle basi anti-istituzionali, ed è evidente che il mero codice tecnico - informatico non possa più essere sufficiente alla regolamentazione.

In futuro si renderà necessaria la creazione di un codice di norme più definito, nonostante possa risultare complesso, perché in un sistema decentralizzato, quale la *Blockchain*, è difficile regolamentare quali *softwares* possono essere installati o meno da un utente sul proprio *computer*.

Di conseguenza, fino ad oggi, tutte le regolamentazioni relative al sistema finanziario informatizzato sono state rivolte alle imprese che operano in questo settore, piuttosto che alla creazione di leggi di carattere generale e statuale.

1.6) Blockchain e GDPR

(si veda anche il rapporto GDPR e *Big Data* al Capitolo 5 della presente Guida)

Per poter comprendere i possibili ambiti di applicazione della tecnologia *Blockchain* è necessario introdurre il Regolamento Generale sulla Protezione dei Dati (GDPR).

Il **Regolamento Generale sulla Protezione dei Dati - GDPR, ufficialmente Regolamento UE n. 2016/679**, è un regolamento dell'Unione Europea che riguarda il **trattamento dei dati personali e la *privacy*.** Questo è stato pubblicato sulla Gazzetta ufficiale dell'Unione Europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio 2016.

In Italia ha sostituito la Direttiva 95/46/CE e ha abrogato gli articoli del codice per la protezione dei dati personali che erano incompatibili con esso.

Il Regolamento in questione è diretto alle imprese ed enti, sia pubblici che privati che trattino dati personali delle persone fisiche non prendendo quindi in considerazione i dati personali delle imprese e degli altri enti.

Il fine di questo Regolamento è quello di rafforzare la protezione dei dati personali dei cittadini e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini.

I dati personali vengono definiti ex **paragrafo 1 articolo 4** _ come "*qualsiasi informazione riguardante una **persona fisica identificata o identificabile**; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica ,economica, culturale o sociale*".

In sintesi, il GDPR:

1. introduce regole più chiare sull'informativa e sul consenso e **definisce i limiti al trattamento autorizzato dei dati personali**;
2. stabilisce **criteri per il trasferimento dei dati all'infuori dell'Unione Europea** e stabilisce le norme per i casi di violazione dei dati;
3. pone le basi per **l'esercizio di nuovi diritti**.

Il nuovo Regolamento ha degli effetti rilevanti in tre ambiti particolari della *Blockchain*:

1) i dati archiviati in una *Blockchain* sono a prova di manomissioni, quindi non sarà possibile cancellarli una volta che questi saranno all'interno della catena distribuita;

2) le *Blockchains* sono distribuite, quindi nemmeno il controllo sui dati può essere centralizzato, ma viene affidato a tutti i partecipanti della *Blockchain* stessa. Questi però non possono essere considerati dei *Data Protection Officer* - DPO, come richiesto dal GDPR;

3) gli *Smart Contracts* rientrano a fare parte del processo decisionale automatizzato, con la possibilità che si creino contestazioni giuridiche di vario tipo, ma non necessariamente dovranno essere inseriti in un meccanismo di *Blockchain* (anche se però costituisce il 98% dei casi) in quanto "la catena" potrebbe essere gestita da meccanismi informatici diversi.

Esplicitiamo quindi alcuni **interrogativi** che rimangono per adesso senza risposta, ma in attesa che la normativa possa intervenire per il corretto funzionamento della *Blockchain*:

1. Il **GDPR** prevede l'esistenza della figura del DPO - *Data Protection Officer*, ma può esistere una simile figura nel contesto di una *Blockchain* distribuita?

2. **In caso di controversie**, quali leggi devono essere applicata e di chi è la giurisdizione? Nel caso si verificasse una situazione nella quale non è possibile identificare il luogo in cui i dati vengono elaborati, è complicato capire quale giurisdizione deve effettuare la valutazione legale. (**Si veda il Reg. U.E. - n. 593 del 17 giugno 2008 c.d. Roma I al capitolo 3.15 della Presente Guida**)

3. All'interno di un *Blockchain*, quali dati possono essere considerati "personali"? L'identità dell'utente è protetta, quindi la normativa dovrebbe fornire una **definizione precisa di dato personale in questo ambito**, poiché non è chiaro se le chiavi pubbliche crittografate siano considerate come dato personale o meno.

4. In una *Blockchain* **i dati vengono mantenuti sui nodi – *computers* - della rete** indipendentemente dallo scopo per il quale questi erano stati inseriti al suo interno. Ci si domanda come si possa coordinare con questa caratteristica una normativa, il **GDPR**, che prevede che gli scopi specifici per i quali i dati personali sono trattati debbano essere specificati, espliciti e legittimi.
   Inoltre la normativa prevede anche che i dati siano **adeguati**, **pertinenti** e **limitati** a quanto necessario in relazione agli scopi per i quali sono trattati.

5. All'interno della *Blockchain*, come abbiamo visto, i dati non sono modificabili e spesso impossibili da aggiornare o eliminare, la conseguenza è quindi l'impossibilità di procedere con il cosiddetto **"diritto all'oblio"** all'interno di tale tecnologia.

Ci si chiede non solo se sia possibile una convivenza tra il **GDPR** e le caratteristiche della *Blockchain*, bensì si apre un ulteriore interrogativo sulla reale importanza dei diritti esecutivi dettati dal **GDPR** quando ci poniamo davanti a una tecnologia di *ledger* – registro - distribuito al posto di un *database* centralizzato controllato da un singolo *controller*.

Il problema principale risulta quindi l'incompatibilità di alcune caratteristiche della definizione di *Blockchain* e le richieste del GDPR.

Infatti, per definizione, tutti i dati inseriti nella *Blockchain* sono pubblici e accessibili da tutti gli utenti che partecipano alla catena, in aggiunta, i dati presenti nella *Blockchain* sono conservati a tempo illimitato.

È compito del legislatore riuscire a regolamentare la protezione dei dati personali GDPR e conciliarla con il sistema innovativo e complesso dato dalla *Blockchain*.

Oltre agli aspetti critici dell'impatto del GDPR sulla *Blockchain* possiamo però evidenziare anche diversi **punti di forza**.

Primo fra tutti esaminiamo la cosiddetta "*security by design*", che, attraverso l'utilizzo della tecnologia *Blockchain*, permette di:

1) disaccoppiare i dati dall'identità individuale che li fornisce e
2) minimizzare questi dati, cioè condividere solo quelli assolutamente necessari.

La protezione dei dati è assicurata dalla chiave pubblica del mittente della transazione e anche da quella del destinatario.

3) Inoltre, troviamo la presenza della crittografia, che assicura l'invariabilità di ciò che è contenuto all'interno della transazione.

A livello informatico è impossibile ricostruire il contenuto di una transazione dall'*hash* – mappatura dei dati - crittografico monodirezionale, che, in parole semplici, si traduce nel fatto che anche se una *Blockchain* è "pubblica", nessuna informazione personale può essere resa pubblica in senso assoluto.

1.7) Alcune tipologie applicative di *Blockchain*

1.7.a) *Blockchain* come strumento di lotta alla Contraffazione

Il settore VITIVINICOLO

L'Ispettorato Centrale della Tutela della Qualità e della Repressione Frodi (ICQRF) evidenzia come la maggior parte delle notizie di reato in ambito agroalimentare in Italia negli ultimi anni si sia concentrata nel settore vitivinicolo.

A questo si deve aggiungere il tema delle contraffazioni e dell'*italian sounding* all'estero di prodotti *made in Italy*, che resta ancora un grave problema e che fa perdere fior di quattrini ai nostri produttori.

Nonostante l'Italia adotti un sistema di certificazione di qualità sofisticato e affidabile, tra i migliori al mondo, un potenziamento dello stesso, che consenta una più elevata trasparenza dei prodotti, andrebbe a tutelare maggiormente sia il produttore che il distributore ed anche il consumatore finale.

A tal fine, uno strumento che può essere integrato in modo efficace nelle filiere del vino è la *Blockchain*.

Teniamo presente, come più volte già detto, che la *Blockchain* è un sistema decentralizzato di immagazzinamento dati in modo che, una volta inserite le informazioni relative a un certo prodotto (che possono andare dalle materie prime, alle lavorazioni, alla logistica etc.), queste informazioni fuoriescono dal controllo diretto di chi le ha immesse nel sistema e restano visibili per tutti i nodi/*computers* collegati e soprattutto restano inalterabili.

Quindi, chiunque desideri controllarle ha la sicurezza che non possono essere state modificate nel tempo.
Quando si parla di **vino**, che è un prodotto complesso al palato e pochi sono gli esperti in grado di distinguere un vino di qualità da un surrogato che ne imiti le caratteristiche, avere a disposizione un tracciamento decentralizzato rappresenta un vantaggio e una tutela in più per il consumatore finale.

Però la *Blockchain* ha anche alcune criticità in quanto il meccanismo non garantisce di per sé la veridicità dei dati inseriti.

Il produttore o trasformatore che abbia intenzioni di compiere frodi può caricare informazioni false o, molto più semplicemente, si può ricadere in un errore umano e in buona fede immettere informazioni scorrette sulla piattaforma *Blockchain*.

In questo caso, poiché i dati non sono più modificabili, se la rilevazione della loro inattendibilità passa inosservata, rimane il rischio che il consumatore sia raggiunto da informazioni inattendibili relative al prodotto.

Per far fronte almeno in parte a questa problematica è possibile integrare la sequenza *Blockchain* con dei *softwares* di analisi/**Oracoli** (**si veda il capitolo 3.9 della Presente Guida**) che consentono di individuare eventuali incoerenze o mancanze.

Da ciò deriva l'importanza di una strategia di filiera.

Facciamo un esempio: ipotizziamo che il produttore A conferisca alla cantina B un certo quantitativo di uve tracciate in *Blockchain*.
Ipotizziamo che la cantina B dichiari nella *Blockchain* la produzione di una quantità di vino che non è coerente rispetto alle uve conferite.
In questa ipotesi è possibile rilevare automaticamente l'incongruenza e attivare gli organi di controllo e tutela.

Da questo esempio si ricavano le potenzialità della *Blockchain* là dove sono presenti più produttori, più trasformatori e più distributori.

Nel caso in cui alcuni soggetti provino ad adottare comportamenti illeciti che potrebbero danneggiare altri soggetti coinvolti in filiera, un utilizzo corretto della *Blockchain* aiuta a tutelare gli operatori onesti e quindi anche a beneficio del consumatore finale.

La *Blockchain* potrebbe essere uno strumento efficace per la trasparenza e la tracciabilità del prodotto, ma **la sua efficacia aumenta se applicata in maniera sinergica tra produttori, distributori, trasportatori, rivenditori**, ecc.
Offrire al mercato interno e soprattutto estero informazioni trasparenti, certe e inalterabili sul prodotto è un modo efficace e serio di tutelare la reputazione e la qualità dei vini italiani, nonché dei marchi dei produttori.

Elenco qui di seguito alcune soluzioni *Blockchain* attualmente disponibili precisando che con tali soluzioni l'Italia si colloca in posizione pionieristica nel settore vitivinicolo dimostrando di saper mettere la creatività digitale al servizio dell'innovazione di settore

Ecco i tre esempi:

1. ***Wine Blockchain***: nato dalla collaborazione della startup padovana EZ Lab ed Ernst &Young, rappresenta il primo caso al mondo di servizio *Blockchain* applicato all'ambito del vino. La sperimentazione e implementazione è stata condotta in collaborazione con la foggiana Cantina Volpone.
2. ***BPPB Winechain***: è un progetto della Banca Popolare di Puglia e Basilicata (BPPB), sviluppato sempre in collaborazione con EZ Lab e implementato con la Cantina Due Palme di Brindisi.
3. ***Italian Wine Crypto Bank (IWCB):*** è la prima banca del vino al mondo e ha lo scopo di promuovere i più prestigiosi vini italiani, coniugando l'operazione commerciale alla finanza legata alle *cryptovalute*. Le cantine aderenti, i consumatori e gli investitori hanno la possibilità di acquistare, vendere o fare *trading* mediante *token* digitali che sono interamente garantiti dal valore del vino custodito dalla banca.

Oltre a questi progetti italiani, vale la pena concludere menzionando VinAssure, ideato da IBM, che ha messo a disposizione la sua *Blockchain* Transparent Supply per le catene di fornitura, ed eProvenance, specializzata in monitoraggio e analisi dei canali di distribuzione del vino.
L'obiettivo di VinAssure è tracciare il processo produttivo dalla vite al bicchiere seguendo il principio *from the land to the fork* che è alla base del Codex Alimentarius Europeo. Attualmente questa soluzione è stata adottata da grossi importatori e imprese vinicole statunitensi, come De Maison Selections e Ste. Michelle Wine Estates.
La Italian Wine Crypto Bank, prima cripto-banca del vino italiano basata su blockchain e criptovalute, nasce come iniziativa promozionale per i vini italiani a livello globale.

È il risultato della fusione rivoluzionaria di due mondi.

Da una parte c'è il mondo "tradizionale" del buon vino italiano, le sue cantine, i suoi distributori, i suoi appassionati collezionisti di tutto il mondo.

Dall'altro lato c'è l'innovativo mondo dei Digital Assets e la sua rivoluzionaria tecnologia blockchain.

Il fondatore e direttore di Italian Wine Crypto Bank, Rosario Scarpato, è l'amministratore delegato di The I Factor LTD, la società con sede a Hong Kong che possiede e gestisce il progetto.
Negli ultimi venticinque anni, Scarpato ha creato e diretto imprese di successo in Australia, Hong Kong e Dubai, qui la IWCB ha il suo cuore tecnologico.
Oggigiorno l'emirato è un hub innovativo di punta nello scenario internazionale, capace di supportare tecnologicamente e sviluppare un progetto così ambizioso e futuribile.
La ragione sociale, invece, è stata stabilita ad Hong Kong, perché i vini italiani stanno conquistando sempre più spazio sul mercato cinese.

Italian wine crypto bank

La *Italian Wine Crypto Bank* di fatto è un luogo, non fisico, in cui comprare vini pregiati italiani utilizzando esclusivamente criptomonete.

La missione della Banca è promuovere i vini pregiati italiani nel mondo, sia a livello globale che su mercati nazionali.
Inoltre, mira a generare ritorni sostanziali, in vari modi, per tutti i suoi *stakeholder*.
La Banca ha tre principali gruppi di *stakeholder*:

1) le Cantine Partner che conferiscono i loro vini al portfolio IWCB, che li mette a disposizione dei propri clienti in tutto il mondo;
2) i clienti, appassionati e collezionisti di vino o di criptovalute;
3) gli investitori, soggetti che investono in sicurezza in IWCB *digital assets, token* emessi dalla IWCB supportati da *asset.*

La peculiarità di questa tipologia di acquisto è che tutto passa attraverso le *cryptovalute* più importanti, come i Bitcoin, ma non solo, in quanto è tutto certificato attraverso la *Blockchain*.
Il meccanismo è accuratamente spiegato da Davide Casalin, Responsabile IWCB per i rapporti con le cantine italiane:

“identifichiamo un lotto di vino che viene conferito dalla cantina alla banca, e in quel momento alla cantina riconosciamo un terzo del valore del mercato al dettaglio in *cryptovaluta*.
I vini vengono inseriti in catalogo e possono essere acquisitati dai correntisti, per berseli o per lasciarli come garanzia di investimento nei nostri magazzini, che si trovano in Belgio e hanno tutti gli standards di sicurezza e conservazione corretta del vino.
Al momento dell’acquisto, noi riconosciamo un altro terzo del valore, in euro, alle cantine che hanno conferito il vino.
In più, c’è la garanzia, per le cantine, che se il vino non viene venduto sul mercato entro 24 mesi, gli verrà pagato lo stesso perché sarà la stessa *Italian Crypto Wine Bank* ad acquistarlo”.

Inoltre, la cantina riceve anche degli “*utility token*” che sono gli “asset digitali” con cui *Crypto Bank* finanzia i suoi progetti.
I *token* possono essere scambiati tra azionisti e correntisti della Banca, o successivamente in luoghi di scambio, come già avviene per questi strumenti.

I “*digital asset*” sono qualsiasi contenuto archiviato digitalmente.
Per identificarli all’interno della moltitudine di prodotti e sottoprodotti digitali che ogni impresa possiede infatti è necessario che rispondano a tre caratteristiche fondamentali.
Gli asset digitali per definirsi tali devono:

1. essere digitali in origine,
2. avere una identificabilità univoca e
3. costituire un valore aggiunto.

Un “*utility token*”, invece, è un tipo particolare di *token* che aiuta nella capitalizzazione o nel finanziamento di progetti per *startup*, imprese o gruppi di sviluppo di progetti.
Utilizzato come biglietto per la partecipazione a vendite all'ingrosso per raccogliere capitali su un progetto consente di avere accesso futuro al prodotto o servizio di un’impresa.
Sono utili quando un’impresa desidera creare un coupon che può essere scambiato in futuro per l'accesso ai propri servizi, questo è spesso usato come strategia per ottenere finanziamenti per un progetto.
Peculiarità di questi *token* è che sono “non fungibili” - NFT, sono, infatti, comunemente definiti come “oggetti digitali creati su blockchain unici e immodificabili”, certificano che un digital asset è unico, quindi non intercambiabile, e la sua funzione è garantire che quello che i dati rappresentano non può essere copiato.

Ciò che viene creato su una *Blockchain* è una registrazione che rappresenta un "oggetto" (fisico o digitale) unico.

In termini più generali si può affermare che gli NFT riescono a riportare nel mondo digitale il concetto di scarsità dei beni presente nel mondo reale, rendendo uniche delle rappresentazioni informatiche che per loro natura sarebbero indefinitamente riproducibili.

Per quanto concerne la IWCB ogni bottiglia con gli NFT reca la firma dell'enologo o del titolare della cantina e la riproduzione dell'etichetta firmata è conservata in esemplare unico nella *Blockchain* della Banca.

In questo modo, non solo il possessore degli NFT ha la possibilità di collezionare un vino pregiato e vendere il suo token unico, facendoci un possibile guadagno per l'incremento fisiologico del suo valore, ma anche per l'unicità "artistica" dello stesso token.

Infatti, anche nel caso che decidesse di godersi il vino, gli rimarrà comunque la possibilità di collezionare sia la bottiglia reale (vuota) con l'etichetta firmata, sia l'etichetta unica digitale tracciata dall'NFT, entrambe con un valore di mercato, peraltro incrementabile.

Ultima novità pronta ad arrivare è la prima *criptovaluta* al mondo interamente garantita da vino, e, in particolare, da quello italiano di alta qualità: è disponibile dal 21 settembre 2021 lo "IWB", e ad emetterlo è l'IWCB.

Davide Casalin spiega:

"IWB è un rivoluzionario *utility token* che sarà scambiabile attraverso Latoken sul mercato secondario, sul quale potrà generare interessanti ritorni per i suoi possessori.

La grande novità rispetto a tutti gli altri token è che in ogni momento i suoi possessori possono redimerli, ottenendo vino pregiato italiano del portfolio dell'Italian *Wine Crypto Bank* per lo stesso valore pagato per i *token* nella IEO (*Initial Exchange Offering*).

Per la prima volta non solo l'investimento di chi compra *token* è totalmente garantito, ma consente anche l'accesso ad altri significativi benefici.

Gli IWB *token* in futuro serviranno anche a comprare vini direttamente dai produttori"

Partito nel dicembre 2020, il progetto dell'*Italian Wine Crypto Bank*, con la imminente emissione del *coins* IWB, entra nella sua terza fase.

Da ottobre 2021, e per la prima volta nel mondo, i possessori di *Bitcoin, Ethereum* e delle principali *criptovalute* potranno utilizzare le stesse per comprare i vini pregiati dell'*Italian Wine Crypto Bank*, per goderseli immediatamente o per investimento.

In quest'ultimo caso non solo vedranno incrementare il valore del vino ma riceveranno anche bonus esclusivi altamente remunerativi legati all'andamento della *criptomoneta* usata.

1.7.b) Operazioni con l'estero e *Blockchain*

Applicazione molto interessante della *Blockchain* è quella dell'utilizzo della stessa per migliorare e potenziare il commercio interno ed esterno all'Unione Europea.

All'interno di una pubblicazione dell'Organizzazione Mondiale del Commercio[1] si fa riferimento ad una "classica" transazione commerciale internazionale dal Kenya ai Paesi Bassi di una serie di prodotti (Rose e Avocado).

Il processo, da quanto si attesta nel documento, ha coinvolto più di 30 attori economici, 100 persone e con un numero di interazioni umane maggiori a 200; oltre a ciò la spedizione ha impiegato 34 giorni per arrivare a destinazione di cui 10 giorni di attesa per l'elaborazione dei documenti.

La grande complessità in termini di documentazione riguarda soprattutto i documenti riguardanti la transazione come il **contratto di vendita** con annessa una possibile bolla di accompagnamento, l'eventuale **lettera di credito**, i **documenti di trasporto** (come la *bill of loading*) e tutta una serie di documenti necessari alla frontiera (come certificati, licenze di esportazione, ecc.).

Tutta questa serie di pratiche, accettate e consolidate nel commercio internazionale, possono, dato l'altissimo numero di processi e attività, portare ad errori o frodi; l'utilizzo della *Blockchain* in tale ambito potrebbe snellire di molto tale meccanismo, anche se tale applicazione non è esente da difficoltà.

La grande complessità di documentazione è anche data, in parte, dalla copertura dei rischi possibili quando ci si interfaccia con operatori di altri paesi; in particolare gli agenti economici vogliono tutelarsi da mancati pagamenti o da merce difettosa attraverso strumenti molto usati, in cui le banche fungono da intermediari, nel contesto internazionale, ovvero le operazioni documentali. Esse si rifanno agli UCP 600, emessi dall'ICC[2], usi che adottati da ogni banca nel mondo che effettua tali operazioni.

Esse possono essere distinte in tre tipologie esposte in modo sintetico:

1) CAD: O incasso documentario, è uno strumento di garanzia che separa merce e documenti e con cui le banche delle rispettive parti effettuano uno scambio denaro-documenti (con determinati requisiti) lato compratore. Il rischio, con tale strumento, è di

[1] Emanuele Ganne, World Trade Organization, 2018, "Can Blockchain Revolutionize international trade?"

[2] https://www.iccitalia.org/prodotto/norme-ed-usi-uniformi-icc-relativi-ai-crediti-documentari/

poco diminuito in quanto il compratore potrebbe, una volta arrivate le merci, non adempiere al contratto con il risultato del blocco delle merci al punto di arrivo.

2) Lettera di credito Semplice: qui interviene, a differenza del CAD, un impegno irrevocabile da parte di una banca di pagare al beneficiario entro la scadenza una presentazione conforme di documenti. Questo tipo di obbligazione assunta dalla banca è certa, autonoma e definitiva ed una volta effettuato il pagamento, dati i documenti conformi, la banca si rifarà sul compratore. Tale strumento elimina il rischio di insolvenza da parte del debitore ma non elimina il c.d. "rischio paese".

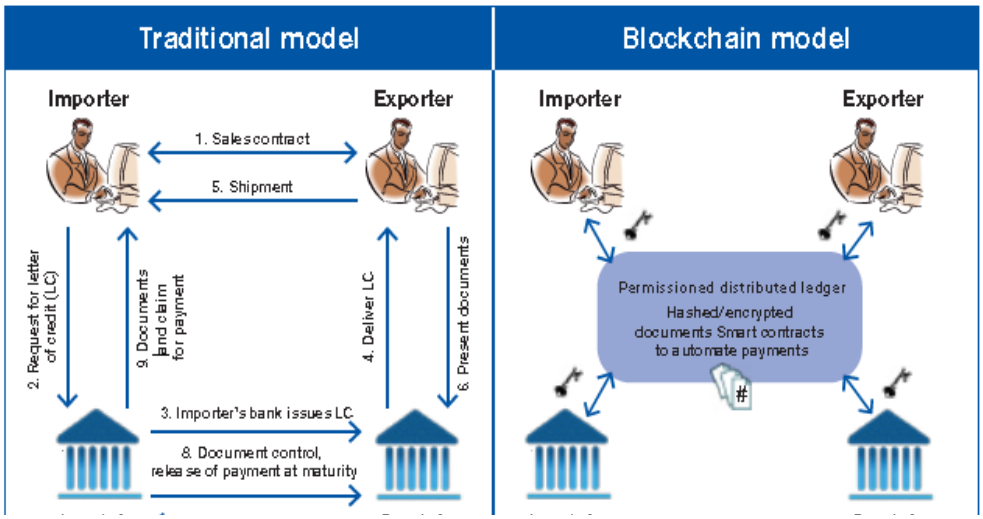
3) Lettera di credito Confermata: essa agisce come la semplice ma a differenza di quest'ultima elimina il rischio paese attraverso l'interposizione di due istituti bancari piuttosto che uno. Il meccanismo è arricchito di una banca c.d. confermante (spesso del paese di origine del venditore) che effettua lo stesso meccanismo dell'istituto bancario all'interno dell'istituto della lettera di credito semplice (pagamento a fronte dei documenti conformi). Una volta effettuato ciò vi è un ulteriore passaggio, identico nella struttura, con la banca emittente, che a sua volta, quindi, pagherà a fronte di una presentazione conforme di documenti da parte della banca confermante. Con tale processo si procede ad eliminare il rischio paese; ovvero tutta quella serie di fattispecie che possono minare l'intero tessuto economico di un paese e che quindi possono portare a crisi economiche o di liquidità per le entità economiche che vi operano all'interno.

4) Open Account: Forma opposta di tutela dei rischi, il conto aperto è stato adottato in maggior quota negli ultimi anni rispetto alle classiche lettere di credito; l'utilizzo maggiore è sicuramente dato dalla maggior competitività, in termini di attrazione di clienti, dello strumento. Esso è definibile come un'operazione dove, in assenza di soggetti che forniscono servizi finanziari, l'esportatore spedisce le merci insieme ai documenti all'importatore prima che esso effettui il pagamento (in genere diventerà esigibile a 30/60/90 giorni). Notiamo dunque come tale meccanismo sia molto a favore dell'importatore aumentando quelli che sono i rischi in capo all'esportatore in termini di insolvenza.

Come può quindi la *Blockchain* migliorare sia in termini di efficienza che in termini di mitigazione del rischio la gestione degli strumenti attualmente in uso?

Uno dei primi esperimenti, circa l'utilizzo dei DLT, è stato effettuato in concomitanza dalla *Bank of America* e dalle *Development Autority of Singapore* implementando un'applicazione atta a migliorare il processo delle lettere di credito attraverso una rete *Blockchain Permissioned*.

Tale applicazione in sostanza utilizza gli stessi meccanismi approvativi della lettera di credito "tradizionale" migliorandone però la velocità attraverso l'automazione (Figura qui sotto)[3], passando da un procedimento che richiede decine di giorni, allo stato attuale, a pochi giorni o addirittura ore.



Traditional Vs Blockchain model

Oltre alle Lettere di Credito, l'applicazione può essere estesa anche per gli strumenti di *Open Account* che, come detto in precedenza, hanno una preponderanza nell'applicazione internazionale.

Data la maggiore rischiosità di tale strumento in capo all'esportatore vediamo come essi possono essere migliorati con l'utilizzo della *Blockchain*.

Una grande scommessa in merito è stata la creazione della *Digital Trade Chain Consortium* rinominata *We.Trade*. che ad oggi conta 16 banche nel proprio organico all'interno di 15 paesi[4].

[3] Emanuele Ganne, World Trade Organization, 2018, "Can Blockchain Revolutionize international trade?"

[4] https://we-trade.com/

L'azione di tale organizzazione è stata quella di creare una *Hyperledger Fabric*[5] contenenti i registri dei soggetti economici operanti e clienti delle banche di riferimento. In tale *ledger* sono memorizzati i dati dei singoli operatori così da poter dare più trasparenza in termini di affidabilità di eventuali controparti inserite nel registro e creare un sistema efficiente di creazione ed esecuzione di *Smart contracts*[6] con termini di contratto e utilizzo di *Open Account* o *Bank Payment Undertaking* (BPU – Garanzia Bancaria).

"These initiatives open particularly interesting opportunities for micro, small and medium-sized enterprises (MSMEs), which often struggle to obtain trade financing because of lack of sufficient collateral or poor or non-existent credit history. By giving financiers greater visibility into the supply chain cash flow and the credit history of companies, Blockchain can facilitate KYC processes and ease MSMEs' access to affordable finance"[7]

Le potenzialità di implementazione della *Blockchain* in ambito transfrontaliero sono quindi molteplici e relativi, oltre al rischio, anche al rilascio e presentazione di tutta una serie di certificazioni e autorizzazioni direttamente collegati alla categoria merceologica di riferimento.

Oltre ai punti di forza però vi sono delle debolezze non trascurabili; prendendo ad esempio la BPO[8] (Garanzia bancaria online) essa non ha preso piede nonostante le grandi potenzialità; lo stesso potrebbe verificarsi con la *Blockchain* nonostante essa sia fortemente ancorata a molti più ambiti e settori operativi.

Altra incertezza è legata alla regolamentazione internazionale relativamente all'utilizzo della *Blockchain* in ambito di commercio internazionale.

[5] https://www.zerounoweb.it/software/blockchain/hyperledger-fabric-blockchain/

[6] Analisi di tutte le componenti ed i principali utilizzi dello Smart contract verranno analizzati al capitolo successivo; detto ciò, è utile capire dove essi possono essere inseriti, così da avere un quadro più chiaro alla fine del percorso.

[7] Asian Development Bank (ADB) (2017), 2017 Trade Finance Gaps, Growth, and Jobs Survey, ADB Brief\ N. 83, September 2017. Retrieved from https://www.adb.org/sites/default/files/publication/359631/adb-briefs-83.pdf on 20 January 2018.

[8] La BPO si propone l'ambizioso obiettivo di supportare e di migliorare gli strumenti di trade finance, attraverso il passaggio da presentazioni cartacee dei documenti, con la relativa discrezionalità dall'analisi degli stessi, a presentazioni elettroniche con il controllo automatico dei dati. (www.mglobale.it)

Come per quanto riguarda le sopra menzionate lettere di credito, le organizzazioni internazionali dovrebbero fornire un quadro normativo chiaro da parte dell'ICC [UCP 600] che identifichi responsabilità specifiche ad ogni passaggio di utilizzo; elemento molto difficoltoso data la struttura decentralizzata del sistema *Blockchain*.

Ultimo punto di difficoltà è legato all'interoperabilità della piattaforma; per essere funzionale in modo ottimale il sistema dovrebbe essere adottato da tutti gli istituti bancari che fungono da intermediari nel commercio transfrontaliero.

Ad oggi esistono enti (come la *We.Trade*) che adottano tale sistema ma l'interoperabilità è limitata alle sole banche associate; nel corso del tempo si auspica quindi una regolamentazione che coadiuvi il focus su tale tecnologia con standard chiari e precisi che ne incentivino l'utilizzo.

Proposte significative, successive al documento su cui si basano le affermazioni precedenti, sono provenienti dalla *International Chamber of Commerce* – ICC - in merito all'armonizzazione della tecnologia *Blockchain*; in particolare due sono le iniziative di maggior rilevo a tal proposito:

TradeTrust[9]*:* un'iniziativa pubblico-privata tra il governo di Singapore, leader mondiali del settore e altri governi, per favorire l'adozione delle tecnologie basate su *Blockchain* nell'ambito del commercio internazionale.

L'iniziativa è finalizzata alla creazione di una piattaforma dotata di interoperabilità tra diverse piattaforme commerciali, per lo scambio di documenti, il tutto basato su una *Blockchain* pubblica (*Permissionless*) che permette di analizzare i flussi commerciali, fornire istruzioni ai partner e visualizzare le principali azioni commerciali in tempo reale, il tutto legato ad una forte riduzione dei costi (monetari e temporali) con una netta diminuzione di errori umani e frodi.

"*Digital platforms will lower existing barriers to international trade in the coming years and enable many more businesses to participate in the new global economy. In line with ICC's 21st century purpose, we are committed to enabling the broadest possible adoption of these digital technologies and support the development and recognition of universally accepted best practice standards for digitalisation, based on global consensus and the work being done by our partners today*,"

John W.H. Denton AO, ICC Secretary General.

[9] iccwbo.org/media-wall/news-speeches/icc-joins-singapore-government-and-major-

1) *Digital Trade Standards Iniziative (DSI)*[10]: iniziativa della Commissione Bancaria dell'ICC con l'obiettivo principale di stabilire standard per chiarire il quadro di riferimento in merito alla *Blockchain* e rendere compatibili le piattaforme esistenti con quest'ultima.

Per raggiungere il risultato l'ICC ha promosso diversi sotto-obiettivi come:

a) la revisione e la modifica degli standard per cui le banche possano accettare o meno documenti e dati elettronici (eUCP 2.0 & eURC 1.0[11]);

b) fissazione di obblighi riguardanti i dati elettronici al fine dell'elaborazione delle transazioni nel commercio digitale;

c) redazione di linee guida circa il come automatizzare il controllo dei documenti, come il credito documentale, utilizzando le nuove tecnologie esistenti;

d) creazione di una *Roadmap* per seguire, in ambito industriale, governativo e dell'ICC stessa, le necessità e le eventuali modifiche da adottare con l'obiettivo di conseguire l'obiettivo principale.

Gli obiettivi riferiti ad ogni attore coinvolto sono a loro volta suddivisi in diversi *steps* identificati all'interno della *Roadmap* di riferimento; in particolare, la stessa auspica il raggiungimento da parte degli enti governativi di 9 *steps* raggiungibili attraverso una serie di riforme strutturali atte al potenziamento della infrastruttura digitale e legale alla base della tecnologia.

1.8) eIDAS e *Blockchain*

In merito alla **forma** i principi, internazionalmente validi convergono nello stabilire che la forma sia libera sempre che non sia regolamentata diversamente nelle normative specifiche dei singoli Ordinamenti.

In quest'ultimo caso, quando il documento dev'essere redatto in forma scritta in che modo la firma digitale può essere ritenuta valida?

LA FIRMA DIGITALE è regolamentata all'interno del Codice dell'Amministrazione Digitale[12], al capo II, facendo riferimento alla **Regolamento eIDAS** (Reg. UE 910/2014) che enuncia all'art.

[10] https://iccwbo.org/global-issues-trends/banking-finance/icc-digitalisation-of-trade-finance/

[11] https://iccwbo.org/media-wall/news-speeches/icc-banking-commission-releases-new-erules-use-electronic-documents/

21 comma 2 che: "*Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha altresì l'efficacia prevista dall'articolo 2702 del Codice civile.*

L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico."

Notiamo quindi come **la firma digitale** possa assumere diverse tipologie e come debba avere un collegamento univoco al titolare così come stabilito dall'art. 24 del precitato codice che sancisce come con essa "*si identifichi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata […] ed essa integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente*".

Data tale definizione, **il Regolamento 910/2014 ai punti 10, 11, 12 identifica tre tipologie di firma elettronica** ma di cui una soltanto ha il c.d. "effetto equivalente della firma autografa", ed abbiamo:

1. Firma elettronica Semplice: definita come i "Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"

2. Firma elettronica Avanzata: "servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate". Tale firma, seppur presentando un livello di sicurezza inferiore rispetto alla qualificata, analizzata al prossimo punto, permette la conclusione di almeno tutti i contratti specificatamente elencati all'art. 1350 comma 3 del Codice civile[13].

[12] https://www.altalex.com/documents/news/2014/10/29/codice-dell-amministrazione-digitale-capo-ii#capo2

[13] Sinteticamente i Contratti per: 1) trasferimento proprietà immobili 2) modificano/trasferiscono diritti di usufrutto, superficie ed enfiteusi 3) servitù prediali 5) contratti di locazione per durata > 9 anni 6) contratti di società/associazione con conferimento di godimento di immobili o altri diritte reali immobiliari > 9 anni 7) Atti che costituiscono rendite

3. Firma elettronica Qualificata: "firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche". Il certificato è rilasciato da soggetti preposti se la firma soddisfa i requisiti dell'art. 29 del II allegato del Regolamento, ed esso è atto a ricollegare in modo univoco la firma digitale al nome (o allo pseudonimo) di un soggetto. La firma qualificata quindi risulta la più sicura fra le precedenti, ma l'azione di certificazione fa sorgere la problematicità legata al tempo. In particolare, una firma elettronica qualificata presenta la medesima valenza in termini giuridici di una firma autografa ma, al contrario di quest'ultima, per essere valida ha bisogno di una "qualificazione" che può essere concessa, ma anche revocata o sospesa. In queste fattispecie le Linee Guida Agid[14] specificano come "essa sia prodotta in un momento in cui il certificato era ancora valido".

Da ciò quindi ne deduciamo come la definizione di uno specifico momento nel tempo può facilmente chiarire l'idoneità della firma; processo non difficile all'interno dell'ecosistema dell'informazione digitale (usando, per esempio, la posta certificata – PEC – possibile però solo con operazioni Italia su Italia e non Italia su Estero).

Fra le tre tipologie di firme sopra riportate, solo la "qualificata" presenta la stessa validità giuridica della firma autografa, mentre per le altre, oltre per i casi stabiliti per legge, la validità passa sotto il vaglio del giudice che ne stabilisce la validità in base al caso di specie.

Anche in ambito ***Blockchain***, dato che le transizioni sono firmate con le loro chiavi private, il certificato di validità della chiave qualificata passa attraverso il rispetto dei requisiti per i certificati qualificati di firma elettronica contenuti nell'allegato I del Regolamento, ma questo riguarda un numero limitato di utenti utilizzatori, spesso imprese.

L'utilizzo delle chiavi private nella *Blockchain*, senza certificazione, può essere equiparato quindi almeno alla firma elettronica semplice.

perpetue/vitalizie 8) atti per la divisione di beni immobili o diritti reali sugli stessi 9) transizioni con oggetto del contratto controversie relativi a rapporti giuridici

[14] AGID [Agenzia per l'Italia Digitale] Guida alla firma digitale, pagina 16, https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/guida_alla_firma_digitale_2009_a_0_0_0.pdf

Per considerare una chiave privata una **"firma di tipo avanzato"** si devono rispettare quattro requisiti identificati dall'ex art. 26 del Regolamento[15], ovvero:

- Connessione univoca al firmatario: con l'utilizzo della tecnologia PKI[16], processo di crittografia asimmetrica con chiave pubblica e privata, si considera tale requisito soddisfatto.
- Consente l'identificazione del firmatario: a) nelle *Blockchain Permissionless* non è consigliabile fornire la propria chiave a soggetti terzi e rendersi identificabili; b) possibilità non da escludere nelle *Permissioned* in cui sono applicabili controlli e assegnazione di specifici ruoli, che, come vedremo successivamente riescono ad attribuire specifiche responsabilità ai soggetti operanti nella *Blockchain*.
- Struttura che permette l'esclusivo controllo del firmatario: oltre alla tecnologia di crittografia asimmetrica diverse piattaforme utilizzano la *One Time Password* ovvero serie di caratteri temporanei, spesso collegati a dispositivi fisici (per esempio cellulare e sms), che permettono l'aumento della sicurezza nell'applicazione della firma. Questo processo può poi essere rafforzato attraverso la combinazione con la c.d. Biometria, processo in base al quale l'autorizzazione e l'esecuzione della firma è condizionata a caratteristiche biofisiche del soggetto, come l'impronta digitale o il riconoscimento vocale. Tali tecnologie sono spesso anche collegate con i *wallet* digitali delle *Blockchain*, come per esempio per la piattaforma Binance[17].
- Collegamento a dati per l'identificazione di successive modifiche: quando parliamo di ***Blockchain***, date le caratteristiche fondanti descritte in precedenza, una delle peculiarità della stessa è **l'immutabilità** dei registri distribuiti. Essa, che agisce con crittografia e con replica del registro in tutti i nodi della rete (appunto, registro distribuito), permette l'identificazione di tutti i cambiamenti del tempo poiché ogni nodo richiama **l'*hash***[18] del blocco precedente, dando informazione di tutte le modifiche intercorse all'interno della *Blockchain* e dunque anche agli utenti che svolgono le operazioni al proprio interno.

[15] Regolamento eIDAS (UE) n. 910/2014

[16] Criterio di crittografia asimmetrica con due chiavi, una pubblica ed una privata che consente di identificare, attraverso la crittografia asimmetrica, la verifica dell'integrità del messaggio ricevuto.

[17] https://www.binance.com/it

[18] Funzione matematica capace di produrre una stringa (sequenza di caratteri) di lunghezza fissa partendo da qualunque file o testo. Ogni minima modifica del file o del testo produrrà una diversa stringa in uscita. La caratteristica fondamentale di queste funzioni è la loro difficile invertibilità: in questo modo, dato un valore di *hash*, è molto difficile risalire al messaggio che l'ha generato; è inoltre molto difficile produrre un messaggio che fornisca una stringa predeterminata.

Date quindi le peculiarità ed i requisiti, nonché le basi su cui definire la tipologia di firma, l'Ordinamento Italiano, facendo riferimento al **Codice dell'Amministrazione Digitale (CAD) all'art. 71**, riconosce che sia la firma avanzata sia la qualificata (peculiarità del nostro ordinamento) sono valide ai fini della redazione del documento.

In tempi più recenti, il c.d. Decreto Semplificazioni del 2019 stabilisce, all'art. 8 ter comma 2, come gli *Smart Contracts* rispettino i requisiti della forma scritta quando vi è l'identificazione informatica delle parti coinvolte nel rapporto, senza però specificare in che modo vi sia una chiara identificazione dei requisiti idonei al riconoscimento. Si ipotizza quindi, secondo l'art. 20 del CAD, come esso sia lasciato al vaglio dei giudici in relazione ai requisiti, precedentemente elencati, descritti per le chiavi avanzate; questione molto variegata e complessa date le differenti caratteristiche delle *Blockchain* utilizzabili, dalle pubbliche alle private, ***permissionless*** e ***permissioned*** (oltre nel presente capitolo).

1.9) Utilizzo della tecnologia *Blockchain* nella governance delle imprese e le implicazioni nei mercati finanziari.

In ambito *Blockchain*, le caratteristiche di "immaterialità", maggiormente presente negli strumenti finanziari, permetterebbero a quest'ultimi di essere meglio collocabili all'interno di tale sfera; in particolare, alla luce delle recenti modalità di intermediazione digitale per alcuni strumenti finanziari (es. **azioni**) si potrebbe facilmente immaginare uno scambio degli stessi attraverso una piattaforma DLT.

L'applicazione della tecnologia porterebbe, date le sue caratteristiche, a migliorare[19] la verifica di proprietà degli strumenti ed ogni trasferimento di proprietà degli stessi all'interno degli operatori economici dando così indicazioni chiare e tempestive in merito alle stesse.

Al paragrafo 2.3 della presente Guida si parlerà del **processo di *Tokenizzazione***, processo effettuabile su particolari beni mobili ed immobili (di cui si può rendere disponibile/indisponibile l'uso).

[19] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart Contract; pagina 527

Prendendo in riferimento il meccanismo appena menzionato, è possibile attuare un collegamento diretto con gli strumenti finanziari tradizionali come azioni ed obbligazioni, includendo le loro possibili varianti.

Tra le possibili operazioni che, attraverso la tecnologia *Blockchain*, potrebbero giovarne in termini di efficienza abbiamo:

- I processi di investimento dei c.d. "investitori consapevoli" che, all'interno del mercato finanziario Europeo, sono soggetti alla normativa MIFID II[20] che è il Regolamento Europeo atto a delineare il profilo di rischio (in base alla sua conoscenza dei rischi dei vari strumenti finanziari) di un soggetto economico intenzionato ad acquisire un determinato portafoglio titoli.

  L'utilizzo della *Blockchain*, con relativi *Smart contracts*, per portare a termine tali operazioni, dunque, dovrebbe presuppore un'altra tipologia di verifica ovvero includere un elemento aggiuntivo rispetto alla conoscenza degli strumenti acquistabili normata dal MIFID, ossia la conoscenza della complessità, in termini stesura/programmazione, dello *Smart contract* finalizzato a tale operazione.

- Il secondo aspetto dei mercati finanziari riguarda l'emissione di tali strumenti all'interno dei mercati primari.

  Il nostro ordinamento prevede modalità specifiche per l'emissione ed il collocamento degli strumenti finanziari ed identifica specifiche peculiarità in termini di processo e di soggetti in grado di acquistare e di introdurre tali strumenti finanziari all'interno del mercato secondario.

  La normativa, dunque, dovrebbe essere aggiornata in modo da prevedere determinate piattaforme *Blockchain* "autorizzate" (di tipo *Private*) con possibilità di controllo in merito alle operazioni effettuate in ingresso e in uscita delle operazioni di raccolta di capitale.

- Ultimo punto di particolare interesse è **il mercato del credito**, mercato primario delle banche commerciali sottoposto a normativa Basilea (I, II, III) e suoi derivati atti a limitare il rischio operativo e di credito di tali istituzioni bancarie.

[20] https://www.consob.it/web/area-pubblica/mifid-2

L'utilizzo della *Blockchain* in tale ambito può essere di notevole vantaggio soprattutto per i processi di sindacazione dei crediti bancari[21] (*il processo di sindacazione bancaria si basa su una approfondita analisi delle condizioni finanziarie ed operative del debitore, favorendo il miglioramento della reputazione e dell'immagine del debitore nel mercato finanziario e industriale*).

Per rispondere alla necessità di proteggere la qualità del credito dall'acuirsi della crisi finanziaria e per rendere più efficaci ed efficienti i processi interni e migliorare i tempi di risposta verso il cliente, Cedacri (leader nel mercato nello sviluppo di soluzioni di outsourcing IT per il settore dei servizi finanziari), ha realizzato un'innovativa piattaforma di Origination Credit che consente alle banche di differenziare il processo di istruttoria sulla base del profilo di rischio/rendimento di ciascuna richiesta in accordo con le politiche creditizie adottate, automatizzando la raccolta delle informazioni e ottimizzando il controllo sulla qualità del credito.

Il processo di istruttoria può contemplare sia elementi "quantitativi" sia elementi "qualitativi" che ciascun cliente può sintetizzare, secondo criteri parametrici, in un indicatore integrato del merito creditizio.

La fase di valutazione del merito creditizio è anche supportata da sistemi automatici di valutazione, che forniscono un'indicazione oggettiva sia sulla rischiosità dei soggetti coinvolti sia sulle perdite attese in caso di default dell'operazione.)

La creazione del **Processo di *Origination*** potrebbe incrementare la propria efficienza automatizzando e caricando nel registro tutti i dati necessari all'erogazione dei crediti.

Al contrario il **Processo di Sindacazione** (creazione di titoli obbligazionari agganciati ad un determinato portafoglio crediti) avrebbe un incremento di efficienza legato a costi ed informazioni, in quanto verrebbe automatizzato attraverso l'utilizzo degli *Smart Contracts* inoltre esso potrebbe essere influenzato dalla diminuzione, in termini probabilistici, di tutta quella serie di errori che potrebbero essere commessi dalla componente umana.

La più grande barriera per tale attuazione parrebbe l'implementazione di un sistema *Blockchain Based* di portata molto ampia.

[21] Bridget Marsh, LSTA Josias Dewey, Holland & Knight LLP; The loan market, blockchain, and Smart contracts: The potential for transformative change; 2021.

Collocandoci in un'ottica di *Governance* di impresa la tecnologia *Blockchain*, secondo la dottrina di riferimento, potrebbe portare ad una migliore efficienza in termini di monitoraggio, ossia **un miglior controllo sul trasferimento della titolarità delle azioni fra soggetti economici.**

Inoltre, attraverso tale tecnologia è possibile l'implementazione di un voto *online*, di tipo certificato, che permetta una gestione più efficiente e celere delle assemblee societarie.

- In merito alla tracciabilità delle azioni, in termini di titolarità delle stesse (assimilate ai titoli di credito e suddivise in "al portatore" o "nominative"[22]), la *Blockchain* potrebbe migliorarne l'efficienza in termini di asimmetria informativa[23] per una pluralità di *shareholders*.

  In particolare, la tracciabilità ed immutabilità del registro consentirebbe di verificare in modo puntuale la distribuzione dei titoli tra i vari soggetti riducendo le probabilità di azioni speculative di soggetti con maggiori informazioni.

  Inoltre, se si adottasse una *Blockchain* di tipo pubblico, si creerebbe un miglioramento notevole della fiducia anche dei potenziali azionisti in quanto soggetti a minore asimmetria informativa[24].
- Per quanto riguarda l'Assemblea dei Soci, essa è disciplinata, in termini di poteri delegati alla stessa, secondo gli articoli 2364, 2364 bis e 2365 del codice civile.

  I poteri dell'Assemblea, in linea di massima riguardano poteri non delegabili al Consiglio d'Amministrazione, come fusioni e decisioni che potrebbero modificare l'assetto societario.

  Tralasciando le tematiche relative ai poteri delegati a tale organo l'interesse di rendere più inclusivo, in termini di votazione, l'ambiente societario è finalizzato a rendere più efficiente il sistema informativo fra gli azionisti ed includere la totalità della compagine azionaria attraverso l'utilizzo di sistemi di votazioni decentralizzati.

  Sistemi di votazione *online* sono già stati implementati in alcune fattispecie attraverso servizi di voto *online* ma con meccanismi centralizzati (affidandosi ad un ente erogatore di

[22] Art. 2354 del Codice civile.

[23] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart Contract; pagina 425

[24] https://www.altalex.com/documents/news/2021/03/18/la-tecnologia-al-servizio-dell-impresa-blockchain-e-iot-creano-valore

tali servizi[25]); l'utilizzo di un sistema decentralizzato però determinerebbe una disintermediazione che eliminerebbe in modo totalitario la discrezionalità della raccolta e comunicazione dei dati che, essendo gestiti da un ente specifico, potrebbero essere soggette a violazioni e/o manomissioni.

Dunque, come si può evincere, l'applicazione di tale tecnologia, oltre ad una riduzione dei costi, migliorerebbe l'inclusività, anche in termini di affidabilità, di tutti i soci; meccanismo attrattivo che potrebbe aumentare il valore della società presa in considerazione.

1.10) Il Regolamento eIDAS (UE) n. 910/2014 in particolare

Il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, per l'Identificazione Elettronica e Servizi Fiduciari per le Transazioni Elettroniche nel Mercato Unico Europeo (abbreviato in **eIDAS**, acronimo di ***electronic IDentification, Authentication*** *and trust* ***Services***) **ha l'obiettivo** di fornire una base normativa a livello comunitario per le **interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni** incrementando la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di *e business* e del commercio elettronico nell'Unione Europea.

L'eIDAS quindi è stato pensato per regolamentare:

1) la firma elettronica (detta anche "firma digitale" o firma "elettronica qualificata"),
2) i trasferimenti di denaro e
3) altri tipi di transazioni elettroniche nel Mercato Unico Europeo.

Ha permesso di creare standard unici per la firma elettronica, certificati digitali, marche temporali, e altre forme di autenticazione elettronica, **consentendo di sostituire documenti cartacei con equivalenti digitali con lo stesso valore legale e aventi riconoscimento ufficiale in tutti i Paesi dell'Unione Europea**.

[25] Esempio: https://xdatanet.com/assemblea/

1.10.a) Le caratteristiche della firma elettronica

1) Garantire l'autenticità del firmatario cioè l'identità della persona o dell'impresa che firma il documento
2) Garantire che il firmatario non possa disconoscere il documento: il cosiddetto "non ripudio"
3) Garantire che i documenti firmati non possano essere modificati dopo la firma
4) Garantire l'integrità del documento
5) Garantire la piena validità del documento sottoscritto
6) Attribuire a tutto ciò pieno valore legale cioè con la firma elettronica un *file* ha lo stesso valore di un documento su cui è stata apposta una firma autografa
7) Tutto questo esclusivamente attuato tramite l'utilizzo di *software*

1.10.b) Caratteristiche dell'utilizzazione della firma digitale

La firma digitale può essere utilizzata:

a) Sia per documenti della Pubblica Amministrazione

b) Sia per sottoscrivere documenti tra privati come ad esempio contratti, fatture, bilanci ecc…

I Paesi membri dell'UE sono tenuti a riconoscere le firme elettroniche che rispettano gli standard fissati dall'eIDAS.

La firma digitale viene rilasciata da "prestatori di servizi fiduciari qualificati" (in Italia tali "prestatori" – ad esempio Aruba - sono autorizzati dall'Agenzia per l'Italia digitale – AgId).

È possibile anche ottenere una **firma digitale remota** (per esempio come quella utilizzata per la verbalizzazione degli esami all'Università di Bologna) cioè una firma digitale generata usando strumenti di autenticazione – in genere uno *user id*, una *password* ed una *one time password* – che consentono la generazione della propria firma su un dispositivo custodito da remoto del proprio certificatore

1) Se la *Blockchain* è aperta – *permissionless* – (per esempio *Bitcoin* ed *Ethereum*) **non richiede la previa identificazione degli utenti** e consente ai medesimi di partecipare al

sistema in maniera anonima o pseudonomizzata creando una **coppia di chiavi crittografiche** che i medesimi utenti utilizzeranno per sottoscrivere le "transazioni" o per esserne i destinatari.

Le evidenze informatiche delle "transazioni" registrate sulla *Blockchain* rientrano nell'ambito della definizione del **Regolamento (UE) n. 910/2014 – eIDAS – di documento elettronico** essendo un "*contenuto conservato in forma elettronica*" nonché in quella di "*documento informatico*" contenuta nel **Codice dell'Amministrazione Digitale** (**CAD – D.Lgs 7 marzo 2005 n. 82 e successive modifiche, da ultimo con il D.Lgs n. 217/2017**) che a livello probatorio afferma, **ex art 20,** che il "*documento informatico*" è idoneo a soddisfare il requisito della forma scritta ed assume **valenza ex art 2702 c.c.** – **scrittura privata** – nel caso il suo autore sia previamente identificato ed il processo garantisca l'integrità e l'immodificabilità del documento creato nonché riesca ad attribuire in maniera manifesta ed inequivoca la paternità del documento stesso al suo autore.

Il potere di stabilire i requisiti affinché un **processo di identificazione informatica** possa dar luogo alla creazione di firme elettroniche con valore pari a quello già oggi conosciuto nell'Ordinamento Italiano è attribuita **all'AgID – Agenzia per l'Italia Digitale**.

Il **punto debole** di una ***Blockchain permissionless*** - aperta, **da un punto di vista probatorio**, è che la procedura **non** permette la certa identificazione del soggetto che agisce in quanto egli può agire anche in maniera anonima o con uno pseudonimo.

In particolare è certo e corretto il meccanismo da un punto di vista oggettivo, ma non si è perfettamente sicuri dell'identità dell'agente.

Le transazioni registrate sulla *Blockchain* **non** potranno essere dotate della validità e rilevanza probatoria che l'Ordinamento giuridico Italiano ed Europeo riconosce ai documenti informatici sottoscritti con tali strumenti ex **Regolamento (UE) n. 910/2014 – eIDAS.**

Sarà comunque **il giudice** che potrà decidere l'ammissibilità o meno della prova se tecnicamente riuscirà ad individuare chiaramente il soggetto od i soggetti interessati alla transazione (informaticamente e proprio per le caratteristiche della *Blockchain* ciò è possibile).

2) Se la ***Blockchain*** è ***permissioned*** cioè **chiusa** quindi si caratterizza per **consentire l'accesso** alla *chain* **solamente a soggetti già identificati** in quanto il meccanismo *Blockchain* in questa ipotesi non è solo esclusivamente basato su una fiducia tecnologico/informatica astratta e automatica, ma sul **controllo** che svolgono i partecipanti alla *Blockchain* consente di superare in maniera più agevole il problema dell'identificazione dei titolari delle chiavi crittografiche ed anche della possibilità di creare un sistema di firma elettronica avanzata con cui sottoscrivere le "transazioni" registrate sulla *Blockchain*.

In questa ipotesi nulla vieta che uno dei partecipanti (*per esempio un **Master Node** che è un server che si occupa di svolgere un lavoro utile a facilitare le "transazioni".*

In particolare, ogni MasterNode:

1. *ospita una copia dell'intera Blockchain*
2. *facilita lo scambio di messaggi sulla rete*
3. *valida le transazioni*
4. *vota per l'accettazione o il rifiuto delle proposte di miglioramento dell'ecosistema*
5. *vota i progetti da finanziare*
6. *permette di effettuare transazioni immediate - funzionalità chiama Instant Send - bypassando i lunghi tempi di attesa necessari per la validazione da parte dei miners.*

Il consenso viene infatti raggiunto fra i vari MasterNode, che poi garantiscono la transazione e la riportano sulla Blockchain, estromettendo i più lenti miners dal processo

*7. permette di effettuare transazioni anonime (Private Send), ovvero movimentazioni nelle quali non è possibile risalire all'indirizzo del mittente e/o a qu*ello del destinatario)

si ponga come soggetto erogatore della soluzione di **firma elettronica avanzata** ex *art. 55 Dpcm 22 febbraio 2013* (*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71)* attestando l'identità dei titolari delle chiavi crittografiche che tecnologicamente sono identiche alle soluzioni utilizzate per la firma digitale senza però essere associate a certificati qualificati utilizzate dai soggetti partecipanti alla *chain* per la sottoscrizione delle transazioni.

Art. 55. Disposizioni generali – DPCM 22/02/2013

1. La realizzazione di soluzioni di ***firma elettronica avanzata*** *è libera e non è soggetta ad alcuna autorizzazione preventiva.*

2. I ***soggetti che erogano o realizzano soluzioni di firma elettronica avanzata si distinguono in****:*

a) coloro che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti di cui alla lettera b);

b) coloro che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore dei soggetti di cui alla lettera a).

Inoltre **il Codice dell'Amministrazione Digitale** ha introdotto degli elementi che sono riscontrabili nel meccanismo *Blockchain*: in quanto afferma che "*il documento elettronico sia formato previa* ***identificazione informatica del suo autore****, attraverso un processo avente i requisiti fissati dall'AgID ex art. 71 CAD con modalità tali da garantire la sicurezza, integrità, ed immodificabilità del documento e, in maniera manifesta ed inequivoca, la sua riconducibilità all'autore.*"

La *Blockchain* tutto ciò lo può garantire (marche temporali, algoritmi di *hash*, sistemi di crittografia asimmetrica, ecc..) e quindi con una "firma elettronica avanzata" e le evidenze informatiche ex art. 20 del Codice dell'Amministrazione Digitale si rientrerebbe nella valenza probatoria ex art. 2702 c.c. – scrittura privata - e sarebbe quindi idonee a soddisfare il requisito della forma scritta.

Infatti, nel momento in cui un soggetto partecipa ad una *Blockchain* gli viene associata una coppia di chiavi asimmetriche e quindi una firma elettronica con cui questo soggetto sottoscrive **con la propria chiave privata** le "transazioni" che intende effettuare (o meglio *l'hash* della "transazione" così come avviene quando si sottoscrive un documento informatico con firma qualificata) e **può diventare destinatario di altre "transazioni" (il cui *hash* è sottoscritto con la sua chiave pubblica**).

Quindi **la firma digitale viene generata** tramite una coppia di chiavi digitali asimmetriche o a chiave pubblica attribuite ad un soggetto:

1) Una è la **chiave privata** che serve a generare la firma ed è conosciuta solo dal titolare

2) L'altra è la **chiave pubblica** che *serve a verificare l'autenticità della firma*.
   La chiave pubblica non serve a ricostruire la chiave privata.

La chiave pubblica è collegata alla chiave privata, perché generata dallo stesso algoritmo Diffie-Hellman, ma da una non si può ricavare l'altra.

In seguito vengono formati dei blocchi di "transazioni", di queste viene creato *l'hash* cioè la "stringa uniforme in linguaggio matematico" ed apposta una marca temporale creata con *l'hash*.

Ciascun blocco è quindi collegato ai blocchi successivi sempre sfruttando la catena di *hash* cioè delle "stringhe" create con linguaggio informatico/matematico.

Il sistema si basa sui medesimi processi che sono previsti per la sottoscrizione con firme elettroniche qualificate dei documenti informatici e della conservazione digitale dei documenti.

L'unico elemento assente in una *Blockchain* è il certificato elettronico che ricollega una firma elettronica al soggetto a cui è stata rilasciata previa identificazione.

Nel momento in cui ad una *Blockchain* è collegata una identificazione e autenticazione informatica sicura di un soggetto per accedere al sistema, ossia se una coppia di chiavi sulla *Blockchain* viene **associata univocamente ad un soggetto** identificato informaticamente tramite sistemi di identificazione ed autenticazione informatica come ad esempio SPID – Sistema Pubblico di Identità Digitale, **la *Blockchain* è idonea a garantire**:

1. la sicurezza, integrità ed immodificabilità del documento;

2. la sua riconducibilità all'autore in maniera manifesta ed inequivoca potendo per esempio utilizzare un PIN (*Personal Identification Number*).

In conclusione, l'introduzione di un modello di firma elettronica che viene attuato tramite un processo in cui a monte vi è l'identificazione sicura, tramite SPID - Sistema Pubblico di Identità Digitale - o altri sistemi di identificazione, trova piena applicazione con l'uso di una tecnologia *Blockchain*.

Come detto tali *Blockchain* potrebbero essere chiuse o semichiuse, garantendo l'accesso unicamente a quei soggetti in possesso dello strumento di identificazione richiesto dalla *chain*.

Ancora sul Regolamento (UE) n. 910/2014 – eIDAS

Considerando 2

Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

Considerando 9

In molti casi i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro Stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri.

Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno.

Disporre di mezzi di identificazione elettronica ***riconosciuti reciprocamente*** *permetterà di agevolare la fornitura transfrontaliera di numerosi servizi nel mercato interno e consentirà alle imprese di operare su base transfrontaliera evitando molti ostacoli nelle interazioni con le autorità pubbliche.*

Considerando 12

Un obiettivo del presente regolamento ***è l'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici.***

Il presente regolamento non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri.

Lo scopo del presente regolamento è garantire che per accedere ai servizi online transfrontalieri offerti dagli Stati membri si possa disporre di un'identificazione e un'autenticazione elettronica sicura.

Considerando 16

I livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata. Il livello di garanzia dipende dal ***grado di sicurezza fornito dai mezzi di identificazione elettronica riguardo all'identità pretesa o dichiarata di una persona*** *tenendo conto dei procedimenti (ad esempio, controllo e verifica dell'identità, e autenticazione), delle attività di gestione (ad esempio, l'entità che rilascia i mezzi di identificazione elettronica e la procedura di rilascio di tali mezzi) e dei controlli tecnici messi in atto.*

Come risultato dei progetti pilota su larga scala finanziati dall'Unione, della normazione e di attività a livello internazionale, esistono varie definizioni e descrizioni tecniche dei livelli di garanzia.

In particolare, il progetto pilota su larga scala STORK e la norma ISO 29115 fanno riferimento, tra l'altro, ai livelli 2, 3 e 4, che dovrebbero essere tenuti nella massima considerazione all'atto di stabilire le norme, le procedure e i requisiti tecnici minimi per i livelli di garanzia basso, significativo ed elevato ai sensi del presente regolamento, assicurando al contempo l'applicazione coerente del presente regolamento in particolare per quanto riguarda il livello di garanzia elevato in relazione al controllo dell'identità ai fini del rilascio di certificati qualificati.

I requisiti stabiliti dovrebbero essere neutrali dal punto di vista tecnologico.

Dovrebbe essere possibile soddisfare i requisiti di sicurezza necessari attraverso tecnologie differenti.

Considerando 17

È opportuno che gli Stati membri incoraggino il settore privato a impiegare volontariamente mezzi di identificazione elettronica ***nell'ambito di un regime notificato a fini di identificazione ove necessario per servizi online o transazioni elettroniche.***

La facoltà di ricorrere a tali mezzi di identificazione elettronica consentirebbe al settore privato di avvalersi dell'identificazione e autenticazione elettroniche già ampiamente impiegate in molti Stati membri almeno per i servizi pubblici e di agevolare alle imprese e ai cittadini l'accesso transfrontaliero ai loro servizi online. Per facilitare l'impiego transfrontaliero di tali mezzi di identificazione elettronica da parte del settore privato, è opportuno che la possibilità di

autenticazione offerta da uno Stato membro sia disponibile alle parti del settore privato facenti affidamento sulla certificazione stabilite al di fuori del territorio di detto Stato membro alle stesse condizioni applicate alle parti del settore privato facenti affidamento sulla certificazione stabilite nel suddetto Stato membro.

Di conseguenza, per quanto riguarda le parti del settore privato facenti affidamento sulla certificazione, lo Stato membro notificante può definire termini di accesso ai mezzi di autenticazione.

Detti termini di accesso possono indicare se i mezzi di autenticazione relativi al regime notificato sono attualmente disponibili alle parti del settore privato facenti affidamento sulla certificazione.

Considerando 26

In considerazione del ritmo dei mutamenti tecnologici, occorre che il presente regolamento adotti un approccio aperto all'innovazione.

Considerando 27

È opportuno che il presente regolamento sia neutrale sotto il profilo tecnologico.

È auspicabile che ***gli effetti giuridici prodotti dal presente regolamento*** *siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti.*

Considerando 30

Gli Stati membri dovrebbero designare uno o più organismi di vigilanza per lo svolgimento delle attività di vigilanza previste dal presente regolamento.

Gli Stati membri dovrebbero altresì avere facoltà di decidere, di comune accordo con un altro Stato membro, di designare un organismo di vigilanza nel territorio di tale altro Stato membro.

Considerando 48

Sebbene sia necessario un elevato livello di sicurezza per garantire il riconoscimento reciproco delle firme elettroniche, in casi specifici come nel contesto della decisione 2009/767/CE della Commissione, è opportuno che siano accettate anche firme elettroniche con una ***garanzia di sicurezza più debole.***

Considerando 49

Il presente regolamento dovrebbe stabilire ***il principio secondo il quale*** *alla firma elettronica* ***non dovrebbero essere negati gli effetti giuridici per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata.***

Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal presente regolamento secondo cui ***una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa.***

Considerando 57

Per garantire la ***certezza giuridica della validità della firma,*** *è essenziale specificare i componenti di una firma elettronica qualificata, che dovrebbero essere valutati dalla parte facente affidamento sulla certificazione che effettua la convalida.*

Inoltre, è opportuno che attraverso la specificazione degli obblighi dei ***prestatori di servizi fiduciari qualificati*** *che possono offrire un servizio di convalida qualificata a parti facenti affidamento sulla certificazione che non vogliono o non possono effettuare esse stesse la convalida di firme elettroniche qualificate siano stimolati gli investimenti del settore privato e pubblico in tali servizi.*

È opportuno che entrambi gli elementi rendano la convalida delle firme elettroniche qualificate semplice e agevole per tutte le parti a livello dell'Unione.

Considerando 58

Qualora una transazione richieda un sigillo elettronico qualificato ***di una persona giuridica****, è opportuno che sia accettabile anche la* ***firma elettronica qualificata del rappresentante autorizzato della persona giuridica.***

Considerando 59

È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.

Considerando 61

È opportuno che il presente regolamento ***garantisca la conservazione a lungo termine delle informazioni****, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici.*

Considerando 63

I documenti elettronici sono importanti per l'evoluzione futura delle ***transazioni elettroniche transfrontaliere nel mercato interno.***

Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.

CAPO I

DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

Allo scopo di garantire il buon funzionamento del mercato interno *perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:*

a) fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro,

b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e

c) ***istituisce un quadro giuridico per*** *le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.*

Articolo 2 - Ambito di applicazione

1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.

2. Il presente regolamento ***non si applica*** *alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.*

3. Il presente regolamento ***non pregiudica*** *il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.*

Articolo 3 – Definizioni

Ai fini del presente regolamento si intende per:

1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica;

2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online;

3) «dati di identificazione personale», un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica;

4) «regime di identificazione elettronica», un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche;

5) «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica;

6) «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento su un'identificazione elettronica o su un servizio fiduciario;

7) «organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;

8) «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio;

9) «firmatario», una persona fisica che crea una firma elettronica;

*10) «**firma elettronica**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;*

*11) «**firma elettronica avanzata**», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;*

*12) «**firma elettronica qualificata**», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;*

13) «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;

14) «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

15) «certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;

16) «servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e ***consistente nei seguenti elementi****:*

a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure

b) creazione, verifica e convalida di certificati di autenticazione di siti web; o

c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;

17) «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

*18) «organismo di valutazione della conformità», **un organismo** ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come **competente** a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati;*

19) «prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;

20) «prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;

21) «prodotto», un hardware o software o i loro componenti pertinenti, destinati a essere utilizzati per la prestazione di servizi fiduciari;

22) «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;

23) «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

*24) «creatore di un sigillo», **una persona giuridica** che crea un sigillo elettronico;*

*25) «**sigillo elettronico**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;*

*26) «**sigillo elettronico avanzato**», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;*

*27) «**sigillo elettronico qualificato**», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;*

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;

30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

33) «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

*36) «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e **fornisce prove relative al trattamento dei dati trasmessi**, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;*

37) «servizio elettronico di recapito qualificato certificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;

38) «certificato di autenticazione di sito web», un attestato che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;

39) «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

41) «convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico.

SEZIONE 4 - Firme elettroniche

Articolo 25 - Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.

2. ***Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.***

3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale ***firma elettronica qualificata in tutti gli altri Stati membri.***

Articolo 26 - Requisiti di una firma elettronica avanzata

Una ***firma elettronica avanzata*** *soddisfa i seguenti requisiti:*

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Articolo 36 - Requisiti dei sigilli elettronici avanzati

Un ***sigillo elettronico avanzato*** *soddisfa i seguenti requisiti:*

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

SEZIONE 6 - Validazione temporale elettronica

Articolo 41 - Effetti giuridici della validazione temporale elettronica

1. Alla validazione temporanea elettronica ***non*** *possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.*

2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.

3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Articolo 42 - Requisiti per la validazione temporale elettronica qualificata

1. Una validazione temporale elettronica qualificata soddisfa ***i requisiti seguenti****:*

a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;

b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e

c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 44 - Requisiti per i servizi elettronici di recapito certificato qualificati

1. *I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:*

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;

b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;

f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

2. *La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai processi di invio e ricezione dei dati. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.*

SEZIONE 8 - Autenticazione dei siti web

Articolo 45 - Requisiti per i certificati qualificati di autenticazione di siti web

1. I certificati qualificati di autenticazione di siti web soddisfano i requisiti di cui all'allegato IV.

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai certificati qualificati di autenticazione di siti web. Si presume che i requisiti di cui all'allegato IV siano stati rispettati ove un certificato qualificato di autenticazione di sito web risponda a tali norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

CAPO IV - DOCUMENTI ELETTRONICI

Articolo 46 - Effetti giuridici dei documenti elettronici

*A un documento elettronico **non** sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.*

1.11) Identità Auto Sovrana e Progetto eIDAS *Bridge*

Blockchain e identità digitale: dove sta andando l'Unione Europea e l'Italia

Nella consultazione avviata nel 2020 dal MI.S.E. sulla strategia nazionale *Blockchain* viene affrontato il tema dell'**Identità Digitale** e dell'utilizzo dell'Identità Auto Sovrana (*Self Sovereign Identity* – SSI) e la compatibilità tra Identità Auto Sovrana - *Self Sovereign Identity* – SSI - e **Regolamento Europeo 910/2014 eIDAS.**

Inoltre, il Ministero dello Sviluppo Economico ha avviato la consultazione sulla Strategia nazionale per *Blockchain* e registri distribuiti.
L'Identità Auto Sovrana (*Self Sovereign Identity* - SSI) è il **passo successivo oltre l'Identità incentrata sull'utente.**

Entrambi i concetti si basano sull'idea che **un utente deve essere centrale per il controllo e l'amministrazione della sua Identità Digitale**, il che richiede non solo la capacità dell'utente di utilizzare un'Identità in più posizioni, ma anche un vero controllo su tale Identità Digitale, **creando l'autonomia dell'utente.**

Per ottenere ciò, un'Identità Auto Sovrana deve essere trasportabile e non può essere collegata a una singola autorità centrale.

Un'Identità Auto Sovrana deve anche consentire agli utenti di fornire affermazioni su sé stessi, che potrebbero includere dati o attributi personali e possono persino contenere informazioni affermate da altri.

Da una prospettiva tecnologica, questo può essere ottenuto utilizzando registri / *Blockchain* distribuiti in quanto consentono l'uso di Identificatori Decentralizzati (*Decentralizer IDentifier* - ***DID***), che sono alla base di questo modello di identità.

I *DID* - *Decentralizer IDentifier* - sono solo Identificatori, non forniscono alcun tipo di informazione sul loro proprietario.

Questo è ciò che fanno le credenziali verificabili, poiché contengono affermazioni fatte da un emittente in merito al titolare della credenziale, entrambe identificate nella credenziale dai rispettivi Identificatori Decentralizzati - *DID*.

Condividendo le credenziali verificabili, gli utenti possono provare le affermazioni su sé stessi, **ma come può il verificatore delle credenziali fidarsi di loro, se l'unica cosa che sa dell'emittente è il suo Identificatore Decentralizzato - *DID*?**

Questo è infatti l'obiettivo di questo progetto.

Dove ed in che modo il Regolamento eIDAS può aiutare?

Come detto sopra **eIDAS sta per identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.**

Esso garantisce la validità giuridica dei documenti elettronici e dei servizi fiduciari transfrontalieri, come firme e sigilli elettronici.

Per rendere eIDAS disponibile come struttura di fiducia nell'ecosistema Identità Auto Sovrana (*Self Sovereign Identity* – *SSI*), **la Commissione Europea** ha sviluppato nell'ambito di questo progetto, il ponte – *bridge* - **eIDAS.**

Il ponte eIDAS assiste sia l'emittente nel processo di firma di una credenziale verificabile sia il verificatore, nel processo di verifica delle credenziali.

"Attraversando" il ponte eIDAS, una credenziale verificabile si dimostra affidabile.

Nell'ambito dell'azione *Innovative Public Services* del programma ISA2, la Commissione Europea ha **sperimentato** questo **nuovo modello di identità**, che ha il potenziale per migliorare il modo in cui i cittadini gestiscono la loro Identità Digitale, nonché la capacità di offrire alle pubbliche amministrazioni nuove modalità di autenticare i cittadini e offrire servizi pubblici migliori.

È anche un concetto interessante che potrebbe aiutare nell'applicazione del **Principio dell'*eGovernment una tantum***, con un approccio incentrato sul cittadino in contrapposizione al tradizionale approccio incentrato sul governo.

Ciò significa che il cittadino dovrebbe richiedere una sola volta una credenziale ad una pubblica amministrazione - o ad un soggetto terzo di fiducia -, conservarla e condividerla con altri sotto il proprio controllo.

Questo PROGETTO è un'implementazione in una fase iniziale della componente eIDAS Bridge che viene ora sviluppata nel contesto dell'***European Self-Sovereign Identity Framework*** (ESSIF),

uno dei casi d'uso selezionati dalla *European Blockchain Partnership* (EBP) e dalla Commissione Europea che è sviluppato nell'ambito della *European Blockchain Services Infrastructure*, un elemento di costruzione del meccanismo per collegare l'Europa.

Ulteriori informazioni su EBSI ed ESSIF sono disponibili nel sito web **EBSI CEF Digital**.

Le novità sono relative a come la *Self Sovereign Identity* - *SSI* - sia compatibile con il **Regolamento eIDAS** e possa farne parte nell'ambito degli aggiornamenti che il Regolamento avrà nei prossimi anni.

Il tema è nato in ambito comunitario con i lavori dell'Osservatorio e Forum Europeo sulla *Blockchain*.

In un'analisi generale sul tema, anche al fine di stimolare l'utilizzo di tali tecnologie nei servizi pubblici con lo scopo di rendere la burocrazia più semplice ed efficiente, l'Osservatorio sottolinea che per un efficace e benefico utilizzo della ***Blockchain* per la fornitura di servizi al cittadino**, i Governi devono sviluppare sistemi di Identità Digitale che utilizzano piattaforme realizzate in modo tale da creare un **modello decentralizzato** di proprietà, gestione, rappresentazione ed attestazione dell'identità di una persona.

L'Identità Digitale viene indicata come "prerequisito essenziale" e i Governi la devono gestire in modo da garantirne la sicurezza in termini di protezione e soprattutto di univocità.

L'Identità "Governativa" ha i suoi alfa e omega nei certificati di nascita e di morte.

Peraltro i Governi ma anche il mondo privato offrono sempre di più servizi *online* e l'identificazione deve avvenire in modo univoco per poi procedere all'autenticazione al servizio.

Una considerazione molto efficace dell'Osservatorio è sul fatto che la più grande piattaforma virtuale costituita da *Internet* non dispone di un sistema di Identità integrato e quindi proliferano meccanismi di attribuzione dell'Identità che non sempre sono generate con metodi affidabili.

In ogni caso l'Identità è a disposizione del fornitore di servizi, nel commercio elettronico, sui *social network* o sempre di più, per l'informazione a pagamento.

Il titolare **non ha** l'effettivo controllo dei propri dati; subisce la perdita accidentale o malevola che costituisce il ben noto problema del Furto di Identità.

1.12) …… Continua: il ruolo della tecnologia dei registri distribuiti

Considerato il suo ruolo, l'Osservatorio Europeo ha individuato nella *Blockchain* e nella Tecnologia dei Registri Distribuiti - Distributed Ledger Technology - DLT, le basi per gestire il problema mediante la *Self Sovereign Identity* - SSI.

- Le informazioni sulla persona non sono gestite e conservate da terze parti.

- Le persone stesse fanno in modo che tali informazioni siano verificate.

L'Osservatorio Europeo propone l'emissione da parte dei Governi, in favore dei cittadini o di chi ne abbia diritto (per esempio: il titolare di permesso di soggiorno), di **credenziali digitali firmate dall'emettitore istituzionale.**

In questo modo si generano attestazioni sui dati anagrafici (nome, cognome, luogo e data di nascita, indirizzo e luogo di residenza, ecc.), la patente di guida, i titoli di proprietà immobiliare e fondiaria, il certificato elettorale, la capacità di sottoscrivere da remoto, ecc.

Consente l'invio di comunicazioni promozionali inerenti ai prodotti e servizi di soggetti terzi rispetto ali Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contratto automatizzate (*Smart contract*) e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

L'utilizzo è *mutatis mutandis* come quello del mondo reale, traslato nel mondo virtuale con rischio bassissimo di furto o falsificazioni vista la tecnologia di base utilizzata (la *Distributed Ledger Technology* - DLT).

Con tutta la convinzione e la tenacia del caso l'Osservatorio Europeo ha ulteriormente sviluppato il tema con uno specifico report.

È in questo documento che gli esperti riprendono i lavori della *DIF* (*Decentralized Identity Foundation*) e del *WWWC* (*World Wide Web Consortium*).

L'elemento cruciale da considerare è il *DID* (***Decentralized Identifier***) che per il *WWWC* sono un nuovo tipo di identificatore per identità digitali verificabili "Auto Sovrane" ed in particolare:

- I *DID* sono completamente sotto il controllo del soggetto *DID*, indipendentemente da qualsiasi registro distribuito, gestore dell'identità o autorità di certificazione.
- I *DID* sono URL che mettono in relazione un soggetto *DID* a mezzi per interazioni affidabili con quel soggetto.
- I *DID* si sostanziano in documenti *DID* – documenti semplici che descrivono come usare quel *DID* specifico.
- Ogni documento *DID* può contenere almeno tre elementi:
  a) scopi probatori,
  b) metodi di verifica ed
  c) *endpoint* di servizio.

Gli scopi probatori sono combinati con metodi di verifica per fornire meccanismi per provare le cose.
Ad esempio, un documento *DID* può specificare che un particolare metodo di verifica, come una chiave pubblica crittografica o un protocollo biometrico pseudonimizzato, può essere utilizzato per verificare una prova creata ai fini dell'autenticazione.

Gli *endpoint* di servizio consentono interazioni affidabili con il *controller DID*.

La Commissione Europea non ha ignorato i documenti dell'Osservatorio e sono scaturite interessanti discussioni scientifiche sulla relazione tra eIDAS e Self Sovereign Identity - *SSI*.

Nel documento si creano le connessioni organizzative e tecnologiche tra i due mondi.

Nel capitolo 4 di questo documento si descrive come connettere il *DID* con le identità conformi alle regole di eIDAS.

Si prendono in considerazione i meccanismi basati sulla notifica degli schemi di identificazione (in Italia **sono notificati il Sistema Pubblico di Identità Digitale – SPID e la Carta d'Identità Elettronica – CIE**).

Il documento è intitolato: "***SSI eIDAS Legal Report – How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market***".

Il lettore che volesse approfondire questi particolari scenari può leggere della *Sovrin Foundation* (www.sovrin.org) e dell'ecosistema che è stato creato per supportare la *SSI*.
Nell'ambito del *Sovrin Founding Steward Program* (sovrin.org/stewards/ è stata realizzata la piattaforma DIZME (*This Is Me*) che ha lo scopo di aggiungere alla conformità al regolamento eIDAS le tematiche del mondo della *SSI*.

Un altro caso interessante è l'utilizzo della piattaforma *Ethereum* a scopi di supporto della *SSI*.
Si tratta dell'APP uPort attiva da circa tre anni nel Comune svizzero di ZUG.
In questa sede sono state numerose le iniziative pratiche con la più originale di natura turistica.
Tramite il sistema di *SSI* è possibile accedere a un sistema di *bike sharing*.

Il cittadino deve essere supportato per le tematiche di "consapevolezza" connesse all'Identità Auto Sovrana.

Un tema cruciale è quello del controllo dei propri dati proprio perché lo stesso è diretto.

Serve piena consapevolezza sulle cautele da utilizzare e sulle modalità "sicure" di recupero di dispositivi (es. *Smartphone*) o di *password*.

DE IURE CONDENDO: Da regolamentare nei nuovi scenari è il tema dell'azione anonima nell'utilizzo dei servizi di rete.

Tutto ciò poi dovrà essere coordinato con il tema della protezione dei dati personali ai sensi dell'altro **Regolamento Europeo 679/2016 (GDPR)** ed i temi dell'accessibilità e del divario digitale.

2) ICO - *Initial Coin Offering* e Token

2.1) ICO *Initial Coin Offering* storia e finalità

Una ICO in italiano, letteralmente "*Offerta di moneta iniziale*", è un mezzo **non regolamentato** di *crowdfunding* nel settore finanziario che consente ai promotori di un'iniziativa di raccogliere fondi a fronte dell'emissione di una moneta virtuale/*cryptovaluta* o *currency/payment token*.

In particolare, le ***Initial Coin Offering*** - ICO sono delle offerte al pubblico (come le più tradizionali IPO *Initial Public Offering* per il mercato borsistico e regolamentato) in cui l'adesione all'offerta, il regolamento dei flussi finanziari, l'assegnazione del titolo, avviene sulla *Blockchain* in forma diretta e decentralizzata oltre che dematerializzata.

In tal modo i costi ed i modi del procedimento risultano molto più veloci e meno onerosi e si assiste anche ad un superamento delle barriere territoriali **favorendo la raccolta di capitali da parte delle imprese.**

Le prime ICO furono lanciate per raccogliere fondi per nuove *cryptovalute*, ma le attuali ICO vengono usate per qualsiasi scopo.

Generalmente, sono venduti dei *token utility* (si veda il paragrafo 2.6 del presente capitolo) per raccogliere denaro.

A differenza di ciò che avviene nella similare OPA (Offerta Pubblica di Acquisto), l'acquisizione dei *token utility* non è regolamentata e potrebbe non garantire la proprietà o altri diritti.

La prima ICO fu creata nel 2013 per il lancio della *cryptovaluta Mastercoin*.

Nel 2014 la *cryptovaluta Ethereum* raccolse denaro con una ICO.

Dal maggio 2017 vi sono circa 20 offerte al mese e la ICO per un nuovo *browser web* chiamato *Brave* ha generato circa 35 milioni di dollari in 30 secondi.

Vi sono almeno 18 siti *web* che tracciano le ICO.

2.2) ICO come raccolta pubblica di capitale

Il funzionamento consiste nel pubblicare sul sito *internet* dell'emittente un documento denominato *white paper* contenente la **descrizione di un progetto imprenditoriale** chiedendo al mercato di **finanziarne la realizzazione** attraverso l'acquisto *on line* in moneta legale o più spesso in *cryptovaluta*, già esistente soprattutto *ether* e *bitcoin*, di un certo numero di *investment token* **cioè di *token* di investimento** che consistono in prodotti finanziari o titoli di partecipazione.

Le *Initial Coin Offering* – ICO – **non prevedono l'attribuzione di una partecipazione nel capitale della società emittente o di un titolo obbligazionario**, essendo la controprestazione sempre rappresentata da un valore digitale autonomamente generato dalla stessa offerente.

La novità introdotta dalle ICO sarebbe duplice riguardando:

1. la modalità dello scambio e
2. l'oggetto dello scambio i *token* (mentre nelle IPO sono gli strumenti finanziari tradizionali).

È giusto però precisare che se fino ad ora non è stata ancora introdotta una ICO azionaria od obbligazionaria è solo imputabile al fatto che se si procedesse in tal senso si sarebbe legati a vincoli normativi già ben definiti anche se alcuni ordinamenti nazionali si stanno muovendo in tal senso (si veda ad esempio per la Svizzera la Guida emessa il 16 febbraio 2018 dalla FINMA – Autorità svizzera di vigilanza dei mercati finanziari – per chi vuole lanciare una ICO).

La caratteristica dell'ICO quindi è la ***tokenizzazione*** **cioè la registrazione dell'offerta.**

Se alla scadenza del termine la raccolta avrà raggiunto l'ammontare minimo - *min cap* – prefissato l'attivazione dello *Smart contract* (si veda il capitolo 3 della presente Guida) garantirà l'assegnazione ai sottoscrittori degli *investment token*, sulla base del rapporto di cambio; in caso contrario l'ICO s'intenderà fallita ed i fondi verranno automaticamente restituiti.

2.3) *Token*: definizione

Un *token* o *cryptoasset* è un insieme di informazioni digitali registrate su una *Blockchain* in grado di conferire un diritto ad un soggetto.

Un *token* quindi dà e sancisce la titolarità di un diritto.

Una definizione più completa di un Token è che esso rappresenta "*una soluzione criptografica che consente la circolazione su rete telematica senza intermediazione di terzi di un asset digitale che incorpora o rappresenta un diritto soggettivo*"[26]. Tale nozione risulta in linea con la definizione di bene (anche digitale) in quanto assoggettabile all'art. 810 del c.c. italiano.

2.4) La tokenizzazione

Che cosa s'intende per *tokenizzazione*?

Che cosa significa *token* nel mondo della *Blockchain*?

Un *token* è un insieme di informazioni digitali all'interno di una *Blockchain* che conferisce un diritto di proprietà o altro diritto a un determinato soggetto.

Nel consegue che la *tokenizzazione* è la conversione dei diritti di un bene in un *token* digitale registrato su una *Blockchain*.

Il bene reale ed il *token* sono collegati da uno *Smart contract*.

Quindi *tokenizzare* significa generare un *token* e collegarlo a un bene mediante uno *Smart contract*.

[26] https://www.blockchain4innovation.it/esperti/token-tra-cripto-asset-e-altri-elementi-digitali/#:~:text=Un%20token%20%C3%A8%20in%20sostanza,obbligazione%20a%20favore%20del%20secondo.

Che cosa è "*tokenizzabile*"?

Teoricamente qualsiasi cosa e ci aspettiamo in un futuro non troppo lontano una vera e propria rivoluzione paragonabile a quello che fu l'avvento di *Internet* nella nostra società: infatti la *Blockchain* è pronta e capace di rivoluzionare non soltanto tutti gli aspetti della finanza, ma anche i servizi pubblici e civili.

È assai verosimile che presto vivremo in un'economia interamente *tokenizzata*, dove ogni forma di archiviazione di valore e registrazione pubblica diventa un *token* con un valore di mercato fluttuante e scambiabile globalmente mediante apposite piattaforme digitali.

Per adesso tra i primi settori in cui la *tokenizzazione* è già stata impiegata sono:

1) **l'ambito immobiliare** (con condomini di lusso abilitati alla *tokenizzazione* su *Ethereum*) che forse si può avvicinare all'istituto giuridico della multiproprietà.

In questo modo la proprietà è stata suddivisa in tante piccole quote da vendere agli investitori in un processo di "democratizzazione" dell'azionariato non escludendo la turnarietà temporale nell'utilizzo dell'immobile.

L'acquisto di una piccola frazione di un immobile permette anche ai piccoli investitori di entrare su un mercato solitamente loro precluso, senza ricorrere a mutui e intermediazioni di istituti di credito.

Per i costruttori il vantaggio di questo tipo di finanziamento è quello di offrire maggiore flessibilità e afflusso di capitali nel breve termine.

2) Si è già assistito anche alla ***tokenizzazione* di alcune opere d'arte** in cui i partecipanti a speciali aste hanno ricevuto delle quote digitali dell'opera (per esempio *Swancoin*).
3) Anche nel **mondo dello sport** alcune società hanno deciso di gestire le decisioni aziendali mediante piattaforme decentralizzate che permettono la vendita di azioni e diritti ai *fans* – *merchandising* - sparsi nel mondo in modo rapido e sicuro dando ai tifosi il vantaggio di poter accedere a contenuti e servizi esclusivi.
4) Ma l'uso di *token* informatici si prospetta utilissimo soprattutto nel **settore borsistico.**

Sono già attivi dei progetti per la *tokenizzazione* degli "***stock exchange***" con la messa a punto di piattaforme decentralizzate, ovvero di infrastrutture per lo scambio delle azioni che sono proprietà di tutti e sono quindi al riparo da manipolazioni diverse da quelle "naturali" del mercato.

Per avviare progetti di questo tipo occorre trasformare le azioni delle società quotate in borsa in *token*, cioè ***tokenizzare* le azioni** (in maniera conforme alle leggi e opportunamente regolamentata).

Si prevede che **in futuro** un sempre maggiore numero di società sceglieranno questa modalità di "piazzamento" delle loro azioni sul mercato, dando l'avvio ad un'enorme rivoluzione nel settore finanziario dove tutte le borse valori del mondo saranno collegate in un'unica piattaforma mondiale che è proprietà di tutti e non necessita di una gestione, poiché si gestisce da sola, come già succede già ora per le *cryptovalute*.

Se si segue questa definizione anche le ***cryptovalute*** come gli *ether* sono da intendersi come ***payment/currency token*** e possono formare oggetto di attribuzione all'interno di una ICO.

Però ciò avviene di rado, perché in genere le ***cryptovalute*** come i ***bitcoin*** sono governate da un sistema di creazione diffusa.

Grazie ai protocolli *open source* non serve disporre di una *Blockchain* dedicata per effettuare una registrazione digitale suscettibile di trasferimento attraverso il protocollo DLT - *Distributed Ledger Technology*.

È sufficiente seguire gli standard (in genere l'ERC 20 di *Ethereum*) per la scrittura dello *Smart contract* e da ciò generare i *token* recanti la rappresentazione crittografica unica ed immodificabile di qualsiasi *asset* legato al mondo reale.

Che sia:

1) un'azione,
2) un'obbligazione,
3) un credito od anche

4) la proprietà di un bene

può essere allo stesso modo "incorporato" in un *token* poiché ciò che rappresenta il *token* è semplicemente il diritto su questi beni ed in questa forma sarà venduto o scambiato in tempo reale senza bisogno di ricorrere ad intermediari (questa è la principale funzione della *Blockchain* in quanto le operazioni di verifica ed autorizzazione avvengono presso tutti coloro che entrano nella catena – *chain* – con il ruolo di nodi).

Con riferimento alla ICO non esiste un vero e proprio modello di riferimento, perché ogni emittente è libera di determinare il contenuto del *digital token agreement* a proprio piacimento.

Attualmente, però, solo la Francia e Malta hanno adottato una normativa che regolamenta le ICO mancando ancora una normativa Comunitaria.

In Italia la CONSOB sta sollecitando il legislatore.

Vista la varietà di fattispecie di *token* passiamo ad esaminare l'ipotesi più frequente di utilizzo di un ICO e cioè l'offerta iniziale di ***utility token*** quindi quei valori digitali che conferiscono al sottoscrittore il diritto di fruire di servizi o di ricevere beni che l'emittente si propone di realizzare grazie ai finanziamenti ricevuti (per esempio un accesso ad uno *storage cloud*, un accesso ad una piattaforma di *gaming* – videogiochi o *trading on line*, ecc…).

2.5) Le "proprietà" *Smart.*

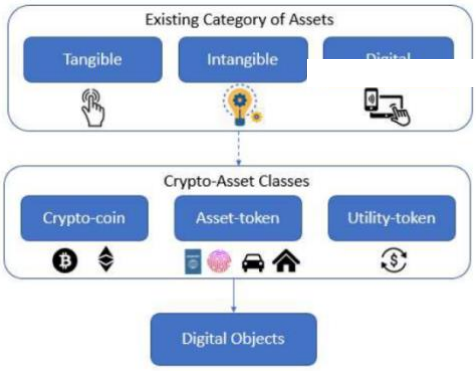
Definendo come attività o *asset* o più semplicemente "bene" ex articolo 810 del c.c. ovvero "cose che possono formare oggetto di diritti" con l'avanzata tecnologica sono emersi una serie di beni che prima dell'era digitale non avevano luogo, ovvero i **beni digitali.**

Essi possono essere definiti come “beni rappresentati in formato binario (ovverosia da una serie di 0 e 1, a-tecnicamente i “file”), di cui si possiedono i relativi diritti di utilizzo, contenuti all'interno di un dispositivo di memorizzazione (fisico o virtuale), che esistono o esisteranno in futuro[27]”.

Con tale definizione è possibile intendere tutti quei beni digitali prima della nascita della *Blockchain*, dove il carattere digitale del bene permetteva in modo univoco la cessione dei diritti di utilizzo.

La creazione delle *Blockchain*, richiamando le caratteristiche menzionate al capitolo 4 della presente Guida in tema di *cryptovalute*, quale la *non double spending*, ha dato luogo ad un’altra tipologia di beni ovvero i c.d. ***Cripto Asset*** che possono essere differenziati in base alla loro funzionalità e finalità ed il cui scambio può far a meno di entità centralizzate.

Un primo schema di differenziazione (fermo e considerando che non esiste uno standard generalmente accettato[28]) è mostrato alla figura qui sotto rappresentata.



Se si procede ad una classificazione delle Cripto Attività possiamo distinguere:

1. ***Cryptovalute* e collegati**: la prima categoria di *Asset* presenti all’interno dei sistemi *Blockchain* sono le c.d. *Cryptovalute* che sono definibili secondo il Glossario finanziario

[27] https://www.networklex.it/post/eredit%C3%A0-digitale-i-beni-digitali-e-gli-account-nella-societ%C3%A0-dell-informazione-puntata-1#:~:text=I%20beni%20digitali%20sono%20beni,esisteranno%20in%20futuro%5B6%5D.

[28] Blockchain Interoperable Digital Objects, June 2019 - DOI: 10.1007/978-3-030-23404-1_6 - In book: Blockchain – ICBC 2019Edition: James Joshi, Surya Nepal, Qi Zhang, Liang-Jie ZhangChapter: Lecture Notes in Computer Science, vol. 11521Publisher: Springer, Cham – Pagina 8.

della Borsa Italiana[29]: "*una valuta virtuale che, secondo la definizione di Banca d'Italia, costituisce una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento. Le cryptovalute possono essere trasferite, conservate o negoziate elettronicamente.*"

2. ***Asset Token*** che sono potenzialmente il ponte di collegamento, inserendo a pari merito degli Oracoli, tra *Blockchain* e mondo reale e come si diceva possono essere definiti come la rappresentazione virtuale di tutta una serie di beni fisici all'interno di un sistema DLT.

3. Oltre a tali beni è giusto menzionare una categoria di beni "virtuali" molto particolari, gli **NFT (*Non Fungibile Token*)**

   Essi possono essere definiti come "*la possibilità di dimostrare un diritto sull'opera, garantito tramite uno Smart contract*"[30].

   La bellezza e particolarità di tali strumenti risiede nella tecnologia utilizzate per la loro creazione e distribuzione.

   Essa si caratterizza nella digitalizzazione di un elemento (sequenza binaria 0-1 di un oggetto digitale), la sua crittografia attraverso l'*hashing* che permette quindi l'inserimento del suo *hash* all'interno di un possibile *Smart contract* (e quindi nella *Blockchain* di riferimento con lo Standard ad essa collegata).

   Dunque, più che l'univocità del bene (che è sempre replicabile nel caso in cui il creatore voglia immetterne diversi) è garantita attraverso il meccanismo di *hashing* il controllo e la tracciabilità dell'oggetto fino ad arrivare al soggetto creatore attraverso gli *hash* (si veda il capitolo 1 della presente Guida).

   Lo scambio avviene attraverso la valuta di rifermento della *Blockchain*; una delle più popolari opere vedute è quella Mike Winkelmann (*Beeple*) – *Every days: the first 5000 days v*enduta per un ammontare superiore ai 69 milioni di dollari[31].

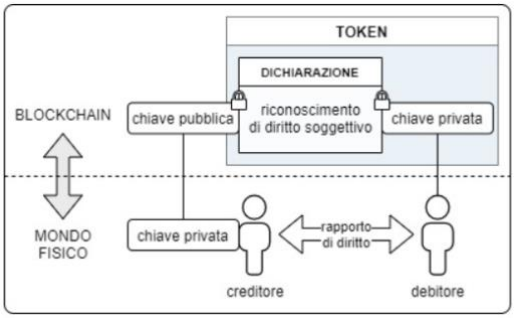
   Essi, per definizione, sono considerate il primo successo della categoria *Smart Property Native*.

[29] https://www.borsaitaliana.it/borsa/glossario/cryptovaluta.html

[30] https://www.agendadigitale.eu/documenti/nft-che-cosa-sono-come-funzionano-come-investire-sui-non-fungible-token/

[31] https://onlineonly.christies.com/s/first-open-beeple/beeple-b-1981-1/112924

La faccia opposta ai *native* sono i c.d. ***Smart Property Tokenizzati*** che rappresentano tutte quei *Token* che, attraverso il processo sia giuridico che tecnico detto *Tokenizzazione*[32], creano un collegamento diretto tra un bene presente nel mondo "reale" ed il mondo *Blockchain*.



Tokenizzazione

Essi agiscono, o dovrebbero agire dato l'elemento della "*Propriety*" sulla disponibilità/indisponibilità del bene, in relazione ad una nuova concezione[33] di circolazione di beni (e diritti) attraverso il trasferimento dei *token*[34].

La nuova modalità di trasferimento quindi, potrebbe risultare compatibile con il sistema italiano (cessione del diritto alla consegna del bene), anzi, innovandolo e rendendolo strumento di risoluzione di problematiche relative al trasferimento di un bene (poiché renderebbe identificabile la transazione in essere), come la conflittualità fra più acquirenti su un medesimo diritto.
Altra questione interessante è data dalla possibilità di includere garanzie identificate in modo univoco nel mondo reale e all'interno degli DLT e utilizzabili, al verificarsi di certe condizioni, attraverso lo *Smart contract.*

Dati dunque i *token* per i beni mobili prospetterebbero un sistema differente rispetto al principio "possesso vale titolo" ex art. 1153 c.c. che al momento vige nel sistema giuridico

[32]https://www.blockchain4innovation.it/esperti/token-tra-cripto-asset-e-altri-elementi-digitali/#:~:text=Un%20token%20%C3%A8%20in%20sostanza,obbligazione%20a%20favore%20del%20secondo.

[33] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart Contract; pagina 450

[34] Blockchain Interoperable Digital Objects, June 2019 - DOI: 10.1007/978-3-030-23404-1_6 - In book: Blockchain – ICBC 2019 Edition: James Joshi, Surya Nepal, Qi Zhang, Liang-Jie ZhangChapter: Lecture Notes in Computer Science, vol. 11521Publisher: Springer, Cham – Pagina 10.

italiano al fine di facilitare il trasferimento di beni mobili (non registrati) passando dunque ad una sorta di sistema pubblicitario mobiliare simile all'iscrizione sui registri immobiliari.

La creazione di un registro di tale ampiezza però dev'essere strettamente collegato ad un'ampia conoscenza tra gli individui della *Blockchain*, per ovviare ad una c.d. colpa grave[35] (che elimina la buona fede), riferita ad un soggetto che acquista un determinato oggetto presente come *token* e già trasferito ad un altro soggetto.

Questione analoga sembrerebbe apparire all'interno dei **beni immobili (o beni mobili registrati)** che, dato l'ordinamento giuridico italiano, richiedono l'opponibilità ai terzi attraverso l'iscrizione/trascrizione ai pubblici registri.
Essi dovrebbero quindi essere implementati all'interno della *Blockchain* attraverso un'azione del legislatore volta alla creazione di un *Registro On-Chain*[36].
Il requisito della prova scritta, come da indicazione delle linee guida AGID, sembrerebbe poter essere risolto mediante firma elettronica; nonché attraverso SPID, strumento incluso e comparato alla firma (si veda il capitolo 1 della presente Guida).
Le grandi potenzialità della *Blockchain*, dunque, parrebbero essere molto incidenti sia per l'economia internazionale nonché per il sistema legale di domani.

Le sue caratteristiche intrinseche potrebbero dar luce a filiere (*Value Chain*) perfettamente localizzate, certe ed immutabili così come la *Blockchain* a cui farebbero riferimento.

Dato l'elevato numero di opere vendute come NFT sembrerebbe che la *Blockchain* permetta una tutela, almeno operativa, maggiore a favore di tutta una serie di diritti di proprietà industriale ed intellettuale dove l'elemento cruciale sarebbe rappresentato dal momento di caricamento delle stesse *on-chain*.

[35] La colpa è "grave" quando la violazione dell'obbligo di diligenza è particolarmente grossolana, con un discostamento molto evidente del comportamento dell'agente dalle regole di diligenza, prudenza e perizia che il caso concreto avrebbe richiesto di osservare.

[36] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart Contract; pagina 452

2.6) Classificazione dei *token*

I *token* possono essere classificati diversamente in base alla loro creazione, da qui abbiamo una suddivisione tra:

a. ***Native***: In riferimento a tutti quei *token*/*cryptovalute* legati in modo univoco alla *Blockchain* di riferimento (*Bitcoin*, *Ethereum*, ecc.)
b. ***Non-Native*** *token* sviluppati da imprese che vogliono sfruttare *Blockchain* e protocolli già esistenti per l'esecuzione delle operazioni per cui sono nate.

Altra differenziazione è effettuabile tra:

1) ***currency token/cryptocurrencies*** che sarebbero le *cryptovalute* concepite come mezzi di scambio per l'acquisto di beni e servizi ed assumono una **funzione solutoria cioè di adempimento di un'obbligazione** (forse è possibile configurali anche come una forma di pagamento – si veda il capitolo 4 della presente Guida).

2) ***utility token*** – *token* di utilizzo - che sono rappresentazioni digitali di diversi diritti ed assumono una **funzione di godimento**.

Gli *utility token* permettono

a) il godimento di un bene o
b) la fruizione di un servizio.

Cioè:

a) permettono di ricevere il diritto ad una determinata prestazione ed
b) attribuiscono il diritto di poter utilizzare il bene.

Gli ***utility token*** potrebbero essere assimilati a dei documenti di legittimazione, la cui unica funzione sarebbe quella di **identificare l'avente diritto alla prestazione**

La funzione degli *utility token* è quella di permettere una più agevole circolazione della ricchezza anche futura.

Può affermarsi che gli ***utility token*** costituiscano una **nuova frontiera** dei titoli di credito "digitali".

L'*utility token* incorpora e rappresenta digitalmente un credito e ne permette sia l'esercizio che la sua circolazione.

In relazione alla circolazione dei beni occorre chiarire che *l'utility token* resta sempre una rappresentazione digitale del bene e che in quanto tale, dal punto di vista materiale, l'acquirente dovrà sempre acquisire la proprietà del bene.

Si tengano in considerazione nei diversi sistemi giuridici il momento di passaggio della proprietà e dei rischi: sistema francese/italiano; sistema romano/tedesco; sistema di common law (sull'argomento si veda a cura di Marco Tupponi "Manuale di Diritto Commerciale Internazionale" 3° Edizione – Giappichelli Editore pagg. 117 ss.).

3) ***security token* o *investment token*** che consistono in **prodotti finanziari** o titoli di partecipazione ed assumono una **funzione di investimento**.

Gli ***investment token*** sono documenti digitali:

a) rappresentativi di diritti economici legati all'andamento dell'iniziativa imprenditoriale oppure
b) rappresentativi di diritti amministrativi.

A seconda dei **diritti digitalmente rappresentati nei *token*** possono distinguersi i titoli di partecipazione e gli strumenti partecipativi al capitale di rischio.

I *token* rappresentativi dei soli diritti amministrativi e patrimoniali di un socio potranno essere assimilati ai titoli di partecipazione che conferiscono e rappresentano lo status di socio.

In questo caso non si ha il trasferimento di un credito nei confronti della società, ma il trasferimento di una più complessa posizione (diritti amministrativi e diritti economici) che deriva dall'essere il socio parte di un contratto di società.

I diritti del socio potranno essere trasferiti attraverso la cessione del *token*.

4) ***Token* ibridi** che raggruppano elementi della tipologia 2) e della tipologia 3).

Quindi la qualifica di quei *token* diversi dalle *cryptovalute* sub1) dipende dalla ricostruzione del rapporto obbligatorio che essi veicolano e la legittimità della loro rappresentazione e, dipende anche, dalle modalità di circolazione e dal grado di imperatività della legge che presiede i rapporti giuridici "incartolati"/titolo di credito.

Concludendo i *token* non sono altro che il veicolo che incorpora il rapporto giuridico/diritto sottostante consentendone la circolazione sulla *Blockchain* sulla quale sono innestati.

2.7) L'*investiment token* come "prodotto/strumento finanziario"

La dottrina partendo dall'assunto che con prodotto finanziario (si rammenti che il prodotto finanziario costituisce il *genus* e lo strumento finanziario costituisce la *species*) si intende l'impiego di capitali con funzione remunerativa ha allargato l'ambito ricomprendendo in essi anche l'acquisto di un bene (diamanti, opere d'arte, ecc.) a titolo di investimento se il venditore ha l'obbligo di riacquisto pagando un prezzo con un "profitto" per il compratore/investitore.

Da ciò si può pensare che anche gli ***investiment token***, se seguono il medesimo percorso possano rientrare nel novero dei prodotti finanziari, sia che il "guadagno":

a) sia monetario, incluse le *cryptovalute*,

b) sia che consista in un altro vantaggio patrimoniale anche sotto forma di un servizio.

Volendo applicare questo ragionamento alle ICO si può sostenere che gli ***investiment token*** possano essere offerti o anche solo previsti nel documento promozionale dove è stabilito che l'emittente si impegna a procedere al riacquisto o comunque a concludere accordi per l'ammissione degli ***investiment token*** alla negoziazione su uno o più *exchange.*

Si rammenta che un ***exchange*** è uno strumento strettamente connesso alle *cryptovalute* in quanto è una piattaforma tecnologica che permette di scambiarle.

La funzione di un *exchange*, quindi, è quella di poter permettere di effettuare l'acquisto e la vendita delle *cryptovalute* e di **realizzare un profitto**.

A seguito di una ICO gli *investiment token* offerti potrebbero dare diritti in natura altrettanto interessanti da un punto di vista patrimoniale rispetto alla moneta corrente od alla *cryptovaluta* come ad esempio:

1. un diritto di voto sulle decisioni di sviluppo del progetto imprenditoriale finanziato,
2. la promessa di un *bonus* economico in natura rapportato all'andamento economico dell'iniziativa,
3. il riconoscimento di un vero e proprio diritto agli utili,
4. ecc…

Una volta che si è acceduto all'opinione che gli ***investiment token*** **abbiano natura giuridica di prodotto/strumento finanziario** sorge il **problema** di stabilire a quale fonte debba essere associata la registrazione digitale.

In particolare, la loro negoziabilità impone di chiedersi se la promessa formulata nella ICO dall'emittente degli ***investiment token*** in uno o più sistemi di scambio - *exchange* – possa legittimare la qualificazione del *token* medesimo in termini, in particolare, di strumento finanziario **ex art. 1 comma 2 del TUF** con quanto ne consegue sul piano normativo ed operativo.

Se l'operazione fosse qualificabile come offerta al pubblico di prodotti finanziari le conseguenze sul piano normativo ed operativo sarebbero molto importanti:

a) sia per le imprese coinvolte che, salvo eccezioni, sarebbero tenute alla redazione del prospetto,

b) sia per il mercato del *Fintech* che si troverebbe costretto a fare i conti con la riserva di attività sancita dall'**art. 125 del Regolamento Intermediari** che obbliga ad informare i consumatori in attuazione dell'art. 32 TUF per la promozione ed il collocamento a distanza in favore dei risparmiatori al dettaglio.

Per esempio, per gli **strumenti finanziari** (ricompresi all'interno della categoria più ampia dei prodotti finanziari) **s'impone l'obbligo** di verifica dell'adeguatezza e la necessità di autorizzazione anche per le attività ancillari di *trading*, consulenza, ricezione ordini, ecc…

Art. 2.

*Per "**strumento finanziario**" si intende qualsiasi strumento riportato nella Sezione C dell'Allegato I. Gli strumenti di pagamento non sono strumenti finanziari* tra cui anche:

Allegato I - Sezione C - Strumenti finanziari

(1) Valori mobiliari.

Da cui il PROBLEMA:

è possibile assimilare gli *investiment token* ai valori mobiliari (per esempio azioni ed obbligazioni societarie)?

Se si esamina **l'art 1 comma 1 bis del TUF**,

- vista l'espressione generica "*categorie di valori*" che "*possono essere negoziati nel mercato dei capitali*"

- e visto che gli ***investiment token*** sono emessi generalmente in massa ed in forma **standardizzata sembrerebbe che l'assimilazione possa essere possibile**.

Art. 1-bis.

*Per "**valori mobiliari**" si intendono categorie di valori che possono essere negoziati nel mercato dei capitali, quali ad esempio:*

a) azioni di società e altri titoli equivalenti ad azioni di società, di partnership o di altri soggetti e ricevute di deposito azionario;

b) obbligazioni e altri titoli di debito, comprese le ricevute di deposito relative a tali titoli;

c) qualsiasi altro valore mobiliare che permetta di acquisire o di vendere i valori mobiliari indicati alle lettere a) e b) o che comporti un regolamento a pronti determinato con riferimento a valori mobiliari, valute, tassi di interesse o rendimenti, merci o altri indici o misure.

Si deve precisare che la circostanza che il contratto di vendita dei *token* poiché **si conclude a distanza** varrebbe comunque ad assicurare ai sottoscrittori/consumatori una qualche forma di tutela quanto meno ai sensi del D.Lgs n. 70/2003 – in tema di commercio elettronico - ed eventualmente anche del Codice del Consumo (ex artt. 49-59 del Codice del Consumo sui contratti a distanza) con la possibilità, ad esempio il diritto di "ripensamento" entro 14 giorni dal contratto concluso.

3) SMART CONTRACT

3.1. – Gli antecedenti degli *Smart contracts*

Qui di seguito traccerò una breve analisi storica relativa agli *Smart contracts* che mi auguro possa essere utile alla chiarezza espositiva di questo strumento giuridico.

La prima definizione che è possibile dare a tale strumento è quella di fattispecie in grado di dare esecuzione ad un contratto in modo indipendente dall'intervento umano.

Nel XIX secolo si sono susseguite una serie di innovazioni similari alla definizione precedentemente attribuita agli *Smart contracts*; per esempio, nel 1832 è stata creata da Richard Carlile[37] una macchina in grado di distribuire in moto automatizzato i libri vietati in Inghilterra al fine di eludere/eliminare la responsabilità formale dell'esecuzione del contratto in capo ad esso.

Nel XX secolo e prima di calarci nell'analisi approfondita degli *Smart contracts* vere e propri voglio delineare le differenze tra questi ed i suoi più prossimi "predecessori".

L'idea di esprimere un rapporto contrattuale in forma elettronica non è certa nuova, così come non lo è quella di assegnare ad un *software* il compito di concorrere alla formazione della volontà negoziale, all'interpretazione o all'esecuzione dell'accordo.

Fin dall'inizio degli anni '60, **la scienza giuridica** ha cominciato ad avvertire le potenzialità connesse all'utilizzo degli elaboratori e della logica matematica.

Tra i primi esperimenti applicativi in materia, può essere rammentata la "traduzione" del *British Nationality Act* del 1981 nel linguaggio di programmazione *Prolog*, acronimo per *Programming in Logic*.

L'obiettivo del lavoro era costituito dallo studio del procedimento di formalizzazione informatica di un testo normativo e del ragionamento giuridico sottostante, nella convinzione che una simile indagine avrebbe favorito sia lo sviluppo delle tecnologie connesse all'intelligenza artificiale (in relazione alle quali il diritto costituisce un ottimo riscontro per i linguaggi formali di

[37] Britannica, The Editors of Encyclopedia. "Richard Carlile". *Encyclopedia Britannica*, 6 Feb. 2021, https://www.britannica.com/biography/Richard-Carlile. Accessed 9 June 2021.

rappresentazione della conoscenza e per gli schemi di risoluzione dei problemi), sia l'intelligibilità di una legge, il *British Nationality Act* appunto, piuttosto articolata e controversa.

Tra la fine del secolo scorso e l'inizio del nuovo, il filone di ricerca tra scienza informatica e diritto ha affrontato nello specifico, la questione relativa alla **formalizzazione dei contratti in un linguaggio informatico che fosse capace di riprodurre il contenuto dell'accordo quanto più fedelmente possibile**, **e che consentisse l'automazione della stesura, dell'analisi, della revisione e dell'esecuzione dei rapporti contrattuali.**

Il fine di questa indagine, oltre a costituire la base sulla quale sono fondati gli *Smart contracts*, ha portato, parallelamente, alla nascita di una serie di **soluzioni *software*** incentrate sull'automazione della redazione di nuovi contratti (ausilio alla stesura di documenti giuridici attraverso l'utilizzo del linguaggio simbolico e della formalizzazione informatica), e sull'analisi di quelli già esistenti (come nel caso dell'impiego delle **tecnologie di apprendimento automatico**, il c.d. *machine learning*, per segnalare la presenza, all'interno del testo di un accordo, di eventuali incoerenze, ambiguità e altri fattori di rischio sul piano logico o lessicale).

Con particolare riferimento all'ambito accademico, merita senz'altro di essere segnalata l'attività svolta dallo *Stanford Center for Legal Informatics* (Codex), relativa soprattutto allo studio della ***computational law***: branca dell'informatica del diritto **che si occupa della meccanizzazione dell'analisi giuridica**, portatrice di importanti riflessi applicativi.

Tra le osservazioni più interessanti emerse dal settore di indagine costituito dalla *computational law* vi è la considerazione che trasporre un contratto in linguaggio informatico importa la possibilità di sottoporlo ad un procedimento di verifica formale.

Questa tecnica, ideata per l'esame teorico dei sistemi *hardware* e *software*, al fine di far emergere eventuali anomalie di funzionamento, consente di dimostrare o contestare in via matematico-formale la rispondenza di un determinato strumento, ad esempio un programma per elaboratore, a specifici requisiti o caratteristiche.

Sottoporre un contratto a verifica formale potrebbe, quindi, permettere di stabilire se le pattuizioni in esso contenute sono logicamente compatibili le une con le altre e se determinano, nel complesso, un assetto di interessi effettivamente coincidente con quanto voluto dalle parti.

Per raggiungere tale risultato si è proposto di utilizzare il *model checking*, **metodo di verifica formale** che si caratterizza per essere facilmente automatizzabile, consistente nell'esplorazione

sistematica ed esaustiva del modello matematico che rappresenta il sistema *hardware* o *software* da sottoporre a test (**in questo caso il contratto**).

Almeno a partire dal 1969, infatti, è stato avviato lo sviluppo di sistemi in grado di rappresentare e classificare gli elementi di un contratto in termini idonei ad essere elaborati da un programma informatico.

Già allora, l'obiettivo che si intendeva conseguire non era il semplice trasferimento del testo di un accordo su di un documento elettronico, bensì la creazione di un modello che consentisse di raffigurare il contenuto di un contratto attraverso un linguaggio formale, comprensibile e processabile da un elaboratore, al posto (o a fianco) dell'utilizzo del linguaggio naturale.

Si cerca, cioè, di trasporre (ove possibile) la semantica contrattuale in chiave **algoritmica**: in questo senso, ad **esempio**, il concetto di «pagamento» può essere espresso con un'operazione che prevede il raffronto dei movimenti di denaro avvenuti tra due parti.

L'aspetto forse più interessante di queste figure, definite alcuni decenni più tardi *data-oriented contract*, è costituito dal fatto che **una macchina diviene per la prima volta destinataria delle pattuizioni contenute nel contratto.**

«A "data-oriented" contract is one in which the parties have expressed one or more terms or conditions of their agreement in a manner designed to be processable by a computer system. Typically, the parties express core elements as precisely defined computer data, rather than (or in addition to) a written language document to facilitate computer analysis, automation, or communication of their contractual obligations».

La rappresentazione del contenuto contrattuale in termini informatici apre la strada all'ingresso dell'automazione.

In altre parole, diviene possibile che **sia lo stesso *software* ad intervenire dinamicamente in un rapporto negoziale**, sulla base della combinazione tra un insieme di istruzioni predefinite ed una serie di *input* forniti al programma.

Dunque, alla descrizione in forma algoritmica dell'accordo **viene aggiunto il collegamento con le informazioni necessarie al *software* per interagire con il contratto** (ad **esempio**, il programma deve essere anche capace di interloquire con un registro degli incassi e dei pagamenti per poter stabilire se il prezzo della merce è stato corrisposto entro il termine pattuito), allo scopo di consentire lo svolgimento in via automatizzata di determinate operazioni.

Si parla, in simili ipotesi, di ***computable contract***.

L'applicazione delle logiche suddette ha portato, nel corso degli anni '70, alla nascita del **modello *Electronic Data Interchange (EDI*),** sviluppato per consentire lo scambio standardizzato di informazioni digitali tra operatori commerciali, e che risulta aver conseguito un buon successo in termini di prevenzione del contenzioso giudiziario.

Gli *Smart contracts* aggiungono, al quadro precedente, una **novità fondamentale**, costituita dalla loro particolare modalità di esecuzione delle prestazioni; mentre, in ultima istanza,

a) l'adempimento di un ***data-oriented contract*** o di un ***computable contract*** può sempre essere interrotto o impedito mediante un'azione, anche unilaterale, posta in essere da uno dei contraenti, perché questo tipo di contratti non era inserito in una *Blockchain*,

b) nel caso degli ***Smart contracts*** queste **interruzioni o impedimenti** sono **esclusi ab origine in quanto inseriti in un meccanismo di *Blockchain*.**

In particolare, quindi storicamente abbiamo avuto:

1. **Contratti in forma elettronica** che sono contratti, dove il corpo degli stessi è sviluppato secondo linguaggio umano ma dove la conclusione avviene attraverso il *web*.

2. ***Data-Oriented Contracts*** che sono contratti, ancorché stipulati fra persone, che possono essere redatti in modo tale da poter essere eseguiti[38] anche attraverso l'automazione di un *computer* dunque redatti attraverso un linguaggio informatico.

[38] https://www.agendadigitale.eu/documenti/litalia-prova-a-normare-gli-Smart-contract-ecco-come-pro-e-contro/

3. ***Computable Contracts*** che sono contratti che differiscono dai precedenti in quanto, oltre all'automazione possibile dell'esecuzione è inoltre possibile includere alcune condizioni (***if-then***) che determinano l'esecuzione in modo condizionato a determinati eventi basati su dati presenti; un **esempio** operativo può essere **il *trading online***.

I problemi, o meglio i limiti, di tali fattispecie riguardano la discrepanza tra il linguaggio "naturale" e quello dei *computers*, in quanto il linguaggio "naturale" risulta molto più normato da regole e questo potrebbe portare ad un problema di comprensione ed esecuzione di clausole contrattuali complesse da parte del computer stesso.

Si sottolinea ancora una volta che anche questo tipo di contratto si differenzia dagli *Smart contracts* in quanto può essere reversibile e modificabile[39].

4. ***Ricardian Contracts*** che sono contratti che rappresentano i veri precursori (e parte integrante) degli *Smart contracts*.

Teorizzati da Ian Grigg nel 1996[40] i Contratti Ricardiani (che prendono nome dall'economista David Ricardo) sono definiti dallo stesso creatore come "*un contratto digitale che definisce i termini e le condizioni di un'interazione, tra due o più parti, che è crittograficamente firmato e verificato*".

È importante sottolineare che un Contratto Ricardiano è leggibile sia dall'uomo che dalla macchina e può essere firmato digitalmente; esso, dunque, come si evince dalla definizione, è un contratto che soddisfa due requisiti fondamentali:

a. Il *Design Pattern*: ovvero l'identificazione delle parti prima dell'esecuzione ed il
b. *Prose Parameters and code*: ovvero il processo mediante il quale viene creata una prosa legale, che permette la validità giuridica, a cui poi è collegata un codice informatico che permette l'esecuzione del contratto.

[39] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 226.

[40] Smart contract Templates: foundations, design landscape and research directions - Christopher D. Clack and Vikram A. Bakshi and Lee Braine - 2017.

	Contratto intelligente	Contratto Ricardiano
Scopo	Eseguire i termini di un accordo	Registrare i termini di un accordo come documento legale
Flusso	Automatizza le azioni sulle applicazioni basate su blockchain	Può anche automatizzare le operazioni sulle applicazioni basate su blockchain
Validità	Non è un documento legalmente vincolante	È un documento o un accordo legalmente vincolante
Versatilità	Non possono essere Contratti Ricardiani	Qualsiasi Contratto Ricardiano può essere anche uno Smart Contract
leggibilità	I contratti intelligenti sono leggibili dalla macchina ma non necessariamente leggibili dall'uomo	I Contratti Ricardiani sono sia leggibili dalla macchina che leggibili dall'uomo

Le caratteristiche dei Contratti Ricardiani, ancorché similari a quelle degli *Smart contracts* li distinguono in modo netto da quest'ultimi; in particolare nella figura[41] notiamo come i Contratti Ricardiani presentino una versatilità maggiore rispetto agli *Smart contracts* sotto diversi aspetti.
Essi sono degli strumenti teorizzati per coadiuvare l'aspetto digitale e legale, nonché normativo, dei contratti moderni collegando ad un testo contrattuale il relativo codice informatico per **l'esecuzione che**, **a differenza degli *Smart contracts*, può avvenire sia all'interno che all'esterno del sistema *Blockchain***, nei casi nei quali quest'ultimo meccanismo non sia utilizzabile per gli *Smart contracts*.

Quindi un contratto Ricardiano può essere, in parte, uno *Smart contract*, mentre uno *Smart contract* non potrà mai essere un Contratto Ricardiano, in quanto non può includere al proprio interno la prosa legale riferita al codice.
Si tenga presente che il sistema, denominato anche *Ricardian Smart contract*, si compone di tre elementi collegati tra loro:

1. il testo del contratto (che rende direttamente comprensibile il codice informatico),
2. lo *Smart contract* ed

[41] https://101blockchains.com/ricardian-contracts/

3. i parametri che influenzano e determinano la sua esecuzione.

3.2) Caratteristiche tecniche e tecnologiche degli *Smart contracts*

Gli *Smart contracts* come tali sono stati oggetto di sperimentazione negli anni ’90, ma l’idea di “contratto intelligente” si può fare risalire già agli anni ’70 in relazione alla necessità di gestire l’attivazione o disattivazione di una licenza *software* in funzione di determinati requisiti.

Uno dei primi a effettuare tali sperimentazioni e a coniare il nome stesso fu Nick Szabo, laureatosi presso l’Università di Washington nel 1989 in informatica, esperto di crittografia, statunitense di origine ungheresi.

Szabo grazie alla passione per la *Data Science* iniziò a ipotizzare già nel 1993, quando ancora non si parlava di *Internet of Things* e di *Big Data*, che **determinati oggetti potessero essere gestiti in modo digitale in virtù di specificate condizioni**.

Scrive infatti Nick Szabo: “*L’idea di base dello Smart contract è che molti tipi di clausole contrattuali (come la garanzia, l’assunzione dell’obbligazione di pagamento, la delimitazione di un diritto di proprietà, ecc.) possono essere incorporati nell’hardware e nel software che trattiamo, in modo da rendere la violazione del contratto costosa per il soggetto inadempiente*”.

Lo stesso Nick Szabo ci fornisce una prima **definizione di *Smart contract*** (si tenga presente che questa definizione fu data prima dell’avvento della tecnologia *Blockchain* di cui al capitolo 1 della presente Guida) definendolo come “*a computerized transaction protocol that executes the terms of a contract. The general objectives of Smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs”*.

Tale è molto in linea con quelli che sono i concetti fondanti della futura *Blockchain*, ovvero la trasparenza, la minimizzazione di intermediari, la riduzione dei costi e delle possibili frodi.

Oltre alle logiche di base e fondanti del termine, le teorizzazioni di Szabo definiscono gli *Smart contracts* come *software* per poter eseguire in modo automatico determinate obbligazioni contrattuali e prevedere rimedi, anch’essi automatizzati, nel caso in cui avvenga un inadempimento contrattuale.

Nel periodo in cui è stata concepita l'accezione di *Smart contract* da Szabo, esso non poteva essere messo in pratica data l'assenza di un'infrastruttura che permettesse la loro adozione pratica; tale situazione cambia radicalmente con l'avvento delle *Blockchain* così come teorizzata da Satoshi Nakamoto nel 2008 in quanto la *Blockchain* crea un ambiente in cui la visione di Szabo può essere adottata, crescere ed ampliarsi, grazie alla possibilità di trasferimento delle informazioni senza che esse siano manomesse, duplicate o eliminate e senza ricorrere a soggetti terzi garanti .

Altro punto di svolta è stata la creazione della *Blockchain Ethereum* (capitolo 4 della presente Guida), ideata da Vitalik Buterin; una *Blockchain* diversa dalle biforcazioni avvenute in precedenza nella *Blockchain Bitcoin* (capitolo 4 della presente Guida).

L'innovazione maggiore della *Blockchain* su cui agisce *Ethereum* è stata quella di includere nella stessa un'ambiente di *runtime* dove si caricano tutte le applicazioni di un programma e le si esegue su una piattaforma nonché la compilazione e creazione di operazioni programmabili.

In pratica essa dà la possibilità di creare delle operazioni nuove attraverso la EVM ovvero l'*Ethereum Virtual Machine con* diversi linguaggi di programmazione che ne permettono l'implementazione.

Esso dà quindi una nuova definizione di *Smart contract*, molto generale, che attiene a qualsiasi programma eseguibile attraverso un *computer* nella rete *Ethereum* e che va a modificare la *Blockchain* con il meccanismo di consenso prestabilito.

Tornando agli aspetti giuridici teniamo presente che il modello giuridico che disciplina la materia dei contratti da cui è partito Szabo è stato quello di *Common Law* e non quello di *Civil Law* (si pensi per esempio, fra le tante difformità di metodo tra i due Sistemi, la letteralità nell'Interpretazione del Contratto che il giudice di Common Law ha come faro principe nell'esaminare un contratto che è entrato in "patologia").

Szabo, partendo dall'**esempio base** del **distributore automatico di bevande (*VENDING MACHINE*)**, offre ulteriori **esempi applicativi**, tra cui uno, ben più "*Smart*", relativo alla possibile gestione automatizzata dei rapporti nascenti dall'acquisto di un autoveicolo mediante pagamento a rate.

Grazie, infatti, ad una combinazione di *hardware* e *software* installati nel veicolo stesso, Nick Szabo giunge ad immaginare che lo *Smart contract* entri in azione per disabilitare la messa in moto dell'auto in caso di mancato pagamento di un certo numero di rate.

Un tale schema giuridico si può collocare nell'alveo delle diverse forme di autotutela previste anche nell'ordinamento italiano, quali, ad esempio:

1) l'eccezione di inadempimento ex art. 1460 c.c.,

Art. 1460. Eccezione d'inadempimento.

Nei contratti con prestazioni corrispettive, ciascuno dei contraenti può rifiutarsi di adempiere la sua obbligazione, se l'altro non adempie o non offre di adempiere contemporaneamente la propria, salvo che termini diversi per l'adempimento siano stati stabiliti dalle parti o risultino dalla natura del contratto.

Tuttavia non può rifiutarsi l'esecuzione se, avuto riguardo alle circostanze, il rifiuto è contrario alla ***buona fede.***

2) il potere di sospendere l'esecuzione in caso di mutamento delle condizioni patrimoniali di controparte ex art. 1461 c.c., (a livello internazionale l'art. 71 della C.I.S.G. 1980)

Art. 1461. Mutamento nelle condizioni patrimoniali dei contraenti.

Ciascun contraente può sospendere l'esecuzione della prestazione da lui dovuta, se le condizioni patrimoniali dell'altro sono divenute tali da porre in evidente pericolo il conseguimento della controprestazione, salvo che sia prestata idonea garanzia.

3) il diritto di ritenzione previsto dagli **artt. 2756 terzo comma e 2761 c.c.**

Art. 2756. Crediti per prestazioni e spese di conservazione e miglioramento.

I crediti per le prestazioni e le spese relative alla conservazione o al miglioramento di beni mobili hanno privilegio sui beni stessi, purché questi si trovino ancora presso chi ha fatto le prestazioni o le spese.

Il privilegio ha effetto anche in pregiudizio dei terzi che hanno diritti sulla cosa, qualora chi ha fatto le prestazioni o le spese sia stato in buona fede.

*Il creditore può **ritenere** la cosa soggetta al privilegio finché non è soddisfatto del suo credito e può anche venderla secondo le norme stabilite per la vendita del pegno,*

Art. 2761. Crediti del vettore, del mandatario, del depositario e del sequestratario.

I crediti dipendenti dal contratto di trasporto e quelli per le spese d'imposta anticipate dal vettore hanno privilegio sulle cose trasportate finché queste rimangono presso di lui.

I crediti derivanti dall'esecuzione del mandato hanno privilegio sulle cose del mandante che il mandatario detiene per l'esecuzione del mandato.

I crediti derivanti dal deposito o dal sequestro convenzionale a favore del depositario e del sequestratario hanno parimenti privilegio sulle cose che questi detengono per effetto del deposito o del sequestro.

*Si applicano a questi privilegi le disposizioni del secondo e del **terzo comma dell'articolo 2756.***

PROBLEMA GIURIDICO: tale possibilità se è sproporzionata rispetto al danno subito non è tutelata, normalmente, dagli ordinamenti giuridici perché recherebbe un danno ben maggiore rispetto a quello subito.

Lo *Smart contract* è funzionale alla più agevole circolazione della ***Smart Property*** (capitolo 2.5 della presente Guida) che in senso lato va considerata come *cryptoricchezza* consistente in beni, crediti, *cryptovalute*, servizi, titoli di partecipazione nonché prodotti finanziari.

La nozione di *Smart Property* fa riferimento a qualsiasi bene materiale o immateriale o diritto che, essendo rappresentati digitalmente, possono essere esercitati o goduti attraverso l'esclusiva disponibilità di un ***token*** (capitolo 2 della presente Guida).

Uno *Smart contract* attraverso la tecnologia *Blockchain* costituisce non solo un sicuro strumento di registrazione di ogni tipo di bene, materiale o immateriale, ma anche un più sicuro e più efficace strumento di scambio.

Fino a qualche tempo fa, lo sviluppo delle tecnologie *Blockchain* è avvenuto essenzialmente a prescindere da qualsiasi valutazione o considerazione circa la loro compatibilità con gli ordinamenti nazionali, ritenuti quasi degli "avversari" nei confronti di un nuovo sistema, caratterizzato:

1) **dalla virtualità**,
2) **dalla decentralizzazione** (attraverso la quale si vogliono porre tutti i soggetti su di un piano di virtuale equivalenza),
3) **dall'indipendenza** (intesa anche nel senso di alternatività o alterità rispetto ad ogni ordine precostituito) e
4) **dall'autogoverno** (ogni vicenda che si svolge all'interno della *Blockchain* è dominata dalla "legge" del codice informatico e del consenso distribuito

La dottrina giuridica, specialmente di matrice anglosassone, ha da subito riservato una notevole attenzione al tema degli *Smart contracts,* interrogandosi su un possibile quadro definitorio, nonché sui connotati caratterizzanti ed essenziali di tali strumenti.

Anche in assenza di una definizione universalmente condivisa, si ritiene opportuno evidenziare quella proposta da Christopher D. Clack, Vikram A. Bakshi e Lee Braine, che risulta particolarmente adeguata: «***a Smart legal contract is an automatable and enforceable agreement.***

Automatable *by computer, although some parts may require human input and control.*

Enforceable *either by legal enforcement of rights and obligations or via tamper-proof* - resistente alle manomissioni - *execution of computer code*».

Tale definizione, ripresa ed approfondita nel contributo della Banca Europea per la Ricostruzione e lo Sviluppo (EBRD), permette di chiarire la distinzione, ricorrente in dottrina che sussiste tra «*Smart contract code*» e «*Smart legal contract*».

1) **La prima espressione («*Smart contract code*»)** si riferisce agli *Smart contracts* nella loro accezione meramente informatica e descrive un ***software***, collocato all'interno di un sistema DLT – *Distributor Ledger Technologies*, che utilizza la logica condizionale per determinare il verificarsi di una o più condizioni prestabilite; a seguito di tale controllo, esso compie **automaticamente** una specifica operazione (secondo lo **schema *if this-then that***), che può avere o meno rilevanza per il diritto.

Lo schema *if this-then that* opera con clausole che stabiliscono:

a) in un dato momento e tenendo conto delle circostanze concrete – ***if this***,

b) il contenuto delle prestazioni delle parti – ***then that.***

Quindi lo *Smart contract* è un contratto necessariamente condizionato dagli eventi - *if this* senza i quali il *software* non potrebbe operare automaticamente – *then that*: l'automatica esecuzione della prestazione *y* è sospensivamente condizionata all'avverarsi dell'evento *x*.

N.B. Lo schema dello *Smart contract* implica la gestione programmata di un accordo che le parti devono avere già concluso: **lo *Smart contract* riguarda la fase dell'adempimento e non della sua formazione.**

3.2.a) Il termine "**DLT**", o ***D**istributed **L**edger **T**echnologies* (Tecnologie a Registri Distribuiti), indica un insieme di protocolli che permettono ad una rete composta da **nodi – *computers*** - di attori di pari entità (*peer nodes*) di gestire un **registro – *ledger* sincronizzato tra i partecipanti** grazie all'**utilizzo della crittografia** e senza necessità di un unico nodo centrale che si occupi della gestione e del controllo del registro.

2) **Il secondo termine («*Smart legal contract*»)**, invece, indica un **contratto** (inteso nel suo significato giuridico) rappresentato, del tutto o in parte, attraverso un codice informatico, le cui prestazioni sono eseguite, parzialmente o totalmente, in via automatica da un programma per elaboratore - *software* - che potrebbe essere inserito in una *Blockchain*.

È proprio il collegamento con le DLT - *Distributor Ledger Technologies* - a costituire il fattore maggiormente innovativo e interessante degli *Smart contracts*, in quanto consente di "saldare" **il momento dell'accordo con la successiva fase dell'esecuzione del contratto** («*Blockchains collapse agreement and execution. Because a Smart contract both is the agreement and executes it*»), rimuovendo la distinzione tra queste due fasi contrattuali.

N.B. L'ambizioso risultato che si intende conseguire è quello di **rendere virtualmente impossibile non adempiere.**

Comunque, gli *Smart contracts* danno esecuzione solamente a ciò per cui sono stati preventivamente programmati.

I contraenti che predispongono il contenuto dello *Smart contract* stabiliscono a priori, tramite il PRINCIPIO di AUTONOMIA CONTRATTUALE, le clausole, le modalità e le regole di controllo e di azione relativi al contratto **i cui effetti**, **dopo essere stati trasposti in codice algoritmico e quindi essere divenuti uno *Smart contract,* non scaturiscono più dalla volontà delle parti che è solo presupposta.**

Quindi il pericolo che uno dei contraenti si renda inadempiente rispetto alle proprie obbligazioni non verrebbe semplicemente mitigato attraverso il deterrente costituito dai tradizionali rimedi previsti dall'ordinamento, **ma, piuttosto, risulterebbe estinto alla radice, perché sarebbe impossibile non adempiere.**

Nel momento in cui una transazione viene disposta all'interno di una *Blockchain* essa è condivisa e replicata tra tutti **i nodi - *computers*** - che compongono la rete, uscendo così dalla sfera di intervento dei singoli utenti.

Gli stessi meccanismi di consenso, che regolano automaticamente la tenuta del registro distribuito (DLT - *Distributor Ledger Technologies*), vengono utilizzati per computare le operazioni e i trasferimenti stabiliti nello *Smart contract.*

Al verificarsi delle condizioni previste, ai fini della sua attuazione, proprio perché inserite in una *Blockchain*, **la transazione diviene irrevocabile, irreversibile ed immutabile**, sebbene, come vedremo, non in modo del tutto assoluto.

N.B. La realizzazione delle prestazioni dedotte nel contratto viene, così, svincolata dal fattore umano.

Per quanto riguarda l'esecuzione automatica della prestazione, come si è detto: non lascia la possibilità per i contraenti di compiere azioni contrarie o diverse da quelle previste nelle clausole contrattuali, limitando il potere discrezionale delle parti;

Occorre, tuttavia, tenere presente che lo schema di attuazione automatica proprio degli *Smart contracts* è in grado di manifestare appieno la sua efficacia **soltanto nell'ambito del contesto tecnologico delle DLT -** *Distributor Ledger Technologies*.

L'esecuzione degli *Smart contracts*, infatti, **perde** la caratteristica di essere effettiva e "resistente alle manomissioni" (*tamper proof*) quando nel trasferimento viene coinvolta un'articolazione della realtà collocata **al di fuori** della *Blockchain*:

1. fino a quando lo scambio avviene tra entità o risorse che nascono ed esistono unicamente nel registro distribuito (come le *cryptovalute*) – DLT, il sistema si rivela efficace e potenzialmente autosufficiente;
2. diversamente, se ad essere coinvolti sono **beni o diritti non incorporati nella *Blockchain***, gli *Smart contracts* non possono garantire la corretta ed effettiva esecuzione delle prestazioni in essi contenute.

Uno degli esempi più famosi di *Smart contract* è quello che ha dato origine ai *Bitcoin*.

I dati del codice informatico dello *Smart contract* acquisiscono una propria unità giuridica solo ed unicamente se, a monte, si riconoscono che i dati raccolti e distribuiti attraverso *Blockchain* **producono effetti giuridici**.

Si veda, ad esempio, la nozione di contratto che dà il nostro codice civile all'art. 1321

*"Il contratto è l'accordo tra due o più parti per costituire, regolare od estinguere tra loro un **rapporto giuridico** patrimoniale"*.

Si veda anche **l'art. 8 ter** del cosiddetto **Decreto semplificazioni del 2018 (legge 12/2019)**.

Dispone infatti l'art. 8-ter del Decreto:

"1. Si definiscono (DLT) *"**tecnologie basate su registri distribuiti**" – **BLOCKCHAIN** - 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** – DLT - 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* (FIRMA DIGITALE) *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".*

Detto articolo definisce quindi le nozioni di DLT - "Tecnologie basate su Registri Distribuiti" - al primo comma e di "*Smart contract*" al secondo, prevedendo al terzo comma gli effetti giuridici della memorizzazione di un documento informatico attraverso l'uso di tali tecnologie basate su registri distribuiti - DLT.

N.B. Ne consegue che il **supporto legale** è di utilità nella stesura dello *Smart contract*, **ma non** nella fase di verifica e attivazione, che avviene in maniera automatica.

3.2.b) L'adempimento del contratto è, come abbiamo detto, **automatizzato** e subordinato unicamente al verificarsi di determinati eventi sottratti alla volontà delle parti (*if this – then that*).

A) L'adempimento "automatico" di uno *Smart contract* è armonico alle teorie "non negoziali acausali" che sottolineano l'irrilevanza dell'*animus solvendi* nell'inquadramento del concetto di adempimento. ASTRAZIONE SOSTANZIALE DELLA CAUSA (DIRITTO ROMANO – *STIPULATIO* – E DIRITTO TEDESCO)

B) Contraria a tale interpretazione è la teoria negoziale causale, secondo cui l'adempimento, per poter essere qualificato tale, deve essere accompagnato da una specifica volontà del debitore di adempiere (cioè dell'*animus solvendi*) e dall'accettazione del creditore. (LA CAUSA È ELEMENTO ESSENZIALE DEL CONTRATTO – È POSSIBILE SOLO UN'ASTRAZIONE PROCESSUALE DELLA CAUSA COME PER ESEMPIO NEL DIRITTO ITALIANO)

In sostanza, è possibile descrivere lo *Smart contract* come un contratto:

- **digitale**: le clausole contrattuali sono incorporate nel *software* sotto forma di codice informatico;

- **autoeseguibile**: l'adempimento, essendo governato dagli *input* previsti nel codice informatico, prescinde non solo dall'*animus solvendi* del debitore, ma finanche dal comportamento delle parti;

- **irrevocabile**: una volta iniziato, il processo di esecuzione non può essere fermato o modificato.

Da tali caratteristiche discendono diversi **VANTAGGI** che contraddistinguono lo *Smart contract* rispetto al contratto "tradizionale":

a) **in primo luogo**, per quei contratti che richiedono la necessaria partecipazione di un terzo intermediario (come, ad esempio, la somministrazione di energia elettrica e gas, la stipula di polizze assicurative, la compravendita di un bene immobile, la concessione di una linea di credito, ecc.) **la conclusione di un contratto sulla *Blockchain* sostituisce la necessità di un terzo intermediario con una "validazione" distribuita**, con conseguente risparmio di tempo e di riduzione di costi normalmente legati all'adempimento dell'accordo contrattuale e ciò riduce (se non azzera del tutto) il rischio di inadempimento di controparte.

b) **in secondo luogo** la registrazione (irreversibile e immodificabile) dello *Smart contract* sulla *Blockchain*, lascia una traccia indelebile e trasparente della storia del bene oggetto del medesimo e **diminuisce il rischio di danni derivanti da errori e frodi**.

Per queste ragioni, vi sono molteplici progetti in svariati settori ove si sperimenta l'applicazione pratica della *Blockchain* e dello *Smart contract* che determina operativamente la vendita del prodotto.

Per esempio: IL PROGETTO AGROALIMENTARE CARREFOUR (pollo contadino di *Auvergne* inserito su *Blockchain* per una tracciabilità del prodotto a beneficio dei consumatori).

Altro esempio: come assicurare ai consumatori l'origine e la qualità di una vaschetta di carne acquistata al supermercato?

Gli attuali sistemi di tracciabilità non sono assolutamente sicuri nel dare risposte certe ai consumatori.

La *Blockchain* invece permette di dare risposte certe.

Se un contratto, anche *Smart contract*, prevede il trasporto della carne ad una temperatura di + 7° il dialogo tra il sistema *Blockchain* e la logistica del prodotto consente di registrare costantemente la temperatura durante il trasporto e di monitorare le anomalie.

Poiché si è utilizzato uno *Smart contract* il pagamento per il vettore avverrà solo dopo aver confrontato la temperatura registrata durante il trasporto con il contenuto concordato nello *Smart contract*.

Ancora un esempio, gli *Smart contracts* possono essere utilizzati nella fornitura e nel pagamento di energia elettrica: al consumo registrato dal **contatore** (che, in questo caso, rappresenta **l'Oracolo** – oltre capitolo 3.7 - che collega il codice informatico alla realtà esterna) ne consegue una bollettazione precisa ed un puntuale pagamento della fattura.

Un quarto esempio è rappresentato dalla **piattaforma *UjoMusic***, che permette agli utenti di ascoltare musica e utilizzare i registri distribuiti – DLT - per pagare direttamente gli artisti, senza ricorrere ad alcun tipo di intermediario.

3.4) La natura giuridica di uno *Smart contract*

La possibilità di creare operazioni digitali personalizzate, che si auto-eseguono sotto certe condizioni rendono uno *Smart contract* un qualcosa di assimilabile alla definizione di contratto?

La risposta è positiva solo a certe condizioni.

Durante il progresso tecnologico la società ha visto susseguirsi una serie di innovazioni tecnologiche che hanno portato ad una sempre più crescete coesione tra uomo e macchina, quest'evoluzione ha riguardato anche il mondo dei contratti, introducendo e variegando una serie di

contratti di tipo digitale (come abbiamo visto al paragrafo 1 del presente capitolo), disciplinati rigorosamente nel corso del tempo.

I contratti di tipo digitale però differiscono in modo netto dagli *Smart contracts* in quanto diversi nelle singole caratteristiche.

Un contratto, così come definito, ad esempio, all'art. 1321 del Codice Civile italiano, rappresenta "l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale."

Ed i suoi elementi essenziali, definiti dall'art. 1325 c.c. sono l'accordo delle parti, la causa, l'oggetto e la forma se è prescritta dalla legge sotto pena di nullità.

Il contratto telematico o digitale, nella sua particolarità, presenta diverse declinazioni come contratto virtuale in senso lato (contratti conclusi mediante internet) o senso stretto (contratti conclusi attraverso un tasto negoziale virtuale)[42] e pone le sue fondamenta, come d'altra parte le pone anche il contratto "tradizionale", sull'autonomia contrattuale delle parti, in merito alle modalità di conclusione del contratto.

La dottrina,[43] riconosce il fenomeno come un'estensione dell'autonomia contrattuale in ambito digitale in merito alla formazione del contratto[44].

Dunque, il termine "virtuale" o "digitale", come si evince, è da riferire alla conclusione del contratto in sé, in quanto le parti sono di fatto reali e l'oggetto del contratto può avere natura materiale o immateriale.

Maggiore attenzione inoltre è stata data a tutti quei contratti virtuali in senso stretto o, cosiddetti, *Point and Click,* ovvero tutti quei contratti, riconosciuti all'art. 1336 c.c. come offerta al pubblico, conclusi, spesso B2C, attraverso l'interazione unica di un "utente che compila un format prestabilito

[42] https://www.diritto.it/la-qualificazione-del-contratto-digitale/

[43] https://www.altalex.com/documents/news/2014/07/30/il-contratto-telematico

[44] E. Tosi, in Digesto delle discipline privatistiche, voce Contratto Virtuale, Torino 2003.

presente sul sito della società venditrice o intermediaria"[45]. Tali contratti sono ampiamente regolamentati dal Codice del consumo e dalle normative di settore[46].

N.B. Ciò che attiene allo *Smart contract* però è una casistica differente sotto molti aspetti rispetto ai contratti virtuali appena descritti; in prima battuta esso si basa, come abbiamo visto, su *Blockchain* e rappresenta un mezzo, mediante il quale, si realizza un'esecuzione di una prestazione in modo autonomo e senza l'intervento di alcun soggetto, sia esso un contraente, un garante o un soggetto terzo.

Dunque, l'utilizzo dell'espressione *Smart contract* se si prende alla lettera potrebbe trarre in errore in merito alla sua natura, in quanto:

- Con il termine "*Smart*" si intende uno strumento che sia capace di "auto apprendere", ovvero che abbia la capacità di auto adattarsi in base a determinate circostanze con cui lo strumento si trovi in contatto.

Lo *Smart contract,* di fatto, non lo è. Esso è uno strumento informatico che, secondo specifiche funzioni ed istruzioni esegue determinate azioni a certe condizioni prestabilite.

Esso, dunque, non ha la capacità di riconoscere un'eventuale "impossibilità sopravvenuta" o un'"eccessiva onerosità" in assenza di istruzioni specifiche che monitorano determinati dati esterni o interni alla *Blockchain* in uso.

- L'attribuzione del termine "*Contract*" richiama un carattere di tipo simbolico dello strumento più che uno stretto collegamento alla definizione contratto sia in *Common Law* che in *Civil Law*.

In particolare, per quanto riguarda **la natura giuridica** di uno *Smart contract* ci si è interrogati circa **la relazione che intercorre tra l'accordo contrattuale e il protocollo/codice informatico – *software* - sotteso allo *Smart contract.***

A) Da un lato si potrebbe sostenere che gli *Smart contracts* siano in grado di sostituirsi completamente ai "contratti tradizionali" e che il codice informatico che si traduce nello *Smart contract* costituisca, in toto, il contratto.

[45] https://www.diritto.it/i-contratti-point-and-click/

[46] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 274.

Il codice informatico, secondo tale interpretazione, avrebbe forza di legge tra le parti ai sensi dell'art. 1372 c.c. e sarebbe, quindi, autosufficiente, autoeseguito e autoimposto, con la conseguenza che gli *Smart contracts* potrebbero porsi al di là di ogni possibile controllo da parte degli Stati e della relativa giurisdizione legale.

Però ritenere che il codice informatico sia legge equivarrebbe ad affermare che qualsiasi errore, clausola illegale o mancato recepimento di norme imperative diventerebbe parte del contratto, rendendo lo stesso scollegato da ogni tipo di controllo esterno.

B) Argomentando in modo diametralmente opposto, invece, parte della dottrina sostiene che si potrebbe ridurre il ruolo degli *Smart contracts* alla mera automazione dell'adempimento sulla scia di quanto avviene nel settore delle *vending machine*.

Secondo tale interpretazione, il vantaggio che conseguirebbe all'utilizzo degli *Smart contracts* sarebbe limitato unicamente alla digitalizzazione e all'automatizzazione dell'adempimento al verificarsi di determinati eventi.

C) **Un'interpretazione più realistica** degli *Smart contracts*, che ne coglie il più ampio potenziale, **li colloca all'interno del sistema giuridico tradizionale**, sottolineando una discrepanza tra l'accordo delle parti e il protocollo codificato in modo informatico e l'esigenza che gli *Smart contracts* debbano necessariamente integrarsi con ulteriori elementi espressione dell'intenzione e della volontà delle parti.

Quest'ultima interpretazione (c.d. ***split contracting model***) se

- da un lato riconosce che gli *Smart contracts* possono determinare un aumento di efficienza in molti settori (con conseguenti riduzioni di costi di transazione e, ad **esempio** dei tempi necessari per lo svolgimento di attività di verifiche o controlli),
- dall'altro pone l'accento sull'incapacità e la difficoltà di tradurre in un unico codice informatico complesse strutture negoziali.

Seguendo tale ragionamento, si comprende, dunque, come **lo *Smart contract* afferisca non alla fase di formazione del contratto, che è e resta costituita dall'accordo tra le parti, ma a quella**

dell'adempimento del contratto, con la conseguenza che **lo *Smart contract* non integrerebbe neppure una fattispecie di contratto atipico ai sensi dell'art. 1322 c.c.**

Peraltro, se,

- da un lato, l'autonomia contrattuale è preservata in relazione al momento di formazione del contratto,

- dall'altro lato la stessa viene limitata in relazione alla fase dell'adempimento.

N.B. Sono, infatti, **sottratti alla volontà e al controllo delle parti e di soggetti terzi** (e, teoricamente, anche all'immediato sindacato del giudice) **gli elementi riferiti all'adempimento del contratto** che vengono attuati automaticamente al verificarsi delle condizioni prestabilite e inserite nel codice informatico (*if this– then that*).

Come si diceva da una diversa prospettiva, si potrebbe inquadrare lo *Smart contract* come una forma atipica di autotutela, alla luce del fatto che **l'esecuzione automatizzata tutela il privato dall'inadempimento contrattuale di controparte**.

3.5) Le maggiori differenze tra gli *Smart contracts* ed i contratti disciplinati dal codice civile sono:

3.5.a) Nei "normali" contratti **la fiducia** viene garantita da una figura terza, che può essere, per esempio, quella di un notaio o di un avvocato.

Nello *Smart contract*, il ricorso ad una figura terza viene meno.

Risulta tuttavia chiaro che alcune garanzie debbano essere comunque sempre rispettate:

1) il codice informatico non deve essere modificabile,

2) le basi e le fonti dei dati devono essere provate ed affidabili, e

3) le modalità di lettura e controllo delle fonti dei dati devono essere certificate.

Negli *Smart contracts* non c'è spazio per la violazione delle condizioni sottoscritte, dal momento che tra le loro caratteristiche intrinseche ci sono l'esecuzione automatica e l'inalterabilità.

L'accordo negoziale (1325 c.c.), che rappresenta uno dei requisiti essenziali del contratto stesso (1321 c.c.), rimane in capo alle rispettive parti.

Dei requisiti del contratto

Art. 1325. Indicazione dei requisiti.

I requisiti del contratto sono:

*1) **l'accordo delle parti**;*

2) la causa;

3) l'oggetto;

4) la forma, quando risulta che è prescritta dalla legge sotto pena di nullità.

Art. 1321. Nozione.

*Il contratto è **l'accordo di due o più parti** per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale.*

Dovrà esserci, come nei "normali" contratti, una perfetta coincidenza tra la volontà delle parti che dovrà essere tradotta in codice informatico.

3.5.b) L'Accordo delle parti

Operativamente la tecnologia *Blockchain* permetto l'accordo delle parti cioè lo scambio del consenso seguendo almeno **due procedure**:

1) "I comandi" che formano lo *Smart contract*, racchiudendo la prestazione delle parti, sono caricati sulla *Blockchain* e sottoscritti da ciascuna parte rifacendosi ad un sistema di **crittografia** a chiave doppia asimmetrica.

2) Lo *Smart contract*, una volta accertato tramite il procedimento di "sicurizzazione crittografica", è registrato su una *Blockchain* e riceve una "Marca Temporale" – il cosiddetto *hash* – che identifica la data e l'ora della transazione e quindi della prestazione del consenso.

Occorre quindi valutare se la tecnologia *Blockchain* possa legittimare la volontà espressa tra le parti all'atto della sottoscrizione dello *Smart contract*.

Il problema si pone perché lo scambio del consenso avviene attraverso la predisposizione di un codice-comando informatico che le parti chiedono reciprocamente di inserire nello *Smart contract*.

N.B. Lo *Smart contract* contiene una sequenza di stringhe di codici la cui lettura combinata dovrebbe certificare il consenso prestato tra le parti.

N.B. Lo *Smart contract* quando è reso esecutivo sulla *Blockchain* è eseguito indipendentemente dalla legittimità o meno delle clausole-comandi in esso incluse.

Date le caratteristiche appena menzionate, il reciproco incontro fra le volontà può dare luogo ad un contratto od anche ad un contratto preliminare,

Inoltre, esso può avvenire con trattative sia nel mondo reale che virtuale attraverso metodi classici o "*Smart*", escludendo però la fattispecie di conclusione con accettazione o con esecuzione senza proposta, in quanto la tecnologia *Blockchain* non presenta i caratteri di esecuzione di una prestazione senza un accordo in codice.

Il problema in merito alla redazione di un documento informatico, strutturato ed immutabile come uno *Smart contract* è duplice:

1) Da una parte bisogna tenere in considerazione che, la creazione di un documento che rispecchi, con codice informatico, le volontà delle parti, può essere soggetto ad aggiornamenti/variazioni in merito al linguaggio usato che possono portare all'incomprensione della proposta (e quindi potrebbe non sorgere un accordo) oppure alla

fattispecie in cui si compiano delle azioni che sono diverse rispetto alla volontà di una o di entrambe le parti.

2) Dall'altra troviamo la non possibilità di un **<u>mutuo dissenso</u>**.

Esso deriva dall'autonomia negoziale delle parti che si evince nell'art. 1321 del c.c. e nell'art. 1372 (*il contratto ha forza di legge fra le parti e può essere sciolto per mutuo dissenso o per cause ammesse dalla legge*).

La prima affermazione dell'art. 1372 ha quasi un aspetto di legge imprescindibile nell'ambito analizzato poiché, una volta validato, esso si auto-eseguirà sotto le condizioni prestabilite[47].

Tale paradigma può essere risolto[48], in modo univoco con un'altra funzione informatica, che vedremo che fu utilizzata nel caso *The DAO* (più oltre al paragrafo 3.5 f), attivabile dalle parti in maniera simultanea (***kill***) che elimina in maniera totale lo *Smart contract* dalla catena.

Esso può rappresentare la soluzione al mutuo dissenso o al recesso unilaterale nel caso esso fosse attivabile da una sola delle due parti.

Altra possibile opzione sarebbe quella della creazione di uno *Smart contract* "Uguale e Contrario" al precedente, tale da annullare quest'ultimo e mantenerlo all'interno della rete.

Le problematicità appena descritte fanno riferimento all'uso dello *Smart contract* a prescindere dal fatto che esso sia classificabile come contratto o come veicolo per dare luogo alle reciproche prestazioni identificate attraverso un contratto stipulato secondo i metodi tradizionali.

Dell'accordo delle parti

Art. 1326. Conclusione del contratto.

Il contratto è concluso *nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte.*

[47] https://www.dirittoconsenso.it/2021/05/17/automatizzare-pagamenti-con-Smart-contract/

[48] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 306.

Si tenga presente che, a monte, sarà necessario soffermarsi, a seconda di quale sarà il diritto che governa lo *Smart contract* (si veda il paragrafo 3.13) quale principio si applicherà per definire il momento di conclusione dello stesso: di cognizione, di ricezione, di spedizione.

A tal proposito si veda a cura di Marco Tupponi il "Manuale di Diritto Commerciale Internazionale" – III Edizione – Edizioni Giappichelli – paragrafo 3.3.5)

L'accettazione deve giungere al proponente nel termine da lui stabilito o in quello ordinariamente necessario secondo la natura dell'affare o secondo gli usi.

Il proponente può ritenere efficace l'accettazione tardiva, purché ne dia immediatamente avviso all'altra parte.

Qualora il proponente richieda per l'accettazione una forma determinata, l'accettazione non ha effetto se è data in forma diversa.

Un'accettazione non conforme alla proposta equivale a nuova proposta.

MIRROR IMAGE RULE

L'accordo fra le parti è definibile come l'incontro delle volontà su un medesimo contratto, ovvero lo scambio tra proposta e accettazione.

Qui nasce la prima problematicità relativa alla caratteristica della *Blockchain* legata all'immutabilità dei registri, infatti, se all'interno della stessa viene caricato uno *Smart contract* (che può essere destinato ad un solo soggetto tramite identificazione di *account* o *wallet* o all'intera *Blockchain*) esso dovrà essere accettato dal soggetto interessato nella sua interezza utilizzando la propria chiave privata.

Nel caso in cui si volesse effettuare una contro proposta (modificando il contratto di riferimento) l'azione non sarebbe perseguibile a causa dell'immutabilità della *Blockchain*.

La soluzione a tale problema sarebbe quella di **creare una nuova proposta da inoltrare al soggetto che aveva emesso il primo *Smart contract*** (nel caso in cui si parli di destinatario specifico) che creerebbe un'inversione dei ruoli, l'accettante diventa proponente e viceversa.

L'accettazione di un contratto può essere anche tacita attraverso determinate azioni/comportamenti che devono però essere concepiti come "una valida accettazione dell'offerta" come l'invio di un certo ammontare di *criptovaluta* al *wallet* del soggetto proponente (comportamento concludente).

Lo scambio di proposta e accettazione all'interno del sistema *Blockchain* avviene attraverso la risposta ed attraverso messaggi determinati che contengono l'accettazione del tutto conforme alla proposta effettuata dal soggetto proponente seguendo il Principio del ***Mirror Image Rule***.

L'accettazione è valida, quindi il contratto è concluso, quando all'indirizzo elettronico del proponente sopraggiunge l'accettazione, a meno che l'offerente non abbia potuto accedere, non per sua colpa, al sistema informatico.

Poiché la struttura della *Blockchain*, come spiegato al paragrafo precedente, lavora attraverso una replica del registro su tutti i nodi della sua rete si ritiene quindi concluso il contratto quando la ricevuta dell'accettazione raggiunge il nodo dell'offerente/proponente.

Art. 1327 Codice Civile

Qualora, su richiesta del proponente o per la natura dell'affare o secondo gli usi, la prestazione debba eseguirsi senza una preventiva risposta, ***il contratto è concluso nel tempo e nel luogo in cui ha avuto inizio l'esecuzione.***

(Questa è una caratteristica dello *Smart contract* in quanto gli *Smart contracts* sono in grado di riprodurre tale modalità di formazione dell'accordo)

L'accettante deve dare prontamente avviso all'altra parte della iniziata esecuzione e, in mancanza, è tenuto al risarcimento del danno.

Il meccanismo *Blockchain/Smart contract* può quindi creare delle difficoltà per quanto riguarda l'irrevocabilità dell'accordo e quindi l'applicabilità di istituti quali:

- **il recesso** (si pensi ad esempio al diritto al ripensamento ex art. 52 del Codice di Consumo),
- **l'annullabilità,** vedremo più oltre PAG 44 ss.
- **la nullità,** vedremo più oltre PAG 44 ss.
- **la risoluzione,**
- **il mutuo dissenso ante pag. 28**

3.5.c) Un altro tema da gestire e regolamentare è quello della **Responsabilità civile**, dal momento che l'intervento umano è limitato bisogna risalire:

a) a chi ha predisposto l'accordo poi tradotto in codice informatico oppure

b) al professionista informatico che ha tradotto in linguaggio informatico l'accordo: "la scrittura" del codice informatico è infatti in grado di fare scaturire delle conseguenze in seguito al verificarsi di determinate condizioni.

Data la descrizione della *Blockchain* nel capitolo 1 della presente Guida, come un sistema distribuito, decentrale, pseudonomizzato e senza intermediari, vi è un problema di carattere generale e comune alla maggioranza delle tipologie di *Blockchain*, ovvero, **le attribuzioni della responsabilità.**

Con tale tecnologia innovativa si innescano una serie di problematiche legate al collegamento sull'assegnazione e trattamento sulla responsabilità in merito a determinati avvenimenti che potrebbero verificarsi nell'utilizzo della *Blockchain*, come per esempio un malfunzionamento della stessa, inadempimenti collegabili alla controparte della transazione di riferimento o eventuali errori nel completamento di una transazione.

All'interno dell'ordinamento giuridico italiano, come anche in altri ordinamenti, sono presenti VARIE TIPOLOGIE DI RESPONSABILITÀ che è giusto suddividere in prima battuta per meglio comprendere l'aggancio giuridico con le problematicità appena descritte:

- Responsabilità Extra-Contrattuale che è definita secondo l'articolo 2043 del Codice Civile Italiano come "*qualunque fatto doloso o colposo che cagioni ad altri un danno ingiusto*"; tale definizione di responsabilità non fa quindi riferimento ad una responsabilità riconducibile ad una violazione di un rapporto obbligatorio fra le due parti, ma bensì ad una violazione di un dovere di tipo "generico" e che obbliga al risarcimento del danno. Il fatto che causa il danno inoltre può essere distinto in varie tipologie in base alla presenza o assenza di volontà od all'inosservanza di fonti normative.[49]

Nel diritto anglosassone, o di *Common Law*, tale fattispecie è identificata all'interno dell'azione di *trespass* e successivamente dalle azioni di *debt* ed *assumpsit.*

[49] https://www.diritto.it/responsabilita-civile-e-responsabilita-penale-peculiarita-e-differenze/

- Responsabilità Contrattuale che è definita come quella responsabilità, che sorge in capo alle parti, di adempiere alle obbligazioni specificate in un contratto a favore della parte beneficiaria di cui si fa menzione nello stesso.

Essenzialmente esse scatta nel caso in cui non vengano rispettati gli obblighi contrattuali che insorgono in capo alle parti.

Nel diritto anglosassone essa fa riferimento all'istituzione del *contract*, ovvero una promessa vincolante per il diritto se e solo se prevede una *consideration* (vantaggio, beneficio, tolleranza, sacrificio) della controparte o se esso è sotto forma di *deed* (come possono essere le donazioni o le promesse unilaterali)[50].

Detto ciò, si può capire come la responsabilità contrattuale prevede l'identificazione di un soggetto tenuto all'adempimento dell'obbligazione contrattuale.

D'altro canto, la responsabilità extra-contrattuale può essere riferita a tutte quelle fattispecie di interessi tutelati dall'ordinamento (*erga omnes*).

Altra menzione utile è rappresentata dalla **Responsabilità Oggettiva**, ovvero quella responsabilità attribuita dall'ordinamento a prescindere dall'autore materiale del fatto.

Identificate le tipologie di responsabilità, è necessario effettuare un'analisi sulle **tipologie di soggetti che possono intervenire nella *Blockchain***, ovvero:

1. gli utenti, ossia i soggetti che eseguono le transazioni che quindi fanno concludono i rapporti contrattuali;
2. i nodi/*computers*, che garantiscono l'archiviazione del registro;
3. i *miners*, soggetti che convalidano le transazioni registrando le stesse su un blocco.

Prendendo come riferimento una rete *Blockchain* di tipo *Permissionless,* il primo dilemma sull'assegnazione di responsabilità all'interno del sistema *Blockchain* nasce nel momento in cui si manifesta un malfunzionamento della rete.

[50] Marco Tupponi et al, 2019, Manuale di Diritto Commerciale Internazionale - Terza edizione, Giappichelli Editore, Pagina 39.

In tale ipotesi teorica la **responsabilità**, data la definizione dei ruoli dei 3 tipi di soggetti appena menzionati, dovrebbe essere identificata in capo ai nodi/*computers* e ai *miners* che agiscono nella rete in quanto sono essi gli operatori che permettono e regolano il funzionamento della *Blockchain*.

Tale attribuzione di responsabilità fa nascere due tipi di problemi[51]:

1) il primo attribuisce una responsabilità ad un insieme non definito di persone dove, inoltre, non avviene un collegamento diretto tra malfunzionamento e azione dei soggetti adibiti al funzionamento della *Blockchain*;
2) il secondo problema è di fattibilità, ovvero l'alta difficoltà nel rintracciare i soggetti riferibili al 51% della capacità computazionale della *Blockchain* dove si è verificato l'errore.

L'alta difficoltà nell'attribuzione della responsabilità a soggetti non perfettamente identificabili crea un "*passaggio di responsabilità*" all'utente della rete, rendendolo responsabile a tutti gli effetti delle problematicità dovute a transazioni errate e/o malfunzionamenti, seppur con remote possibilità di accadimento, della *Blockchain Permissionless* utilizzata.

Tutto questo, d'altro canto, risulta perfettamente in linea con il principio di decentralizzazione della catena, con l'eliminazione di enti centrali preposti al funzionamento e garanzia del registro (eliminando possibili azioni fraudolente del soggetto centrale).

L'azione migliore che si può porre in essere quindi, risulta identificata nella conoscenza della controparte e nell'attenzione meticolosa a condurre una transazione all'interno della catena, tale da minimizzare il rischio di problematicità.

3.5.d) Le clausole vessatorie

Altra problematica è costituita dalle cosiddette **clausole vessatorie**, disciplinate dal Codice Civile Italiano e dal Codice del Consumo, che rappresentano un ulteriore criticità in termini di tutela del contraente più debole in uno *Smart contract*.

[51] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 88.

Spesso i contratti sono frutto **dell'elaborazione unilaterale da parte di un soggetto che predispone schemi contrattuali uniformi**, destinati ad operare nei confronti della generalità della clientela, prescindendo dunque da una reale trattativa negoziale.

Ipotesi dei contratti in serie, conclusi mediante moduli o formulari (art. 1342 c.c.), o con condizioni generali di contratto (art. 1341 c.c.).

Nei contratti con condizioni generali di contratto le clausole sono predisposte unilateralmente dal contraente più forte, tipicamente sono riferibili ad una limitazione delle garanzie ed al declino della responsabilità e la volontà del contraente più debole è ridotta al minimo in quanto può semplicemente o accettare o rifiutare.

In sostanza, sono **clausole** chiamate "**vessatorie**" perché particolarmente sfavorevoli sia da un punto di vista economico che giuridico.

A tal riguardo, l'ordinamento italiano prevede due diverse discipline: il Codice Civile, se si tratta di clausole vessatorie in contratti B2B e il Codice del Consumo, in caso di contratti B2C.

E' questa la problematica della *gross disparity* che a livello internazionale non viene risolta come dal Legislatore italiano agli artt.. 1341 e 1342 c.c.

Art. 1341. Condizioni generali di contratto.

Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.

In ogni caso non hanno effetto (**nulle**)*, se non sono specificamente approvate per iscritto* (**clausole vessatorie**)*, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze , limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi , tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.*

Art. 1342.

Contratto concluso mediante moduli o formulari.

Nei contratti conclusi mediante la sottoscrizione di moduli o formulari, predisposti per disciplinare in maniera uniforme determinati rapporti contrattuali, le clausole aggiunte al modulo o al

formulario prevalgono su quelle del modulo o del formulario qualora siano incompatibili con esse, anche se queste ultime non sono state cancellate.

Si osserva inoltre la disposizione del secondo comma dell'articolo precedente.

Risultano innegabili le limitazioni che potrebbero sorgere quando si parla di *Smart contract*, ma d'altra parte, considerando un contesto ideale, si potrebbe risolvere il problema alla radice attraverso **il consenso distribuito condiviso con tutti i nodi e convalidato dai miners, che è il meccanismo che sta alla base della *Blockchain*, facendone venire meno, in tal modo, "forse", la vessatorietà**.

La natura informatica, automatizzata e distribuita degli *Smart contracts* presenta, oltre ad interessanti profili applicativi, numerose **problematiche** che originano dalle loro caratteristiche tecniche.

3.5.e) Innanzitutto, va considerata la questione della **lingua nello *Smart contract***.

Per quanto riguarda il **linguaggio in codice informatico**: è necessario che le parti si affidino da un lato ad un esperto informatico in grado di tradurre in codice informatico il testo dell'accordo, dall'altro a **figure giuridiche intermediarie (avvocati – notai)** atte alla corretta trasmissione della volontà delle parti all'esperto informatico, al fine di evitare equivoci o incomprensioni, che comprometterebbero la reale volontà delle parti (anche se si è ben coscienti che l'utilizzo delle figure terze farebbe perdere una delle ragioni per cui si sono creati gli *Smart contracts*).

È evidente che un linguaggio informatico non lascia dubbi o meglio non dovrebbe lasciarli all'interpretazione, mentre un "linguaggio naturale" li potrebbe lasciare più facilmente.

Si tenga presente che tale problematica è molto sentita nel mondo di *Common Law* visto che il primo criterio ermeneutico per interpretare un contratto e quello della letteralità.

Non a caso nei contratti redatti in un ambiente culturale di *Common Law* la prima parte del contratto, dopo le premesse, se il contratto è un pò articolato, è dedicata alle *definitions*.

Nello *Smart contract* il linguaggio umano, infatti, viene sostituito dal codice di programmazione, che rimpiazza la normale comprensibilità, flessibilità e duttilità del linguaggio naturale con la rigida dialettica binaria tra 0 e 1.

Se,

- **da un lato**, il linguaggio informatico consente di comporre un regolamento contrattuale che sia privo delle incertezze e delle ambiguità proprie del linguaggio dell'uomo in quanto il contratto viene strutturato secondo lo schema "se X allora Y" – *IF - THEN*, all'interno del quale le variabili e le condizioni possiedono un solo ed unico significato oggettivo (che, però, non necessariamente coincide con l'intenzione delle parti),

- **dall'altro lato**, l'utilizzo del **codice informatico** – ***coding*** - pone dei dubbi in ordine alla intelligibilità dell'accordo da parte dei contraenti e, conseguentemente, alla validità del consenso da essi prestato specie se sono sprovvisti di particolari competenze in campo informatico e/o appartengono a categorie tutelate (per esempio minori, incapaci).

In particolare, ci si chiede se nel concetto di "libertà di lingua", con il quale si intende la generale libertà dei soggetti privati di scegliere ed impiegare una qualsiasi lingua nello svolgimento della propria attività negoziale, possa essere ricompresa anche la facoltà di adottare il codice informatico come "lingua" del contratto e quali siano i presupposti per l'applicazione della disciplina dei vizi della volontà nell'eventualità di una inesatta rappresentazione del contenuto dell'accordo dovuta all'uso del linguaggio di programmazione.

Un possibile metodo, per superare questo genere di problematiche, è stato rinvenuto nell'idea di connettere, direttamente allo *Smart contract*, un documento contrattuale elettronico, redatto in linguaggio umano, che ne rappresenti e costituisca l'esplicitazione poiché la trasposizione del linguaggio e delle regole del diritto in forma algoritmica rappresenta una tematica di notevole attrattiva, ma non priva di difficoltà.

Il codice informatico, con cui sono stati programmati i contratti all'interno della *Blockchain*, non sono immediatamente comprensibili da parte dell'utente medio; infatti, la quota dei soggetti che hanno conoscenza del linguaggio sono una piccola parte della popolazione utilizzante l'ecosistema *Blockchain*.

In merito a ciò la dottrina prevalente afferma che "per tutelare l'efficienza e la certezza giuridica dei rapporti contrattuali l'accordo dev'essere inteso dal punto di vista esterno di un osservatore ragionevole"; ciò sta a significare che, nei rapporti contrattuali le parti devono valutare in base alla qualità della controparte e adottare le misure più idonee alla propria tutela in modo coerente e farsi carico in modo responsabile della conclusione ultima del contratto.

In merito a fattispecie particolari, ma comunque in preponderanza numerica, derivanti dalla c.d. offerta al pubblico, quindi senza un destinatario precisamente identificato, troviamo i contratti ***Point and Click*** ovvero ***Click Wrap***[52].

Essi rappresentano dei contratti che trovano la loro **conclusione attraverso la pressione di un pulsante o icona digitale**; come si può notare dunque, tali contratti devono presentare una maggiore specificità rispetto al solo codice informatico per una chiarezza maggiore verso il pubblico a cui è rivolta.

In maniera specifica tali contratti sono identificati e regolamentati all'interno di diverse dottrine come la *Click-Trough Agreement* elaborata dall'*American Bar Association* o come la Direttiva comunitaria 2009/136/CE, che convergono in diversi punti per una validità di tali contratti, ovvero:

1. Vi dev'essere la facoltà di esaminare i termini dell'accordo prima o contestualmente all'invio dell'accettazione per *click.*
2. Si devono presentare modalità trasparenti di informativa circa i termini dell'accordo, con contenuto e forma in linea con le norme in vigore
3. Ci deve essere un'assenza di ambiguità nella possibilità di accettazione o rigetto dei termini dell'accordo con espressa comunicazione dell'avvenuta accettazione al soggetto accettante
4. Ci deve essere la conservazione di dati inerenti all'accordo telematico con eventuale trattamento e protezione degli stessi nel rispetto delle normative vigenti.

Da ciò che si è appena spiegato tali disposizioni sono del tutto sovrapponibili agli *Smart contracts* in quanto essi possono essere proposti, potenzialmente, univocamente con codice informatico non facilmente comprensibile da parte di un soggetto medio utilizzatore dell'ecosistema *Blockchain.*

[52] https://rivista.camminodiritto.it/articolo.asp?id=6704: la dottrina li definisce come gli accordi in forma elettronica predisposti unilateralmente e conclusi con la pressione di bottoni o icone elettroniche o tramite la digitazione di parole o frasi.

Da ciò il proponente deve quindi accompagnare la propria offerta al pubblico con una versione del testo in codice in un linguaggio comprensibile dall'utente medio, come per esempio la lingua utilizzata dall'eventuale gruppo identificato.

In tali contratti predisposti unilateralmente vi si accede attraverso una procedura particolare già riscontrata in altri contratti telematici, da ciò ne consegue che essi possono essere indirizzati verso il medesimo quadro normativo nazionale ed internazionale[53].

Anche negli *Smart contracts* quindi, come abbiamo analizzato, vige l'accettazione in qualunque forma (eliminando il caso della controproposta non attuabile), ed essa è distinguibile in due tipologie[54]:

1. *Bilateral Contract*: con cui si identifica l'accettazione con manifestazione espressa.
2. *Unilateral Contract*: con cui si identifica l'accettazione attraverso l'esecuzione di una specifica prestazione per effettuare un'accettazione valida. (Caso dei c.d. *Click-Wrap)*

Si vuole ribadire, richiamando ancora l'attenzione che esprimere un contratto in forma algoritmica comporta l'introduzione di un nuovo insieme di **criticità**, che consistono nell'eventualità che il codice informatico illustrante l'accordo sia affetto da errori, difetti o vulnerabilità, causati ad **esempio** da errori di sintassi nel **codice informatico**, che possono portare il programma ad un'inesatta interpretazione dei requisiti necessari per effettuare una determinata azione, o che possono dare agli utenti (le parti del contratto) la possibilità di porre in essere comportamenti illegittimi.

3.5.f) A tal proposito, il riferimento forse più significativo riguarda **il caso *The DAO*, una piattaforma partecipativa per la raccolta di capitale di rischio, costituita attraverso uno *Smart contract* collocato sulla *Blockchain Ethereum*.**

Con l'acronimo *DAO* si identifica la categoria delle *Decentralized Autonomous Organizations*: entità che risiedono su di un registro distribuito - DLT – *Blockchain* -, le cui attività sono svolte in

[53] Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I)

[54] Marco Tupponi et al, 2019, Manuale di Diritto Commerciale Internazionale - Terza edizione, Giappichelli Editore, Pagina 85.

parte autonomamente dal *software* e in parte mediante l'apporto, riservato soprattutto alle questioni decisionali, di soggetti umani.

Nel maggio del 2016, alcuni componenti della comunità *Blockchain* hanno utilizzato le possibilità tecniche offerte da *Ethereum* per realizzare una *Decentralized Autonomous Organization*, denominata «*The DAO*», con lo scopo di **raccogliere fondi, in forma di *cryptovaluta***, da destinarsi al finanziamento di attività sia commerciali sia senza scopo di lucro.

Tuttavia, ad appena un mese di distanza dal lancio della piattaforma, che in questo breve lasso di tempo aveva ricevuto un ammontare di *cryptovaluta* per un valore superiore ai 150 milioni di dollari, **uno dei partecipanti**, sfruttando una vulnerabilità del codice informatico impiegato per realizzare lo *Smart contract* sul quale poggiava *The DAO*, **è riuscito ad appropriarsi indebitamente** di più di un terzo dei fondi, determinando, alla fine dei conti, il fallimento di tutta l'iniziativa.

La vicenda, come pure le misure che sono state adottate nel tentativo di mitigarne gli effetti più negativi, offre alcuni fondamentali spunti di riflessione.

Si è detto che i **trasferimenti** stabiliti in uno *Smart contract* sono **irrevocabili**, **irreversibili** e **immutabili**, in quanto vengono eseguiti dal sistema in via automatica al verificarsi delle condizioni previste dallo stesso *Smart contract*, senza che alcun intervento umano possa impedirli o modificarli.

Proprio in ragione di questa mancanza di flessibilità, risulta di importanza primaria che **il codice informatico alla base dello *Smart contract*** sia:

a) **da un lato**, esente da anomalie o vulnerabilità e,

b) **dall'altro**, in grado di rappresentare fedelmente l'assetto di interessi che le parti intendono effettivamente realizzare.

In proposito, alcuni autori hanno suggerito di utilizzare le **tecniche della verifica formale anche con riferimento agli *Smart contracts***, ritenendo che tali procedimenti siano in grado di prevenire il ripetersi di eventi analoghi al caso *The DAO*.

Allo stesso tempo, però, occorre rilevare come gli stessi caratteri dell'irrevocabilità, dell'irreversibilità e dell'immutabilità non siano del tutto assoluti.

La regola fondamentale che governa la *Blockchain* (e quindi, di riflesso, anche gli *Smart contracts*) **è quella del consenso distribuito**; essa funge da presidio e garanzia della ***trustless*** (assenza di fiducia) sulla quale si fondano tali sistemi.

La fiducia tra le parti non è necessaria, perché è data dal sistema informatico e dall'attività dei *miners*.

Detta regola, tuttavia, presenta anche **un lato negativo**: infatti, almeno in linea teorica, consente di modificare o cancellare una transazione già effettuata sulla *Blockchain*, **solo a condizione che** detto intervento incontri l'approvazione di un numero di partecipanti al sistema, capace di esprimere la **maggioranza ai sensi del meccanismo di consenso distribuito utilizzato.**

Per quanto riguarda le architetture *Blockchain* basate su algoritmi di consenso di tipo *Proof-of-Work* (ad oggi ancora il più diffuso), **il concetto di maggioranza è determinato non per teste, ma in relazione alla quota di potenza elaborativa immessa da ciascun soggetto nel sistema (è l'attività dei *miners*).**

È questa la strada che, non senza notevoli resistenze e soltanto a seguito di un lungo dibattito, si è scelto di percorrere con riferimento alla vicenda *The DAO*.

La maggioranza dei partecipanti alla *Blockchain Ethereum*, riscontrata l'insufficienza e l'impraticabilità tecnica di interventi meno invasivi, si è accordata **per "riscrivere"** il registro delle transazioni - DLT, **eliminando – *kill*** - l'operazione con la quale era stata distratta una parte dei fondi raccolti da *The DAO* e ripristinando lo *status quo ante*.

La decisione, del tutto estrema ed eccezionale, **ha suscitato numerose critiche**, dovute soprattutto alla considerazione che in tal modo si è deliberatamente sacrificato il principio, da molto ritenuto imprescindibile, della certezza ed immodificabilità delle transazioni, provocando un'inevitabile crisi di fiducia.

3.6) Vizi nella Formazione dello *Smart contract*

Se lo *Smart contract* fa salva l'autonomia delle parti nella fase di formazione del consenso e, al pari di qualsiasi contratto, è basato su una manifestazione di volontà, può verificarsi che la formalizzazione di tale volontà manifestata esternamente **non** corrisponda al vero intento negoziale del dichiarante.

L'ordinamento italiano, come anche gli altri Ordinamenti, considera e disciplina tali scenari, prevedendo che i contratti conclusi da un contraente il cui **consenso sia stato dato per errore, estorto con violenza morale o carpito con dolo** possano essere annullati su richiesta del medesimo contraente alle condizioni di cui agli **artt. 1427 ss. c.c.,** ossia quando:

1. l'**errore** è essenziale ed è riconoscibile dall'altro contraente (**art. 1428 c.c.**),
2. la **violenza** prospetta un male ingiusto e notevole (**art. 1435 c.c.**)
3. il **dolo** è determinante per la conclusione del contratto (**art. 1439 c.c.**).

Al riguardo, per gli *Smart contracts* potrebbe assumere particolare importanza la disciplina sul c.d. **errore ostativo** di cui **all'art. 1433 c.c**. che, consentendo l'annullamento del contratto quando **l'errore riguarda non la formazione della volontà (errore vizio), ma la dichiarazione della volontà**, porrebbe un rimedio per tutte quelle situazioni in cui il codice informatico non trasponga correttamente la volontà delle parti.

Inoltre, a tutela di soggetti considerati particolarmente vulnerabili dall'ordinamento, il codice civile, **all'art. 1425**, sancisce anche l'annullabilità del contratto concluso **dall'incapace legale** e, in presenza delle condizioni di cui **all'art. 428 c.c**., dall'incapace naturale.

Tuttavia, se tali meccanismi di tutela trovano normale applicazione con riferimento ai "contratti tradizionali", **occorre invece interrogarsi circa la loro possibile applicazione agli *Smart contracts* qualora ricorrano le condizioni allo scopo previste dall'ordinamento.**

Si ricordi che la conseguenza che uno *Smart contract* utilizzi una piattaforma ***Blockchain*** è la **immodificabilità** della stessa **impedendo di fatto l'eccezione di inadempimento ex art. 1460 c.c.**

Art. 1460 Codice Civile

Nei contratti con prestazioni corrispettive, ciascuno dei contraenti può rifiutarsi di adempiere la sua obbligazione, se l'altro non adempie o non offre di adempiere contemporaneamente la propria, salvo che termini diversi per l'adempimento siano stati stabiliti dalle parti o risultino dalla natura del contratto.

Tuttavia non può rifiutarsi la esecuzione se, avuto riguardo alle circostanze, il rifiuto è contrario alla buona fede.

L'unica strada possibile in questo caso per eliminare **lo *Smart contract* viziato** è la **procedura *kill* (di autodistruzione), prevista per esempio dalla *Blockchain Ethereum***.

Solo il nodo che ha creato il contratto può azionare tale funzione inoltrando un nuovo accordo tra le parti ed immettendo nella *Blockchain* il corrispondente codice autodistruttivo elettronicamente firmato.

La conseguenza della immodificabilità dello *Smart contract* veicolato tramite *Blockchain* è che **le parti non possono esperire "soluzioni di risoluzione del contratto"**, ma solo "**rimedi restitutori" (*restitutio in integrum***) adempiendo cioè ad una prestazione in forma specifica o per equivalente, ove ciò sia possibile.

Ulteriori problemi in relazione alla **capacità di agire e corretta formazione della volontà contrattuale riguardano la possibilità di verificare l'identità della parte contraente** (si veda il capitolo 1 della presente Guida).

Infatti, esaminate le caratteristiche degli ***Smart contracts***, è evidente che gli stessi non possano essere ricondotti facilmente a una persona fisica o giuridica, **considerata la possibilità di agire in via anonima o sotto pseudonimi.**

Per ovviare a ciò si è pensato ad una *Blockchain* "identificativa" che, però ancora operativamente non è stata realizzata.

Da ciò consegue la difficoltà di riuscire a stabilire:

1) se le parti contraenti avessero o meno la capacità d'agire al momento della conclusione del contratto e

2) se la relativa volontà contrattuale sia stata eventualmente viziata.

Pertanto, nonostante sia ormai indiscussa la possibilità di concludere contratti, e quindi anche *Smart contracts*, per via informatica, tenuto conto della diffusione sempre maggiore del commercio elettronico, non si può escludere il rischio che il codice informatico non contenga una corretta trasposizione della volontà della parte contraente e vi siano differenze tra l'accordo contrattuale e la traduzione nell'algoritmo.

La sussistenza di un errore di programmazione, la presenza di una vulnerabilità informatica o anche il semplice verificarsi di una circostanza non prevista possono determinare esiti quasi irreversibili, in considerazione della notevolissima difficoltà e del prezzo (in termini di perdita di credibilità) che una riscrittura delle transazioni contenute nella *Blockchain* comporta per l'intero sistema.

In concreto, gli unici interventi che le parti possono operare su di uno ***Smart contract,* già formalizzato**, rischiano di essere (soltanto) quelli già esplicitamente contemplati, *ab origine*, nell'accordo stesso, con l'inevitabile conseguenza, specialmente con riferimento ai rapporti contrattuali più complessi, di un notevole incremento dei costi negoziali o, addirittura, della sostanziale impossibilità di ricorrere ad uno *Smart contract*.

Le parti, infatti, devono regolare preventivamente e specificatamente tutte le circostanze che possono astrattamente verificarsi: perciò, in ipotesi di accordi non facilmente standardizzabili, i

contraenti potrebbero trovarsi a dover sopportare costi ed oneri molto superiori rispetto a quelli che avrebbero sostenuto optando per un contratto tradizionale.

Sempre ragionando in questa prospettiva, non si può fare a meno di rilevare come l'inflessibilità degli *Smart contracts* incida profondamente anche sull'applicabilità delle regole e dei rimedi previsti dall'ordinamento in relazione alle diverse forme di **patologia del contratto**.

L'automaticità dell'esecuzione, unita con la non modificabilità delle transazioni, comporta, **ad esempio**, il pericolo che gli effetti di una eventuale **sentenza di nullità o annullamento** restino puramente teorici, in quanto le prestazioni contenute nello *Smart contract* verranno comunque eseguite dal sistema, dal momento che, **anche in presenza di un contratto invalido, la possibilità di non adempiere resta esclusa in radice.**

Esaminiamo in particolare alcune patologie che sono presenti nei contratti "tradizionali" e come sono gestibili in uno *Smart contact*.

1) **Nullità totale**: la nullità è un concetto tipico del contratto[55] tradizionale e trova applicazione per diverse cause, che elencheremo a seguire, e comporta la considerazione del contratto come se esso non fosse mai esistito.
    a. La prima casistica identificata è quella della nullità nel caso in cui il contratto sia contrario a norme imperative. Ciò che potrebbe permettere la nullità di uno *Smart contract* risiede proprio nella sua capacità di "capire" determinate situazioni. L'ipotesi[56] sostenuta è rappresentata dalla possibilità di includere nella programmazione determinati algoritmi che permettano, al verificarsi delle condizioni di violazione di norme imperative, la riduzione in pristino[57] alla fase antecedente

[55] https://www.brocardi.it/codice-civile/libro-quarto/titolo-ii/capo-xi/art1418.html#:~:text=Dispositivo%20dell'art.,1418%20Codice%20Civile&text=Il%20contratto%20%C3%A8%20nullo%20quando,legge%20disponga%20diversamente(1).&text=Il%20contratto%20%C3%A8%20altres%C3%AC%20nullo,%2C%202744%5D(3).

[56] Smart contract e patologia contrattuale: l'ipotesi della nullità: Donato Silvano Lorusso, Nicolino Gentile e Iacopo De Totero.

[57] https://www.brocardi.it/dizionario/1360.html

all'inizio dell'esecuzione sia in ambito *on-chain* che *off-chain* attraverso i c.d. Oracoli (si veda più oltre il paragrafo 3.7).

b. Nel caso in cui la nullità sia identificata attraverso l'assenza dei requisiti previsti dal 1325 (accordo, oggetto, causa e forma), vi sono diverse ipotesi differenti in base alla specifica mancanza:

i) <u>Forma</u>: essendo libera nel caso in cui vi sia la richiesta della forma scritta per quel determinato contratto pena nullità, la codificazione è, secondo le interpretazioni odierne della dottrina intellegibile da parte dei redattori e da parte di soggetti terzi poiché le funzioni e gli algoritmi rappresentano un univoco e certo comando a cui seguono degli effetti prestabiliti. Essa, dunque, rappresenta una forma idonea per tutte le fattispecie e presenta, inoltre, una maggior certezza della prestazione in quanto non ammettono sfumature interpretative e/o attenzioni meramente soggettive derivanti dalla lingua umana (con cui si redigono i contratti tradizionali) o dal comportamento umano.

ii) <u>Causa e motivo</u>: nel caso in cui la causa "*meritevolezza dell'interesse perseguito dai contraenti*[58]" o il motivo (interesse comune di entrambe le parti) intrinseco nello *Smart contract* fosse illecito la dottrina rimanda all'azione di riduzione in pristino stabilita ex-ante attraverso il linguaggio di programmazione e, se non previsto, si potrebbe, come già illustrato, utilizzare la formula del *Reverse Smart contract* uguale e contrario per annullarne gli effetti.

iii) <u>Determinatezza, Possibilità o Illiceità dell'Oggetto</u>: nelle prime due fattispecie lo *Smart contract* elimina in modo netto la possibilità che si verificano tali condizioni in quanto esso può avere luogo se e solo se sono identificati (e dunque possibili) gli oggetti, nel mondo *on/off chain*, oggetto di modifica *if-then*.

Invece l'illiceità dell'oggetto è dunque sempre possibile, nulla vieta di concludere un contratto, e dunque uno *Smart contract* con oggetto illecito.

La soluzione in sede pregiudiziale è la medesima del *Reverse Smart contract*.

In merito alla impossibilità sopravvenuta dell'oggetto in questo caso è necessario, per dare esecuzione allo *Smart contract* (o la parte restante che non ha avuto esecuzione), dare informazione della vicenda *on/off chain*.

iiii) <u>Carenza dell'Accordo</u>: data la metodologia di approvazione la conclusione ed esecuzione dello *Smart contract*, cioè l'incontro tra proposta e accettazione (non trova luogo la controproposta in quanto vi è solo la possibilità di accettare/rifiutare la proposta) avviene in modo unico ed identico

[58] https://www.altalex.com/documents/altalexpedia/2016/02/29/causa#_Toc444157893

in quanto lo *Smart contract*, in linea teorica, non permette la non coincidenza fra le volontà delle parti, trascritta sottoforma di codice informatico.

2) **Nullità parziale**: in merito alla nullità parziale, essa non porta in automatico la nullità dell'intero contratto nel caso in cui le parti, anche in mancanza della stessa, hanno il medesimo interesse nel concludere il contratto anche in presenza di essa (principio di conservazione del contratto).

In merito a tale fattispecie si identificano due criticità[59]:

la prima è data dalla sostituzione con norme imperative delle clausole soggette a nullità. Esse potrebbero essere applicate attraverso Oracoli coercitivi ed esterni;

la seconda è riferita alla volontà delle parti nel proseguire anche senza le suddette clausole. A tal proposito si potrebbe far riferimento al testo redatto in lingua "tradizionale" che potrebbe fungere da volontà contrattuale che enfatizzi l'intenzione principale dell'intero contratto e dunque accettare o meno l'assenza delle clausole oggetto di nullità (per esempio una clausola che dica, tradotta ovviamente in algoritmi: " *le parti dichiarano che se dopo la conclusione del contratto riscontreranno una o più clausola nulle nel presente contratto saranno nulle esclusivamente tali clausole, mentre il restante contratto produrrà i propri effetti*".

L'azione di nullità, sia parziale che totale, può essere "*fatta valere da chiunque vi abbia interesse (art. 1421 del c.c.) ed è imprescrittibile (art. 1422 del c.c.)*[60]" e sarà il giudice ad effettuare la sussistenza di cause di nullità o meno.

A tal proposito si può pensare di redigere un documento interpretativo dello *Smart contract* che ne enunci effetti ed intenzioni.

3) **Annullabilità**: tale azione è ammessa quando si ha un "vizio del consenso (art.1427), incapacità legale (intendere e di volere – ab origine) (art. 1425), o per avere indotto il consenso con errore, violenza morale o dolo. L'azione di annullamento si prescrive in cinque anni dalla scoperta[61]".

[59] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 324.

[60] https://www.altalex.com/documents/altalexpedia/2016/05/05/nullita

[61] Dispositivo dell'art. 1442 → LIBRO QUARTO - Delle obbligazioni → Titolo II - Dei contratti in generale → Capo XII - Dell'annullabilità del contratto → Sezione III - Dell'azione di annullamento

Una fattispecie particolare relativa agli *Smart contracts* avviene se l'annullabilità è conseguente ad un c.d. errore di calcolo[62]. In questa ipotesi l'annullabilità potrà essere rilevata solo nel caso in cui l'errore di calcolo non riguardi la quantità (esempio: conoscenza errata del prezzo di un bene).
In tutti i casi di errore rettificabile si ha che lo *Smart contract*, nel caso in cui sia prevista una modifica unilaterale, può, in modo parallelo ad un contratto tradizionale, preservare l'attività contrattuale ai sensi dell'articolo 1432 del Codice Civile.
Le tre fattispecie appena descritte (nullità totale, nullità parziale ed annullabilità, però risultano in antitesi con quello che rappresenta, attualmente, lo *Smart contract* ed il suo carattere *Self-Executing.*

In particolare, la possibilità che si presentino delle azioni di Nullità e/o Annullabilità al vaglio di un Giudice o un Arbitro (con i rispettivi termini per l'azione stabiliti dalla legge[63]), è direttamente proporzionale alla facoltà delle parti di agire sul flusso di azioni relative allo *Smart contract* sotto forma di contratto.

La esecuzione ineluttabile dello *Smart contract*, nel caso si verifichino tutte le condizioni prestabilite nel codice informatico, non permette la possibilità materiale di effettuare un "dietro-front" o uno "stop" rispetto alla "corsa" che lo "*Smart contract*" sta compiendo sui "binari" della *Blockchain*.

Una soluzione possibile[64] potrebbe essere quella di dedicare un determinato lasso temporale alla verifica delle azioni poste in essere dal meccanismo a tutela del contraente debole (anche in relazione alla sua conoscenza del linguaggio di programmazione); tale opzione però, deve essere condivisa dalle parti e programmata fin dall'inizio.

Altra possibile soluzione per sopperire a tale problema sarebbe quella della creazione, come già affermato in precedenza, di "Oracoli coercitivi", quindi elementi esterni allo *Smart contract*, di specifiche disposizioni (con un immaginabile discrezionalità aggiunta dall'intelligenza artificiale) che comunichino e modifichino lo *Smart contract* a determinate condizioni.

4) Rescissione e Risoluzione di uno *Smart contract*:

[62] https://www.laleggepertutti.it/codice-civile/art-1430-codice-civile-errore-di-calcolo

[63] Nullità: Senza prescrizione – Annullabilità prescrizione ordinaria, in 5 anni.

[64] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 328

In merito alla tematica della **Rescissione** "La rescissione è un'azione che spetta al contraente, che abbia stipulato a condizioni svantaggiose, in quanto il suo consenso è stato estorto in uno stato di pericolo (art. 14479 o in uno stato di bisogno (art.1448)[65]. Tale azione ha come obiettivo, non tanto l'invalidità del contratto, ma l'equità del contratto[66].
A tal proposito la dottrina a supporto indica come possibile soluzione l'inclusione, nel caso si verifichi un'*ultra dimidium,* di specifiche condizioni che, previste nello *Smart contract*, possa riportarlo in condizione di Equità Contrattuale.

La pronuncia di **Risoluzione del contratto**, così come dettato dall'art. 1453 c.c. produce un effetto liberatorio *ex-tunc* e rappresenta anche una delle colonne portanti degli *Smart contracts* in quanto molto più automatizzati dei contratti "tradizionali".

L'azione è esercitabile attraverso quattro metodologie: la lettera di diffida, il processo civile, la clausola risolutiva espressa ed il termine essenziale.

La Risoluzione si può verificare[67] per:

1) **Inadempimento di una delle due parti**: quando avviene la parte adempiente ha il diritto alla risoluzione o all'adempimento ed al risarcimento del danno.

Notiamo che, data la struttura programmabile di uno *Smart contract*, tale fenomeno può essere incluso attraverso una funzione automatizzata *if/then* (gestione contrattuale della controversia).
La risoluzione per inadempimento contrattuale vale se e solo se la prestazione oggetto di inadempienza sia non di scarsa importanza ex art. 1455 c.c..
In tal caso le parti potrebbero convenire nel redigere una *white/black list* per la classificazione delle obbligazioni all'interno del documento informatico.
L'effetto della risoluzione ha effetto retroattivo e quindi, di conseguenza devono essere inficiate tutte le azioni poste in essere dallo *Smart contract*, con relativo risarcimento del danno.
2) **Diffida ad adempiere** ex art. 1454 c.c.[68]: anch'essa è implementabile attraverso un'operazione di *intra Smart contract*, specificatamente attraverso l'inclusione di invio e notifica della diffida al

[65] https://www.altalex.com/documents/altalexpedia/2016/05/05/rescissione-del-contratto

[66] https://www.dirittoprivatoinrete.it/rescissione.htm

[67] https://www.studiolegale-online.net/contratti_r01.php

verificarsi della condizione. Il termine, al decorrere del quale, si procede ad inviare la diffida potrebbe essere implementato manualmente o assoggettarlo ad una fonte esterna (Oracolo) e dunque ad una serie di dati e informazioni derivanti da prassi di settore utilizzando i dati attingibili e selezionabili dai *Big Data* (ad esempio sentenze) di settore.

3) **Clausola Risolutiva Espressa ex art 1456 c.c. (e Termine Essenziale ex art. 1457 c.c.)**: è una clausola che permette la risoluzione del contratto nel caso in cui non si esegua una determinata obbligazione secondo le modalità previste. Anch'essa è implementabile attraverso le precitate soluzioni.

4) Impossibilità sopravvenuta ex artt. 1463 ss. c.c.: in merito ad essa gli *Smart contract* non trovano particolari limiti di applicazione. Essa avviene quando la prestazione diviene impossibile (es. perimento del bene in un contratto di vendita) e quindi si dovrà restituire la controprestazione se già posta in essere. L'impossibilità, così come l'impossibilità parziale[69], all'interno degli *Smart contracts* è un qualcosa di possibile[70] poiché essi sono in grado di comunicare con l'esterno attraverso Token (che analizzeremo più avanti) e Oracoli.

5) Eccessiva onerosità sopravvenuta ex art. 1467 c.c.: l'ultimo caso di risoluzione è quello dell'eccessiva onerosità. In questa ipotesi possono essere inseriti dei limiti superati i quali essi giustifica la risoluzione del contratto.

La natura degli *Smart contracts* ha come elemento fondante dati, condizioni e quindi numeri che ben si prestano nell'affrontare tale tematica.

Le precedenti soluzioni possono essere adottate per tutti quei casi di Eccezione d'inadempimento (condizione affinché si adempia) e Mutamento delle condizioni patrimoniali (tali da pregiudicare l'esecuzione – con *scoring, rating*, assicurazioni e garanzie *on/off chain*)

In termini diversi, si può affermare che gli *Smart contracts* realizzano un'inversione del paradigma tradizionale del diritto contrattuale: «*from ex post authoritative judgment to ex ante automated assessments*».

---

[68] **Art. 1454** *Alla parte inadempiente l'altra può intimare per iscritto di adempiere in un congruo termine, con dichiarazione che, decorso inutilmente detto termine, il contratto s'intenderà senz'altro risoluto. Il termine non può essere inferiore a quindici giorni, salva diversa pattuizione delle parti o salvo che, per la natura del contratto o secondo gli usi, risulti congruo un termine minore. Decorso il termine senza che il contratto sia stato adempiuto, questo è risoluto di diritto.*

[69] Art. 1464 c.c. prestazione di una parte è divenuta solo parzialmente impossibile, l'altra parte ha diritto a una corrispondente riduzione della prestazione da essa dovuta, e può anche recedere dal contratto [1373] qualora non abbia un interesse apprezzabile all'adempimento parziale [1181]

[70] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 341

Resta, tuttavia, il problema di contemperare le rigidità di un meccanismo concepito «[*to*] *eliminate the act of remediation, by admitting no possibility to breach*», che trasla e comprime tutte le possibilità di intervento sul contratto nel momento della stipula, con la necessità di assicurare un efficace controllo giudiziario a posteriori.

Detto bilanciamento (il controllo giudiziario a posteriori) è ineliminabile: sarebbe, infatti, impensabile rinunciare alle tutele e alle garanzie offerte dall'ordinamento in nome di un'autonomia negoziale assoluta ed illimitata.

Sarebbe, inoltre, vano pensare, come dimostra il caso *The DAO*, che le parti possano sempre essere in grado di regolare a priori tutti gli elementi capaci di incidere sul proprio rapporto contrattuale, siano essi relativi a difetti, o vulnerabilità del codice informatico, o dovuti, più in generale, al verificarsi dell'imprevisto o dell'imprevedibile.

Questo rovesciamento di prospettive comporta, sempre restando nell'esempio di un **contratto dichiarato nullo o annullato**, una notevole difficoltà nel ristabilire lo *status quo ante* (**nullità *ex tunc***), data l'inalterabilità dei sistemi *Blockchain* ad ogni intervento di modifica del registro delle transazioni - DLT.

Ciò determina il rischio che **non sia possibile** riportare la sfera giuridica delle parti nella situazione in cui si sarebbe trovata se lo *Smart contract* non fosse stato mai concluso.

Infatti, sebbene possano certamente ipotizzarsi **rimedi di tipo restitutorio o risarcitorio** (come l'obbligo di concludere un nuovo *Smart contract* che inverta i trasferimenti effettuati dal precedente), gli effetti restano, comunque, profondamente differenti nella sostanza: **una cosa è rifiutarsi di eseguire un contratto invalido, altra è chiedere (ed ottenere) la ripetizione di quanto già prestato.**

Basti soltanto pensare al caso in cui **un bene trasferito in esecuzione di uno *Smart contract* che poi è stato risolto, ma sia già stato ritrasferito, con un successivo *Smart contract,* a terzi di buona fede**.

Conciliare adeguatamente le esigenze della certezza ed immodificabilità delle transazioni *Blockchain* con il necessario rispetto delle garanzie e delle forme di tutela prescritte dagli ordinamenti giuridici rappresenta una delle prove più impegnative alle quali è chiamato a rispondere il legislatore.

Sotto un ulteriore profilo, l'ambiguità del codice informatico rende notevolmente complessa l'inserzione, in uno *Smart contract,* di **clausole contrattuali o espressioni volutamente o necessariamente dubbie o vaghe,** cui le parti possono voler ricorrere qualora non siano in grado di predeterminare esattamente il contenuto delle reciproche prestazioni.

Per esempio: "tempo ragionevole", "oggetto determinabile", "eventi straordinari ed imprevedibili", ecc… Anche in questi casi una soluzione possibile è quella di ricorrere ad Oracoli esterni al meccanismo *Blockchain – Smart contract.*

Infatti, nel caso in cui il rapporto negoziale richieda un certo livello di astrazione o di flessibilità nel valutare situazioni esterne, oppure la successiva condotta dei contraenti, potrebbe risultare impossibile, o semplicemente troppo impegnativo, traslare simili variabili in espressioni stimabili da un programma informatico, salvo, come si diceva, l'utilizzo degli Oracoli.

Nel caso di "avvenimenti straordinari ed imprevedibili", presupposto della **Forza Maggiore**, potrebbe venire in aiuto (anche in Italia dal marzo 2020) la dichiarazione che, normalmente le Camere di Commercio od altri Enti pubblici in tutto il Mondo, fungendo da Oracoli (a seguire nel prossimo paragrafo 3.7 il loro inquadramento), rilasciano dichiarando la straordinarietà ed imprevedibilità dell'avvenimento e quindi giustificando l'eventuale inadempimento contrattuale.

Lo stesso documento potrebbe essere utile anche per rinegoziare la prestazione oggetto dello *Smart contract* se è intervenuta un'ipotesi di ***hardship***.

3.7) L'Oracolo

Uno *Smart contract* consiste in un insieme di clausole, espressione di un accordo tra due o più parti, che sono programmate in codice alfanumerico.

Il "Codice Informatico" rappresenta un *set* di istruzioni con la descrizione di condizioni al verificarsi delle quali vengono automaticamente attivate specifiche azioni, anch'esse definite nel codice informatico.

Come abbiamo visto il Codice Informatico viene conservato sulla *Blockchain*, così come le transazioni sono preservate normalmente su altre catene di controllo.

Il segnale che determina l'esecuzione delle istruzioni registrate nello *Smart contract* può dipendere da variabili interne allo stesso, e cioè:

1) dalla successione di avvenimenti già compresi all'interno del codice informatico (come, ad esempio, lo spirare di un termine) oppure

2) da circostanze esterne (per esempio, un tasso di interesse).

In tale seconda ipotesi è necessario l'intervento di un **elemento esterno alla *Blockchain*** (il c.d. "**Oracolo"**) che costituisce un **collegamento tra la *Blockchain* e il mondo reale** e permette la verifica del soddisfacimento delle condizioni esterne.

Ogni volta che un Oracolo si collega alla *Blockchain* e registra informazioni sui blocchi della catena, uno *Smart contract* può eventualmente corrispondere pagamenti anche in *token* (si veda il paragrafo 2.3 della presente Guida).

I *token* diventano incentivi a registrare, implementare e verificare informazioni sulla *Blockchain* in quanto arricchiscono di informazioni e di *know-how* gli attori coinvolti nelle "transazioni" commerciali.

Esistono **due grandi classificazioni per gli Oracoli *Blockchain*** a seconda della fonte da cui si ottengono questi dati.

Oracoli *software*: questi sono gli Oracoli più diffusi e funzionano collegati a fonti di informazioni *online* come *database*, *server*, pagine *Web*, ecc.

Oracoli *hardware*: questi Oracoli funzionano se collegati a fonti di informazione nel mondo fisico, come *scanner* di codici a barre o sensori elettronici, e "traducono" gli eventi del mondo reale in valori digitali in modo che possano essere compresi da uno *Smart contract*.

Evidenziamo alcuni esempi:

1) uno *Smart contract* può essere utilizzato nella fornitura e nel pagamento di energia elettrica: al consumo registrato dal **contatore** (che, in questo caso, rappresenta **l'Oracolo** che collega il codice informatico alla realtà esterna) ne consegue una bollettazione precisa ed un puntuale pagamento della fattura.

2) Uno *Smart contract* prevede il pagamento automatico di una certa cifra da A verso B come corrispettivo per una merce che B fornisce ad A.

In questo caso la gestione del pagamento è interamente effettuata sulla base di informazioni presenti sulla *Blockchain* stessa (verificare che A abbia abbastanza fondi per effettuare il pagamento).

Tuttavia, la semplice logica presente in questo *Smart contract* (se A riceve la merce si proceda al trasferimento delle somme da A a B) necessita di un'informazione che non è presente sulla *Blockchain* e cioè il fatto che A abbia ricevuto la merce.

Alcune piattaforme *Blockchain* utilizzano pertanto la figura dell'Oracolo per risolvere tale problema, in tal caso l'Oracolo potrebbe essere collegato all'informazione fornita dallo spedizioniere, il quale acquisisce la conferma di consegna tramite la firma di A.

Quindi lo *Smart contract* dovrebbe verificare la firma di A, la firma dello spedizioniere, ecc…

3) Uno *Smart contract* è utilizzato per stipulare ed eseguire un contratto di assicurazione antincendio su una casa.

Il contratto tra le due parti (il proprietario della casa e la compagnia di assicurazione) stabilisce che, se la casa va a fuoco, l'assicurazione pagherà al proprietario una certa cifra.

Da questa fattispecie si ricavano tre elementi: una polizza attiva, un controllo nei confronti dello stato della casa e, se si verifica la condizione di incendio, l'obbligo da parte della compagnia di assicurazione di indennizzare il contraente della polizza (*if-then*).

Nei contratti "ordinari" prima di liquidare la polizza è necessario accertare una serie di elementi come:

- Su quale conto bancario la compagnia assicuratrice deve pagare l'indennizzo
- Se la polizza è ancora attiva.
- Se i contraenti hanno sempre rispettato i propri obblighi.
- Se chi presenta il reclamo è veramente l'assicurato.
- Se la compagnia assicurativa ha i fondi per indennizzare l'assicurato, e
- soprattutto, accertarsi se la casa è veramente bruciata.

Quest'ultima verifica richiederà l'attestazione di una fonte esterna e terza, che nello specifico potrebbero essere i vigili del fuoco.

Solo dopo tutte queste verifiche la polizza verrà liquidata all'assicurato.

Se invece il contratto di assicurazione assumerà la veste di uno ***Smart contract*** esso sarà in grado di verificare in maniera autonoma tutti gli elementi che abbiamo elencato sopra in quanto:

- potrebbe garantire la presenza di fondi nel conto corrente della compagnia di assicurazione,
- darà certezza dell'indirizzo della casa dell'assicurato che è bruciata,
- darà conto dello stato dei pagamenti della polizza (sapere quindi se è attiva o meno),

Sussisterebbe però, comunque, un elemento incerto che deve essere verificato da una fonte esterna alla *Blockchain* ed è l'effettiva distruzione della casa a causa di un incendio.

In questo caso sarebbero i vigili del fuoco che, come fonte esterna e terza allo *Smart contract*, costituirebbero l'Oracolo e darebbero l'input allo *Smart contract* comunicando l'avvenuta distruzione della casa a causa dell'incendio dando così il via all'esecuzione finale del pagamento dell'indennizzo assicurativo.

Potrebbe avvenire che un singolo Oracolo possa essere scorretto nel fornire le informazioni richieste ed agire in modo pregiudizievole nei confronti dello *Smart contract* e dei soggetti parti dello stesso.

Se ciò si dovesse verificare tale comportamento andrebbe ad intaccare il concetto della fiducia diffusa che sta alla base della *Blockchain* e quindi, in questo caso, dello *Smart contract*.

In questi casi "l'intelligenza" dello *Smart contract* è direttamente proporzionale (o strettamente correlata) all'intelligenza/etica/onestà dell'Oracolo, che può fare prendere allo *Smart contract* una direzione per adempiere oppure un'altra.

Nonostante la negatività derivante dal comportamento illecito dell'Oracolo se si volesse trovare un dato positivo da questa situazione patologica, al di fuori della fattispecie singola, si deve far notare che la *Blockchain* su cui è inserito lo *Smart contract*, allo stesso tempo traccia in modo indelebile l'attività dell'Oracolo ed i suoi input.

Quindi se un Oracolo effettua più di una volta degli input falsi e sbagliati, tutto questo è scritto e salvato in modo ben in chiaro nella *Blockchain* così che la comunità della *chain* potrà segnalare l'Oracolo come fraudolento ed escluderlo da qualsiasi altro contratto.

Inoltre si avrebbero le prove incancellabili per denunciare l'Oracolo e chiedergli un risarcimento del danno per dolo o per colpa.

Nella pratica, per ridurre al minimo questa possibilità, è consigliabile che lo *Smart contract* interroghi più Oracoli indipendenti allo scopo di verificare l'informazione richiesta da più fonti avendo così maggiori garanzie di obiettività e veridicità.

Anche l'Oracolo stesso può essere strutturato per interrogare più fonti al fine di accertare il verificarsi di fattori esterni alla *Blockchain* (ad esempio, un *data feed* per ricevere dati aggiornati su un tasso di interesse, un sensore che trasmette dati atmosferici quali temperatura e umidità, un GPS che trasmette una posizione, oppure un organismo terzo che gestisce un conflitto).

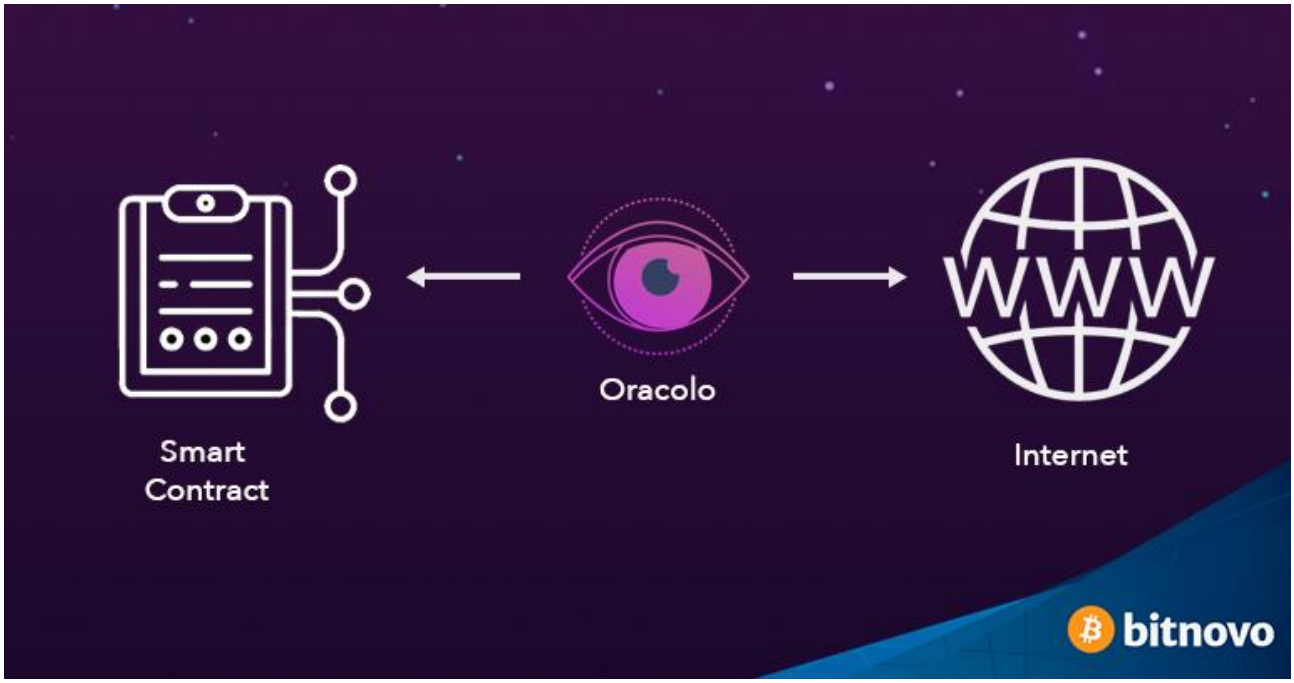
La responsabilità personale dell'Oracolo dipende anche dal fatto se esso si sia reso o meno parte attiva nel fornire le informazioni necessarie allo *Smart contract*.

a) Se le parti dello *Smart contract* hanno fatto semplicemente affidamento, ad esempio ad un sito istituzionale come quello della borsa valori – che in questo caso svolge la funzione di Oracolo istituzionale, che rimane di fatto estraneo al rapporto contrattuale, la responsabilità dei dati sussiste solo se si dimostra che erano falsi o scorretti.
b) Se invece l'Oracolo è un imprenditore privato che svolgendo la propria attività, stipula un accordo con le parti dello *Smart contract* e fornisce una prestazione non adeguata – colpa - o volutamente scorretta – dolo - la responsabilità sulla fattispecie concreta è più immediata, diretta ed evidente a carico dell'Oracolo.

Nell'ambito del Principio di conservazione del contratto, in tema di Integrazione del contratto ex art. 1374 c.c., l'Oracolo potrebbe avere una funzione determinante come fonte esterna che interviene sulla *Blockchain* per far sì che le lacune dello *Smart contract* possano essere colmate senza che si possa determinare un'ipotesi di invalidità dello stesso.

Articolo 1374 Codice Civile

Il contratto obbliga le parti non solo a quanto è nel medesimo espresso, ma anche a tutte le conseguenze che ne derivano secondo la legge, o, in mancanza, secondo gli usi e l'equità.



https://blog.bitnovo.com

3.8 Momento di passaggio della proprietà e momento di passaggio dei rischi

A seconda del sistema giuridico di riferimento vige il sistema francese/italiano, il sistema romano/tedesco od il sistema anglosassone (a tal proposito si veda a cura di Marco Tupponi il "Manuale di Diritto Commerciale Internazionale" – III Edizione – Edizioni Giappichelli – paragrafo 4.1).

1) Se allo *Smart contract* si applica il principio consensualistico il principio "*res perit domino*" si avrà con il semplice scambio dei consensi.

2) Se allo *Smart contract* si applica il principio consenso + consegna il principio "*res perit domino*" avverrà con la consegna del bene.

3) Se allo *Smart contract* si applica il sistema di *Common Law* la cosa perisce in capo a chi ne ha la disponibilità diretta od indiretta (problematica degli *INCOTERMS*).

Questi tre differenti meccanismi di trasferimento della proprietà devono essere tenuti presente nel momento in cui si trasmettono al tecnico informatico le indicazioni giuridiche di come egli deve traslare in algoritmi gli aspetti legali.

Art. 1376* c.c. *Contratto** *"consensuale"* **con effetti reali

Nei contratti che hanno per oggetto il trasferimento della proprietà di una cosa determinata, la costituzione o il trasferimento di un diritto reale ovvero il trasferimento di un altro diritto, la proprietà o il diritto si trasmettono e si acquistano per effetto del consenso delle parti legittimamente manifestato (1155, 1265, 1465, 1472, 1520 e seguenti, 2644, 2684, 2808-2).

3.9) Interpretazione dello *Smart contract*

Alcune problematiche possono emergere con riferimento all'interpretazione del contratto, posto che tale operazione si pone come necessario presupposto logico dell'esecuzione del contratto, operazione, quest'ultima, cui il *software* dovrebbe provvedere automaticamente.

In particolare per quanto riguarda l'interpretazione soggettiva del contratto relativa all'intenzione dei contraenti, all'interpretazione complessiva delle clausole, all'interpretazione di buona fede, ecc. l'utilizzo di uno *Smart contract* pone problematiche che a tutt'oggi creano problematiche di difficile soluzione.

Se si coinvolge, impugnando il linguaggio informatico, un giudice sull'interpretazione della trasposizione della clausola giuridica nel codice informatico le problematiche interpretative diventano molto complesse, perché è rarissimo che un programmatore abbia sufficienti nozioni giuridiche così da riuscire a spiegare in un "linguaggio naturale" ciò che è stato trasposto in linguaggio informatico.

Il Codice Civile Italiano prescrive una serie di criteri (Libro IV, Capo V, artt. 1362 - 1371) cui conformarsi nell'interpretazione del contratto.

È prassi distinguere tra

1) criteri di interpretazione soggettiva (e.g. artt. 1362 e 1363) e
2) criteri di interpretazione oggettiva (artt. 1366 e 1367).

Risultano di tutta evidenza problematiche di tipo applicativo con riguardo a canoni di carattere soggettivo.

Si pensi all'**interpretazione del contratto**

1. secondo la comune intenzione delle parti o

2. secondo il comportamento complessivo delle stesse.

Infatti, se **nel primo caso** si richiede di procedere all'accertamento di un elemento la cui stessa esistenza potrebbe fare sorgere ulteriori problematiche, **nel secondo** è richiesta la considerazione di elementi che debbono necessariamente porsi al di fuori del testo contrattuale.

Entrambe le ipotesi richiedono comunque il compimento di operazioni che allo stato attuale non sembrano essere eseguibili in via del tutto automatica da parte di un *software* quindi con lo strumento dello *Smart contract*.

Ma neppure le regole rientranti tra i **criteri oggettivi**, quali ad **esempio** l'interpretazione secondo buona fede (art. 1366) ed il principio di conservazione del contratto (art. 1367) o dell'interpretazione contro l'autore della clausola (art. 1370), sembrano, in ragione della complessità delle operazioni di valutazioni richieste, potersi eseguire da un software in totale autonomia.

Art. 1366 Interpretazione di buona fede

Il contratto deve essere interpretato secondo buona fede

Art 1367 Conservazione del contratto

Nel dubbio, il contratto o le singole clausole devono interpretarsi nel senso in cui possono avere qualche effetto, anziché in quello secondo cui non ne avrebbero alcuno.

Art. 1370 Interpretazione contro l'autore della clausola

Le clausole inserite nelle condizioni generali di contratto o in moduli o formulari predisposti da uno dei contraenti s'interpretano, nel dubbio, a favore dell'altro.

Ridurre uno *Smart contract* al mero codice informatico determinerebbe l'eliminazione di qualsivoglia spazio per l'interpretazione.

Infatti, se gli *Smart contracts* consentono **l'adempimento automatico secondo regole programmate sottese a ciò per cui sono programmati**, non potrebbero trovare applicazione le regole ermeneutiche di cui agli artt. 1362 - 1371 ss. c.c. che, nel caso dei contratti "tradizionali", sono utilizzate per la ricerca della comune intenzione delle parti contraenti al momento della conclusione del contratto, talvolta nascosta dietro il significato oscuro o ambiguo delle espressioni utilizzate nel testo contrattuale.

Come si diceva alcune locuzioni giuridiche "qualitative" (ad esempio, **buona fede**) difficilmente possono essere tradotte nel linguaggio dei codici informatici impiegato negli *Smart contracts* e richiedono necessariamente un intervento dell'interprete che tenga conto del settore di applicazione e della tipologia contrattuale.

Si noti che in *Common Law*, come già evidenziato, il principale criterio ermeneutico, invece è la **letteralità** per cui gli *Smart contracts* nel mondo giuridico anglosassone hanno vita più facile sotto l'aspetto dell'interpretazione contrattuale.

In ***Civil Law*** anche sotto questa prospettiva, dunque, occorre che gli *Smart contracts* possano agganciarsi ad un elemento esterno - Oracolo.

Al pari di tutti i contratti, anche l'interpretazione degli *Smart contracts* deve quindi tenere conto dei criteri dettati dalle previsioni codicistiche di cui sopra e, in particolare, non può sottrarsi ad uno dei principi cardine del nostro ordinamento, sancito dall'art. 1366 c.c., ossia **l'obbligo di interpretare il contratto secondo buona fede.**

3.10) La Forma dello *Smart contract*

Tra i requisiti del contratto, la forma scritta in generale e quella *ad substantiam* in particolare cioè per la validità del contratto è quella che suscita maggiori perplessità.

Si potrebbe ritenere che lo *Smart contract* sia un contratto elaborato per iscritto redatto in un "codice *software*".

Si rammenti che la forma scritta trova la sua ragione di essere per due principali motivi:

- *Ad substantiam*: la forma è richiesta per la validità stessa del contratto.
- *Ad probationem*: la forma costituisce il mezzo per provare l'esistenza di quel contratto.

La questione della forma scritta nei documenti informatici è stata affrontata dal **D.Lgs 7 marzo 2005, n. 82 e successive modifiche** - "Codice dell'Amministrazione Digitale." (si vedano anche i paragrafi 1.10 e ss. della presente Guida)

L'art. 20 del suddetto Decreto richiede che **il documento informatico** soddisfi il requisito della forma scritta e abbia **l'efficacia di cui all'art 2720 c.c.** ("piena prova" della provenienza delle dichiarazioni di chi ha sottoscritto il documento salvo un disconoscimento da parte quest'ultimo) **qualora sia sottoscritto con una** firma digitale, qualificata o avanzata, o, nel caso di documenti sottoscritti con firme elettroniche differenti, qualora rispetti gli standard tecnici individuati dall'AgID - Agenzia per l'Italia digitale - (con modalità volte a garantire sicurezza, integrità, immodificabilità del documento e riconducibilità dell'autore).

Nei restanti casi il valore probatorio del documento informatico è rimesso al libero giudizio degli organi giudicanti.

Altri elementi di interesse sono il tema dell'**identificazione del firmatario** (e le relative modalità in cui questo può avvenire, come per esempio, con la firma elettronica, o con l'uso di SPID – Sistema Pubblico per l'Identità Digitale) per cui l'AgID sta definendo dei requisiti idonei a far sì che un processo di identificazione informatica possa dar luogo alla creazione di firme elettroniche.

I documenti informatici sono da intendersi come i documenti elettronici che contengono la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Gli artt. 20 comma 1-bis e 21 comma 2-bis

del Decreto Legislativo 5 marzo 2005, n. 82 e successive modifiche rispettivamente dispongono:

*"Il documento informatico soddisfa il requisito della **forma scritta** e ha l'efficacia prevista dall'articolo **2702 del Codice civile** quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 **con modalità tali da garantire la sicurezza, integrità e***

immodificabilità del documento *e, in maniera* ***manifesta e inequivoca, la sua riconducibilità all'autore****. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.".*

e:

"Salvo il caso di sottoscrizione autenticata, ***le scritture private*** *di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con* ***firma elettronica avanzata****,* ***qualificata o digitale*** *ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo."*

Capo II - Della prova documentale - Sezione II - Della scrittura privata

Articolo 2702 Codice Civile

La scrittura privata *[1967, 2701, 2715, 2821, 2835]* ***fa piena prova, fino a querela di falso*** *[221 c.p.c.], della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta [2652 n. 3; 214 c.p.c. 215 c.p.c.]*

Si potrebbe far leva sull'utilizzo del meccanismo di **crittografia a chiave asimmetrica** ad opera dei fruitori della *Blockchain* per **riconoscere** anche allo ***Smart contract*** il requisito della forma scritta e l'efficacia di piena prova sino a querela di falso ai sensi della menzionata previsione codicistica.

3.11) L'Adempimento dello *Smart contract* e la Buona Fede

Nonostante l'adempimento negli *Smart contracts* sia automatizzato, potrebbero **sorgere contestazioni** tra le parti in merito **all'esattezza dell'adempimento**.

Nel nostro ordinamento la previsione cardine su questo tema è rappresentata **dall'art. 1375 c.c.**, che impone alle parti di **eseguire il contratto secondo buona fede**: interpretando ed applicando tale disposizione, la Suprema Corte di Cassazione ha più volte affermato che, in presenza di talune circostanze, anche un'esecuzione perfettamente aderente alla lettera del contratto (come nel caso dell'esecuzione automatica dello *Smart contract*) potrebbe costituire nei fatti un inadempimento perché contraria al canone generale della buona fede.

A) Sul punto, non manca chi sostiene che tali problemi possano essere affrontati predeterminando criteri precisi nel codice informatico e, quindi, sottraendo alle parti ogni margine di discrezionalità valutativa.

Tale soluzione, tuttavia, non pare del tutto soddisfacente, in quanto difficilmente possono essere predeterminati *ex ante* tutti i criteri necessari ad escludere del tutto la necessità di una valutazione qualitativa.

B) Più condivisibile sembra essere la posizione di coloro i quali ritengono che tali questioni debbano essere risolte, anche con riferimento agli *Smart contracts*, attraverso **i metodi tradizionali di risoluzione delle controversie.**

3.12) L'Integrazione e l'Esecuzione forzata dello *Smart contract*

Occorre interrogarsi circa i rimedi attivabili qualora gli *Smart contracts* si pongano **in contrasto** con **norme di ordine pubblico o norme imperative**.

Come noto, le norme cogenti trovano applicazione indipendentemente dalla volontà dei singoli (ad esempio, sono nulle pattuizioni che hanno l'effetto di privare il consumatore di determinate protezioni derivanti dal codice del consumo).

Analogamente, in caso di controversie relative al contratto, l'esecuzione può essere ottenuta attraverso l'intervento di organi giudiziari che, definita la controversia, possono altresì imporre **l'esecuzione in forma specifica** delle obbligazioni **ovvero il risarcimento dei danni.**

Considerato che gli *Smart contracts* **non sono modificabili** e **l'adempimento è automatico**, si discute se sia possibile ottenerne l'esecuzione o la risoluzione senza la necessità di coinvolgere organi terzi.

Anche a tale riguardo non manca chi sostiene l'assoluta indipendenza degli *Smart contracts* dagli impianti tradizionali, **ritenendo che pure le fasi patologiche del rapporto si possano affrontare traducendo nel codice informatico le "reazioni" ad azioni/inadempimenti predefiniti.**

Per esempio, la clausola risolutiva espressa ex art. 1456 c.c., la sospensione dell'esecuzione in caso di mutamento delle condizioni patrimoniali di controparte ex art. 1461 c.c., il diritto di ritenzione previsto dagli artt. 2756 e 2761 c.c., il pegno irregolare art. 1851 c.c., ecc.

Come evidenziato sopra, tuttavia, è difficile immaginare che si riescano a prevedere e a codificare in anticipo tutte le possibili reazioni.

D'altronde occorre rilevare come il **ricorso agli organi giurisdizionali** per ottenere l'esecuzione di uno *Smart contract* possa rivelarsi estremamente complesso, a causa della lentezza di adeguamento del sistema giudiziario e giuridico in generale alle nuove tecnologie.

Per tale motivo, le parti ben potrebbero considerare di ricorrere ai sistemi di **risoluzione alternativa delle controversie** come **l'arbitrato**: strumento flessibile, che ben si adatta alle caratteristiche degli *Smart contracts*.

All'interno del codice informatico dello *Smart contract* può essere **inserita una** clausola compromissoria che stabilisca che ogni eventuale controversia derivante dall'esecuzione del contratto stesso sia demandata alla competenza esclusiva di un arbitrato.

Lo *Smart contract* potrebbe attivare automaticamente il meccanismo di risoluzione della lite e potrebbe, a sua volta, utilizzare l'infrastruttura *Blockchain*: il lodo arbitrale verrebbe registrato a sua volta nel ***Digitalized Ledger*** - DLT - ed eseguita sulla stessa *Blockchain*, tramite l'esecuzione di un codice informatico che preveda il trasferimento delle somme riconosciute come dovute dal lodo arbitrale dal conto riconducibile alla parte condannata a quello riconducibile alla parte vincitrice.

Nello *Smart contract* bisognerebbe prevedere una "girandola" di ipotesi solutorie con più opzioni (l'informatica si sostituirebbe al giudizio degli arbitri in carne ed ossa)

3.13) La Legge applicabile ed il Foro competente

La *Blockchain* impiegata per sviluppare uno *Smart contract* può essere rappresentante da **una rete di *computers* – cosiddetti nodi** – localizzati ovunque e privi di una entità centrale che li coordini.

Non dimentichiamoci mai che si tratta di una tecnologia nata per funzionare indipendentemente dai punti di accesso cioè dai centri di interesse e di imputazione.

Questo meccanismo potrebbe far scattare l'idea, sbagliata, che tale mancanza permetterebbe alle imprese, soprattutto del settore *high tech*, di operare al di fuori di un preciso quadro normativo.

Lo *Smart contract* però potrebbe essere nullo o annullabile, potrebbero sorgere ipotesi di inadempimento ed altre patologie contrattuali quindi è fondamentale porsi il problema:

1) Quale è la legge che governa uno *Smart contract*? e

2) Come si decide il foro competente o l'arbitrato internazionale?

3.13.a) La Legge applicabile

Data la complessità e la grande dimensione, in termini geografici, su cui operano le principali *Blockchain* attive nasce la necessità di individuare la legge applicabile, in merito allo *Smart contract* che la *Blockchain* veicola, nel caso in cui nascano delle controversie fra le parti.

Su tale argomento, almeno intra UE, il riferimento normativo è il **Regolamento n. 593/2008 - Roma I** che afferma che, in assenza di una clausola concordata tra le parti ex art. 3, si applica l'art. 4 e, come principio di chiusura, al secondo comma dell'art. 4, la *legge del Paese dove si svolge **la prestazione caratteristica***; mentre in materia extracontrattuale vige il Regolamento Roma II che identifica un meccanismo atto a seguire la legge applicata in ambito contrattuale anche in riferimento alla responsabilità extra-contrattuale.

La normativa però non risulta applicabile in un contesto di *Blockchain Permissionless*, in quanto gli utenti non risultano identificati univocamente poiché spesso utilizzano pseudonimi e la collocazione geografica risulta sconosciuta o di difficile attribuzione in molti casi: nodi, *miners*, Oracoli, creandosi così un meccanismo di difficile collocazione giuridica in quanto coesistono nella stessa entità virtuale una moltitudine di ordinamenti giuridici differenti.

Da tale considerazione[71] si delinea uno scenario troppo incerto ed acerbo ed ancora in fase di sviluppo per poter applicare una metodologia di scelta legislativa definitiva ed assolutamente certa.

Una possibile soluzione sarebbe quella dell'identificazione giuridica della rete come società di fatto al fine di creare i presupposti per l'applicazione del diritto internazionale privato ma essa, date le sue caratteristiche (cooperazione non basata su un accordo ma a livello prettamente tecnico) non trova identificazione nella precitata tipologia di società come società di fatto.

Tale paradigma non ha ancora trovato soluzione se non la dotazione, da parte della *Blockchain,* di uno statuto che regoli responsabilità interne alla stessa e identifichi una legge di riferimento.

In merito alla legge applicabile al singolo *Smart contract* (sia come atto esecutivo che come contratto) ci si chiede se ad esso, riconoscendo la sua peculiarità transnazionale, si possano ricondurre le soluzioni richiamate dal **diritto internazionale privato**.

A tal proposito pare avvalorarsi una tesi[72] che coniuga questi ambiti internazionali attraverso una schematizzazione a tre elementi degli *Smart contracts*.

1. Qualora rappresenti un **documento contrattuale** in tal caso si sostiene come esso rappresenti la legge fra le parti (ai sensi dell'art. 1372) con le relative difficoltà, menzionate anche in precedenza, in merito a tutte quei termini giuridici quali ragionevolezza, diligenza, ecc. non tramutabili in linguaggio informatico.
2. Se invece si intente lo *Smart contract* semplicemente uno strumento finalizzato all'esecuzione del contratto in tal caso esso, rappresentando un mero strumento giuridico

[71] Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide, Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF N°4-2017 - December 2017

[72] Smart contracts Are No Problem for the World's Legal Systems, so Long as They Behave Like Legal Contracts, Stephan Meyer and Martin Eckert - Feb 8, 2019 by Cointele

di esecuzione (automatica) delle prestazioni, non ricadrebbe nell'applicazione del diritto internazionale privato.

3. Se addirittura si propende per intenderlo come un mero codice informatico non si avrà nessun collegamento con la disciplina contrattuale.

Nel primo caso, intendendolo come un documento contrattuale, la dottrina[73], sembra propendere verso il principio di autonomia contrattuale che crea un ponte di collegamento fra diritto internazionale privato (Roma I e II) e lo *Smart contract*.

Come si diceva un argomento basilare è definire la **territorialità della prestazione principale** nel caso in cui la legge applicabile al rapporto contrattuale sia stata definita dalle parti ex art. 4 di Roma I.

Le caratteristiche della *Blockchain*, in termini di identificabilità dei soggetti, non permettono la creazione di un collegamento fra domicilio della parte ed il suo pseudonimo all'interno della *Blockchain*; infatti le parti potrebbero optare per la conclusione di un contratto con un soggetto non identificabile ed in questo caso, anche riconosciuta la prestazione caratteristica, non vi è possibilità di effettuare il collegamento della legge applicabile in base al paese in cui risiede il soggetto collegato.

In contrapposizione alle fonti nazionali ed internazionali i membri della *Blockchain* sembrano avvalorale un curioso paradigma, quello della **c.d. *Lex Cryptographica*** che rappresenta una serie di regole informatiche volte[74] a "*disciplinare l'utilizzo e lo scambio delle informazioni digitali nonché promuovere la stabilità senza ricorrere ad ordinamenti nazionali*".

Essa si caratterizza dunque da una serie di algoritmi e funzioni intrinseche alla tecnologia che permettono, a prescindere dai vari ordinamenti, una corretta e stabile coesione fra i partecipanti della rete.

Essa può essere paragonata ad una sorta di ***Lex Mercatoria***, ovvero una serie di norme che non proviene da una fonte legislativa ma piuttosto da fonti differenti.

[73] Blockchain Networks and European Private International Law, November 26, 2018 by Giesela Ruehl

[74] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 365

Mentre per la *Lex Mercatoria* le fonti si identificano tra le altre in: 1) usi e consuetudini normativi (es. Incoterms) 2) Schemi contrattuali creati da società multinazionali 3) Lodi degli arbitri.

La *Lex Cryptographica* dovrebbe provenire da fonti informatiche ed in particolare da codici aggiornati in modo continuo atti a rendere il sistema uniforme e stabile.

A tal proposito, **il parere di molti studiosi**[75] pare convergere nell'integrazione e coesistenza di entrambi gli ordinamenti (*Lex Cryptographica* e *Lex Mercatoria*) questo poiché anche se l'informatizzazione e l'automazione appare la soluzione più efficiente possibile essa non può prescindere da quella che è l'evoluzione sociale di un certo paese o sistema internazionale in termini puramente qualitativi e, conseguentemente, legislativi nonché da tutte le norme di applicazione necessaria.

In tema di **Regolamento 593/2008 - ROMA I**

considerando *quanto segue:*

(11)

La libertà delle parti di scegliere la legge applicabile *dovrebbe costituire una delle pietre angolari del sistema delle regole di conflitto di leggi in materia di obbligazioni contrattuali.*

Articolo 3 Libertà di scelta (Principio di Autonomia contrattuale)

1. *Il contratto è regolato dalla legge scelta dalle parti. La scelta dev'essere espressa, o risultare in modo ragionevolmente certo dalle disposizioni del contratto o dalle circostanze. Le parti possono designare la legge applicabile a tutto il contratto, ovvero a una parte soltanto di esso.*

Operativamente sembra difficile tradurre questa possibilità di "libertà di scelta" in algoritmo in quanto, in tema di **scambio dei consensi** anche nel caso di scelta della legge applicabile rimane il dubbio se la scelta sia imputabile:

a) alla parte,
b) all'algoritmo,
c) a colui che lo ha creato

[75]Zamfir in R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 368

La decisione sulla legge applicabile allo *Smart contract* necessita, secondo parte della dottrina, di una scelta secondo le forme tradizionali e con "linguaggio naturale".

2. Le parti possono convenire, in qualsiasi momento, di sottoporre il contratto ad una legge diversa da quella che lo regolava in precedenza, vuoi in funzione di una scelta anteriore secondo il presente articolo, vuoi in funzione di altre disposizioni della presente convenzione. Qualsiasi modifica relativa alla determinazione della legge applicabile, intervenuta posteriormente alla conclusione del contratto, non inficia la validità formale del contratto ai sensi dell'articolo 9 e non pregiudica i diritti dei terzi.

*3. La scelta di una legge straniera ad opera delle parti, accompagnata o non dalla scelta di un tribunale straniero, qualora nel momento della scelta tutti gli altri dati di fatto si riferiscano a un unico paese, non può recare pregiudizio alle norme alle quali la legge di tale paese non consente di derogare per contratto, qui di seguito denominate «**disposizioni imperative**».*

4. L'esistenza e la validità del consenso delle parti sulla legge applicabile al contratto sono regolate dagli articoli 8, 9 e 11.

Articolo 4

Legge applicabile in mancanza di scelta

PRINCIPIO della PRESTAZIONE CARATTERISTICA

1. In mancanza di scelta esercitata ai sensi dell'articolo 3 e fatti salvi gli articoli da 5 a 8, la legge che disciplina il contratto è determinata come segue:

a) il contratto di vendita di beni è disciplinato dalla legge del paese nel quale il venditore ha la residenza abituale;

b) il contratto di prestazione di servizi è disciplinato dalla legge del paese nel quale il prestatore di servizi ha la residenza abituale;

c) il contratto avente per oggetto un diritto reale immobiliare o la locazione di un immobile è disciplinato dalla legge del paese in cui l'immobile è situato;

d) in deroga alla lettera c), la locazione di un immobile concluso per uso privato temporaneo per un periodo di non oltre sei mesi consecutivi è disciplinata dalla legge del paese nel quale il proprietario ha la residenza abituale, purché il locatario sia una persona fisica e abbia la sua residenza abituale nello stesso paese;

e) il contratto di affiliazione (franchising) è disciplinato dalla legge del paese nel quale l'affiliato ha la residenza abituale;

f) il contratto di distribuzione è disciplinato dalla legge del paese nel quale il distributore ha la residenza abituale;

g) il contratto di vendita di beni all'asta è disciplinato dalla legge del paese nel quale ha luogo la vendita all'asta, se si può determinare tale luogo;

h) il contratto concluso in un sistema multilaterale che consente o facilita l'incontro di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, quali definiti all'articolo 4, paragrafo 1, punto 17, della direttiva 2004/39/CE, conformemente a regole non discrezionali e disciplinato da un'unica legge, è disciplinato da tale legge.

*2. **Se il contratto non è coperto dal paragrafo 1** o se gli elementi del contratto sono contemplati da più di una delle lettere da a) ad h), del paragrafo 1, il contratto è disciplinato dalla legge del paese nel quale la parte che deve effettuare la **prestazione caratteristica** del contratto ha la residenza abituale.*

3. Se dal complesso delle circostanze del caso risulta chiaramente che il contratto presenta collegamenti manifestamente più stretti con un paese diverso da quello indicato ai paragrafi 1 o 2, si applica la legge di tale diverso paese.

1. *Se la legge applicabile non può essere determinata a norma dei paragrafi 1 o 2, il contratto è disciplinato dalla legge del paese con il quale presenta il collegamento più stretto.*

Articolo 19

Residenza abituale

molto difficile da definire in caso di *Blockchain/Smart contract*

1. Ai fini del presente regolamento, per residenza abituale di società, associazioni e persone giuridiche si intende il luogo in cui si trova la loro ***amministrazione centrale****.*

Per residenza abituale di una persona fisica che agisce nell'esercizio della sua attività professionale si intende la sua ***sede di attività principale****.*

2. Quando il contratto è concluso nel quadro dell'esercizio dell'attività di una filiale, di un'agenzia o di qualunque altra sede di attività, o se, secondo il contratto, la prestazione deve essere fornita da una siffatta filiale, agenzia o sede di attività, il luogo in cui ***è ubicata la filiale, l'agenzia o altra sede di attività è considerato residenza abituale****.*

3. ***Al fine di determinare la residenza abituale il momento rilevante è quello della conclusione del contratto.***

3.13 b) Il Foro competente e l'Arbitrato

Altro aspetto a cui prestare molta attenzione è rappresentato dalla **scelta del foro competente** nel caso in cui nascano delle controversie.

È sempre possibile che le Parti diano la propria preferenza attraverso un accordo esterno allo *Smart contract* in tema di foro competente o arbitrato.

L'Arbitrato, se economicamente è conveniente tra le parti (si tenga presente, però, che il costo di un procedimento arbitrale internazionale è di varie centinaia di migliaia di euro) potrebbe eliminare anche il problema dell'eseguibilità della sentenza, tipico problema dei giudizi ordinari, nel caso in cui il paese ricada all'interno dei 156 paesi che, a tutt'oggi, hanno ratificato la Convenzione di New York del 1958[76] in tema di riconoscimento dei lodi arbitrali stranieri sul proprio territorio.

Il lodo arbitrale internazionale potrebbe essere strutturato come codice informatico che, all'emissione ed esecuzione nella *Blockchain* di riferimento, venga eseguito e modifichi determinate somme/dati/algoritmi.

REGOLAMENTO (UE) N. 1215/2012 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 dicembre 2012

[76] legge 19 gennaio 1968, n. 62 (pubblicata nella gazzetta ufficiale del 21 febbraio 1968, n. 46) adesione alla convenzione per il riconoscimento e l'esecuzione delle sentenze arbitrali straniere, adottata a New York il 10 giugno 1958 e sua esecuzione.

*concernente la **competenza giurisdizionale**, il **riconoscimento** e l'**esecuzione** delle decisioni in materia civile e commerciale*

CAPO I - ***AMBITO DI APPLICAZIONE E DEFINIZIONI***

Articolo 1

1. Il presente regolamento si applica in materia civile e commerciale, indipendentemente dalla natura dell'autorità giurisdizionale. Esso non si estende, in particolare, alla materia fiscale, doganale e amministrativa né alla responsabilità dello Stato per atti o omissioni nell'esercizio di pubblici poteri (acta iure imperii).

2. Sono esclusi dall'ambito di applicazione del presente regolamento:

a) lo stato e la capacità delle persone fisiche, il regime patrimoniale fra coniugi o derivante da rapporti che secondo la legge applicabile a questi ultimi hanno effetti comparabili al matrimonio;

b) i fallimenti, le procedure relative alla liquidazione di società o altre persone giuridiche che si trovino in stato di insolvenza, i concordati e le procedure affini;

c) la sicurezza sociale;

d) l'arbitrato;

e) le obbligazioni alimentari derivanti da rapporti di famiglia, di parentela, di matrimonio o di affinità;

f) i testamenti e le successioni, comprese le obbligazioni alimentari mortis causa.

Articolo 2

Ai fini del presente regolamento s'intende per:

*a) «**decisione**»: a prescindere dalla denominazione usata, qualsiasi decisione emessa da un'autorità giurisdizionale di uno Stato membro, compresi un decreto, un'ordinanza, una decisione o un mandato di esecuzione, nonché una decisione relativa alla determinazione delle spese giudiziali da parte del cancelliere.*

Ai fini del capo III, la «decisione» comprende anche i provvedimenti provvisori e cautelari emessi da un'autorità giurisdizionale competente a conoscere nel merito ai sensi del presente regolamento. Essa non comprende i provvedimenti provvisori e cautelari emessi da tale autorità

giurisdizionale senza che il convenuto sia stato invitato a comparire, a meno che la decisione contenente il provvedimento sia stata notificata o comunicata al convenuto prima dell'esecuzione;

*b) «**transazione giudiziaria**»: la transazione approvata dall'autorità giurisdizionale di uno Stato membro o conclusa davanti all'autorità giurisdizionale di uno Stato membro nel corso di un procedimento;*

*c) «**atto pubblico**»: qualsiasi documento che sia stato formalmente redatto o registrato come atto pubblico nello Stato membro d'origine e la cui autenticità:*

i) riguardi la firma e il contenuto dell'atto pubblico; e

ii) sia stata attestata da un'autorità pubblica o da altra autorità a tal fine autorizzata;

*d) «**Stato membro d'origine**»: lo Stato membro nel quale, a seconda dei casi, è stata emessa la decisione, è stata approvata o conclusa la transazione giudiziaria, è stato formalmente redatto o registrato l'atto pubblico;*

*e) «**Stato membro richiesto**»: lo Stato membro in cui è chiesto il riconoscimento della decisione o l'esecuzione della decisione, della transazione giudiziaria o dell'atto pubblico;*

*f) «**autorità giurisdizionale d'origine**»: l'autorità giurisdizionale che ha emesso la decisione di cui si chiede il riconoscimento o di cui si sollecita l'esecuzione.*

Articolo 3

*Ai fini del presente regolamento, la nozione di «**autorità giurisdizionale**» comprende le seguenti autorità nella misura in cui sono competenti per le materie rientranti nell'ambito di applicazione del presente regolamento:*

a) in Ungheria, nei procedimenti sommari relativi a ingiunzioni di pagamento (fizetési meghagyásos eljárás), il notaio (közjegyző);

b) in Svezia, nei procedimenti sommari relativi a ingiunzioni di pagamento (betalningsföreläggande) e all'assistenza (handräckning), l'autorità per l'esecuzione forzata (Kronofogdemyndigheten).

CAPO II ***COMPETENZA*** *SEZIONE 1*

Disposizioni generali

Articolo 4

1. A norma del presente regolamento, le persone ***domiciliate*** *nel territorio di un determinato Stato membro sono convenute, a prescindere dalla loro cittadinanza, davanti alle autorità giurisdizionali di tale Stato membro.* ***(Conf. Art. 62 primo comma)***

2. Alle persone che non possiedono la cittadinanza dello Stato membro nel quale esse sono domiciliate si applicano le norme sulla competenza vigenti per i cittadini di tale Stato membro.

Articolo 5

1. Le persone domiciliate nel territorio di uno Stato membro possono essere convenute davanti alle autorità giurisdizionali di un altro Stato membro solo ai sensi delle norme di cui alle sezioni da 2 a 7 del presente capo.

2. In particolare, nei confronti delle persone di cui al paragrafo 1 non trovano applicazione le norme nazionali sulla competenza giurisdizionale che gli Stati membri devono notificare alla Commissione ai sensi dell'articolo 76, paragrafo 1, lettera a).

Articolo 6

1. Se il convenuto non è domiciliato in uno Stato membro, la competenza delle autorità giurisdizionali di ciascuno Stato membro è disciplinata dalla legge di tale Stato, salva l'applicazione dell'articolo 18, paragrafo 1, dell'articolo 21, paragrafo 2, e degli articoli 24 e 25.

2. Chiunque sia domiciliato in un determinato Stato membro può, indipendentemente dalla propria cittadinanza e al pari dei cittadini di questo Stato membro, far valere nei confronti di tale convenuto le norme nazionali sulla competenza in vigore nello Stato medesimo, in particolare quelle che gli Stati membri devono notificare alla Commissione ai sensi dell'articolo 76, paragrafo 1, lettera a).

SEZIONE 2 ***Competenze speciali***

Articolo 7

Una persona domiciliata in uno Stato membro può essere convenuta in un altro Stato membro:

1) *a)* ***in materia contrattuale****, davanti all'autorità giurisdizionale del luogo di esecuzione dell'obbligazione dedotta in giudizio;*

IL PROBLEMA è che la prestazione disciplinata in uno *Smart contract* è eseguita nel registro distribuito – DLT - per il tramite dell'intervento di una molteplicità di nodi – *computers* – di numero indefinito.

E ciò vale sia per i contratti ad effetti obbligatori sia per i contratti ad effetti reali.

Da ciò consegue, come si diceva, che è difficile stabilire il luogo fisico ove la prestazione è stata o deve essere eseguita.

b) ai fini dell'applicazione della presente disposizione e salvo diversa convenzione, il luogo di esecuzione dell'obbligazione dedotta in giudizio è:

— nel caso della compravendita di beni, il luogo, situato in uno Stato membro, in cui i beni sono stati o avrebbero dovuto essere ***consegnati*** *in base al contratto,*

PROBLEMA nel caso di **compravendita con *Blockchain*** la transazione si conclude sulla *Blockchain* cosicché anche nell'ipotesi di compravendita di un **bene *tokenizzato* (si veda il capitolo 2.3 della presente Guida)** ossia di compravendita della rappresentazione digitale del corrispettivo del bene fisico o immateriale, **il contratto si considera concluso:**

1) con la prestazione del consenso o

2) con il trasferimento nel portafoglio virtuale dell'acquirente del *token* rappresentativo di quel dato bene.

In entrambi i casi manca la certezza del luogo dove il bene viene messo nella disponibilità effettiva dell'acquirente.

— nel caso della prestazione di servizi, il luogo, situato in uno Stato membro, in cui i servizi sono stati o avrebbero dovuto essere prestati in base al contratto;

c) la lettera a) si applica nei casi in cui non è applicabile la lettera b);

*2) in materia di **illeciti civili dolosi o colposi*** (cioè extracontrattuali)*, davanti all'autorità giurisdizionale del luogo in cui l'evento dannoso è avvenuto o può avvenire;*

PROBLEMA

Cosa avviene se tali illeciti sono stati compiuti tramite l'impiego di *Blockchain*?

È difficile, per non dire che sia pressoché impossibile individuare i luoghi prescritti dalla norma.

3) qualora si tratti di un'azione di risarcimento danni o di restituzione nascente da illecito penale, davanti all'autorità giurisdizionale presso la quale è esercitata l'azione penale, sempre che secondo la propria legge tale autorità giurisdizionale possa conoscere dell'azione civile;

4) qualora si tratti di un'azione per il recupero, sulla base del titolo di proprietà, di un bene culturale ai sensi dell'articolo 1, punto 1, della direttiva 93/7/CEE, avviata dal soggetto che rivendica il diritto di recuperare il bene in questione, davanti all'autorità giurisdizionale del luogo in cui si trova il bene culturale quando viene adita l'autorità giurisdizionale;

5) qualora si tratti di controversia concernente l'esercizio di una succursale, di un'agenzia o di qualsiasi altra sede d'attività, davanti all'autorità giurisdizionale del luogo in cui essa è situata;

6) qualora si tratti di una controversia proposta contro un fondatore, trustee o beneficiario di un trust costituito in applicazione di una legge o per iscritto o con clausola orale confermata per iscritto, davanti alle autorità giurisdizionali dello Stato membro in cui il trust ha domicilio;

7) qualora si tratti di una controversia concernente il pagamento del corrispettivo per l'assistenza o il salvataggio di un carico o un nolo, davanti all'autorità giurisdizionale nell'ambito della cui competenza il carico o il nolo a esso relativo:

a) è stato sequestrato a garanzia del pagamento; o

b) avrebbe potuto essere sequestrato a tal fine ma è stata fornita una cauzione o altra garanzia, purché la presente disposizione si applichi solo qualora si faccia valere che il convenuto è titolare di un interesse sul carico o sul nolo o aveva un tale interesse al momento dell'assistenza o del salvataggio.

Articolo 8

*Una persona **domiciliata** in uno Stato membro può inoltre essere convenuta:*

*1) in caso di **pluralità di convenuti**, davanti all'autorità giurisdizionale del luogo in cui uno di essi è domiciliato, sempre che tra le domande esista un collegamento così stretto da rendere opportuna una trattazione unica e una decisione unica onde evitare il rischio di giungere a decisioni incompatibili derivanti da una trattazione separata;*

*2) qualora si tratti di **chiamata in garanzia o altra chiamata di terzo**, davanti all'autorità giurisdizionale presso la quale è stata proposta la domanda principale, a meno che quest'ultima non sia stata proposta solo per distogliere colui che è stato chiamato in causa dalla sua autorità giurisdizionale naturale;*

*3) qualora si tratti di una **domanda riconvenzionale** derivante dal contratto o dal fatto su cui si fonda la domanda principale, davanti all'autorità giurisdizionale presso la quale è stata proposta la domanda principale;*

*4) **in materia contrattuale**, qualora l'azione possa essere riunita con un'azione in materia di **diritti reali immobiliari** proposta contro il medesimo convenuto, davanti all'autorità giurisdizionale dello Stato membro in cui l'immobile è situato.*

Articolo 9

Qualora ai sensi del presente regolamento un'autorità giurisdizionale di uno Stato membro abbia competenza per le azioni relative alla responsabilità derivanti dall'impiego o dall'esercizio di una nave, tale autorità, o qualsiasi altra autorità giurisdizionale competente secondo la legge nazionale, è anche competente per le domande relative alla limitazione di tale responsabilità.

SEZIONE 4 Competenza in materia di contratti conclusi da consumatori

Articolo 17

1. Fatto salvo quanto previsto dall'articolo 6 e dall'articolo 7, punto 5, la competenza in materia di contratti conclusi da una persona, il consumatore, per un uso che possa essere considerato estraneo alla sua attività professionale è regolata dalla presente sezione:

*a) qualora si tratti di una **vendita a rate di beni mobili materiali**;*

b) qualora si tratti di un ***prestito con rimborso rateizzato*** *o* ***di un'altra operazione di credito****, connessi con il finanziamento di una vendita di tali beni; o*

c) ***in tutti gli altri casi****, qualora il contratto sia stato concluso con una persona le cui attività commerciali o professionali si svolgono nello Stato membro in cui è domiciliato il consumatore o sono dirette, con qualsiasi mezzo, verso tale Stato membro o verso una pluralità di Stati che comprende tale Stato membro, purché il contratto rientri nell'ambito di dette attività.*

2. Qualora la controparte del consumatore non abbia il proprio domicilio in uno Stato membro ma possieda una succursale, un'agenzia o qualsiasi altra sede d'attività in uno Stato membro, essa è considerata, per le controversie relative al loro esercizio, come avente domicilio in quest'ultimo Stato membro.

3. La presente sezione non si applica ai contratti di trasporto che non prevedono prestazioni combinate di trasporto e di alloggio per un prezzo globale.

Articolo 18

1. L'azione del consumatore contro l'altra parte del contratto può essere proposta davanti alle autorità giurisdizionali dello Stato membro in cui è domiciliata tale parte o, indipendentemente dal domicilio dell'altra parte, davanti alle autorità giurisdizionali del luogo in cui è ***domiciliato il consumatore****.*

2. L'azione dell'altra parte del contratto contro il consumatore può essere proposta ***solo*** *davanti alle autorità giurisdizionali dello Stato membro nel cui territorio è* ***domiciliato il consumatore****.*

3. Le disposizioni del presente articolo non pregiudicano il diritto di proporre una domanda riconvenzionale davanti all'autorità giurisdizionale investita della domanda principale in conformità della presente sezione.

SEZIONE 6 Competenze esclusive

Articolo 24

Indipendentemente dal domicilio delle parti, hanno ***competenza esclusiva*** *le seguenti autorità giurisdizionali di uno Stato membro:*

*1) in materia di **diritti reali immobiliari e di contratti di locazione di immobili**, le autorità giurisdizionali dello Stato membro **in cui l'immobile è situato**.*

Tuttavia, in materia di contratti di locazione di immobili a uso privato temporaneo stipulati per un periodo massimo di sei mesi consecutivi, hanno competenza anche le autorità giurisdizionali dello Stato membro in cui il convenuto è domiciliato, purché il conduttore sia una persona fisica e il locatore e il conduttore siano domiciliati nel medesimo Stato membro;

*2) in materia di **validità della costituzione, nullità o scioglimento delle società o persone giuridiche, o riguardo alla validità delle decisioni dei rispettivi organi**, le autorità giurisdizionali dello Stato membro in cui la società o persona giuridica ha sede. Al fine di determinare tale sede l'autorità giurisdizionale applica le proprie norme di diritto internazionale privato;*

*3) in materia di validità delle **trascrizioni e iscrizioni nei pubblici registri**, le autorità giurisdizionali dello Stato membro nel cui territorio i registri sono tenuti;*

*4) in materia di **registrazione o di validità di brevetti, marchi, disegni e modelli e di altri diritti analoghi** per i quali è prescritto il deposito ovvero la registrazione, a prescindere dal fatto che la questione sia sollevata mediante azione o eccezione le autorità giurisdizionali dello Stato membro nel cui territorio il deposito o la registrazione sono stati richiesti, sono stati effettuati o sono da considerarsi effettuati a norma di un atto normativo dell'Unione o di una convenzione internazionale.*

Fatta salva la competenza dell'Ufficio europeo dei brevetti in base alla convenzione sul rilascio di brevetti europei, sottoscritta a Monaco di Baviera il 5 ottobre 1973, le autorità giurisdizionali di ciascuno Stato membro hanno competenza esclusiva in materia di registrazione o di validità di un brevetto europeo rilasciato per tale Stato membro;

4) *in materia di **esecuzione delle decisioni**, le autorità giurisdizionali dello Stato membro nel cui territorio ha o ha avuto luogo l'esecuzione.*

SEZIONE 7 **Proroga di competenza**

Articolo 25

1. *Qualora le parti, indipendentemente dal loro domicilio, abbiano convenuto la competenza di un'autorità o di autorità giurisdizionali di uno Stato membro a conoscere delle*

*controversie, presenti o future, nate da un determinato rapporto giuridico, la competenza spetta a questa autorità giurisdizionale o alle autorità giurisdizionali di questo Stato membro, **salvo che l'accordo sia nullo** dal punto di vista della validità sostanziale secondo la legge di tale Stato membro. Detta competenza è esclusiva **salvo diverso accordo tra le parti**.*

L'accordo attributivo di competenza deve essere:

a) *concluso per iscritto o provato per iscritto*;

Tale condizione ovviamente è difficile da accertare nel caso lo *Smart contract* sia negoziato e concluso su *Blockchain*

b) *in una forma ammessa dalle pratiche che le parti hanno stabilito tra di loro; o* **(è difficile tradurre tramite algoritmi il concetto di "pratiche")**

c) *nel commercio internazionale, in una forma ammessa **da un uso** che le parti conoscevano o avrebbero dovuto conoscere e che, in tale ambito, è ampiamente conosciuto e regolarmente rispettato dalle parti di contratti dello stesso tipo nel settore commerciale considerato.*

È DIFFICILE CONCORDARE TRAMITE ALGORITMI IL CONCETTO DI "***USI***"

2. *La forma scritta comprende qualsiasi comunicazione con mezzi elettronici che permetta una registrazione durevole dell'accordo attributivo di competenza.*

Da questa definizione è esclusa letteralmente **la *Blockchain*** ed in generale la tecnologia a "registro distribuito".

Per farvela rientrare sarebbe necessario operare una interpretazione estensiva della norma.

3. L'autorità o le autorità giurisdizionali di uno Stato membro alle quali l'atto costitutivo di un trust ha attribuito competenza a giudicare hanno competenza esclusiva per le azioni contro un

fondatore, un trustee o un beneficiario di un trust, ove si tratti di relazioni tra tali persone o di loro diritti od obblighi nell'ambito del trust.

4. Gli accordi attributivi di competenza e le clausole simili di atti costitutivi di trust non sono valide se in contrasto con le disposizioni degli articoli 15, 19 o 23 o se derogano alle norme sulla competenza esclusiva attribuita alle autorità giurisdizionali ai sensi dell'articolo 24.

5. Una clausola attributiva di competenza che fa parte di un contratto si considera indipendente dalle altre clausole contrattuali.

La validità della clausola attributiva di competenza non può essere contestata per il solo motivo che il contratto è invalido.

CAPO III RICONOSCIMENTO ED ESECUZIONE

SEZIONE 1 - Riconoscimento

Articolo 36

*1. La decisione emessa in uno Stato membro **è riconosciuta** in un altro Stato membro senza che sia necessario il ricorso ad alcuna procedura particolare.*

2. Ogni parte interessata può, conformemente alla procedura di cui alla sezione 3, sottosezione 2, chiedere una decisione attestante l'assenza di motivi di diniego del riconoscimento di cui all'articolo 45.

3. Se l'esito di un procedimento pendente davanti a un'autorità giurisdizionale di uno Stato membro dipende dalla soluzione di una richiesta di diniego di riconoscimento sollevata in via incidentale, tale autorità giurisdizionale è competente al riguardo.

SEZIONE 2 – Esecuzione

Articolo 39

*La decisione emessa in uno Stato membro che è **esecutiva** in tale Stato membro è altresì esecutiva negli altri Stati membri senza che sia richiesta una dichiarazione di esecutività.*

Articolo 40

Una decisione esecutiva implica di diritto l'autorizzazione a procedere a provvedimenti cautelari previsti dalla legge dello Stato membro richiesto.

Articolo 62

1. Al fine di determinare se una parte ha il ***domicilio*** *nel territorio dello Stato membro le cui autorità giurisdizionali siano adite, l'autorità giurisdizionale applica la propria legge nazionale.* ***(Conf. Art. 4)***

2. Qualora una parte non sia domiciliata nello Stato membro le cui autorità giurisdizionali sono adite, l'autorità giurisdizionale, al fine di stabilire se essa ha il domicilio in un altro Stato membro, applica la legge di quest'ultimo Stato.

Articolo 63

1. Ai fini dell'applicazione del presente regolamento, ***una società o altra persona giuridica*** *è domiciliata nel luogo in cui si trova:*

a) la sua sede statutaria;

b) la sua amministrazione centrale; oppure

c) il suo centro d'attività principale.

2. Per quanto riguarda l'Irlanda, Cipro e il Regno Unito, per «sede statutaria» si intende il «registered office» o, se non esiste alcun «registered office», il «place of incorporation» (luogo di acquisizione della personalità giuridica), ovvero, se nemmeno siffatto luogo esiste, il luogo in conformità della cui legge è avvenuta la «formation» (costituzione).

3. Al fine di definire se un trust ha domicilio nel territorio di uno Stato membro le cui autorità giurisdizionali siano adite, l'autorità giurisdizionale applica le norme del proprio diritto internazionale privato.

N.B. Da tutto ciò che si è detto la Convenzione Bruxelles I bis (Regolamento UE n.1215/2012 in vigore dal 10 gennaio 2015) **non sembrerebbe applicabile alla fattispecie che prevede l'operatività di *Blockchain* e Smart contract.**

E, per analogia, anche per il diritto processuale domestico.

Sarà quindi necessario trovare fonti alternative.

Norme a tutela dei consumatori

Tali difficoltà di applicazione riguardano anche le **norme a tutela dei Consumatori** di cui alla **Direttiva U.E. 2011/83** in tema di contratti **stipulati al di fuori dei locali commerciali.**

Articolo 5

Obblighi d'informazione per contratti diversi dai contratti a distanza o negoziati fuori dei locali commerciali

1. *Prima che il consumatore sia vincolato da un contratto diverso da un contratto a distanza o negoziato fuori dei locali commerciali o da una corrispondente offerta,* ***il professionista fornisce al consumatore le sequenti informazioni*** ***in modo chiaro e comprensibile****, qualora esse non siano già apparenti dal contesto:*

difficilmente si può sostenere che in caso di *Blockchain* e Smart contract il linguaggio utilizzato per un consumatore sia "***chiaro e comprensibile***".

Sarebbe quindi preferibile fornire una traduzione completa in linguaggio "naturale" che diventi parte dello Smart contract.

4.14) Le Risoluzione delle controversie in tema di *Smart contract*

Un esempio nell'UE:

La piattaforma ODR (On Line Dispute Resolution)

https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=IT

La piattaforma europea di risoluzione delle controversie online (ODR) è messa a disposizione dalla Commissione Europea per rendere gli acquisti online (**in Usa alcune *start up* stanno utilizzando una piattaforma simile in tema di *Smart contracts***) più sicuri e più equi tramite il ricorso a validi strumenti di risoluzione delle controversie.

Se si è residenti nell'UE, in Norvegia, Islanda o Liechtenstein (Paesi EFTA, ma manca la Svizzera), si può utilizzare per trovare la soluzione migliore al problema avuto come **consumatore**, affidandosi direttamente ad un professionista oppure utilizzando un Organismo di Risoluzione delle Controversie che si occupi del caso.

La piattaforma ODR non è collegata ad alcun professionista in particolare.

Si può utilizzare la piattaforma ODR in tutte le lingue dell'UE oltre che in islandese e norvegese.

La piattaforma ODR informerà il professionista della richiesta di assistenza.

Se il professionista è disposto a dialogare, si potranno scambiare messaggi direttamente attraverso il pannello interattivo e inviare allegati, come le fotografie del prodotto, o programmare una riunione online.

Si avrà un massimo di 90 giorni per raggiungere un accordo.

Il soggetto che si è rivolto al professionista tramite la piattaforma ODR e il professionista stesso possono interrompere i colloqui diretti in qualsiasi momento.

Il professionista può anche proporre un elenco di organismi di risoluzione delle controversie cui ricorrere invece di trovare una soluzione direttamente.

In questo caso si avranno 30 giorni per concordare un organismo di risoluzione delle controversie.

In assenza di accordo il caso sarà archiviato sulla piattaforma.

Se il professionista rifiuta categoricamente la richiesta di assistenza, una delle parti decide di non partecipare più alla procedura oppure se trascorrono 90 giorni senza esito positivo, si potrà ricorrere alle seguenti opzioni:

1) trovare una soluzione con l'aiuto di un organismo di risoluzione delle controversie. In questo caso, si avranno ulteriori 30 giorni per concordare con il professionista un organismo di risoluzione delle controversie autorizzato cui affidare la gestione del vostro caso.

2) utilizzare uno strumento di risoluzione delle controversie

Si potrà utilizzare la piattaforma ODR per risolvere il problema con l'aiuto di un organismo di risoluzione delle controversie autorizzato.

Gli organismi di risoluzione delle controversie sono soggetti terzi neutrali che aiutano i consumatori e i professionisti a risolvere le controversie in modo non conflittuale.

Generalmente il ricorso a tali organismi è più economico e più rapido rispetto all'avvio di azioni giudiziarie.

La piattaforma ODR informerà il professionista del reclamo.

Se il professionista accetta di utilizzare la procedura ODR, si dovrà concordare con lui un organismo di risoluzione delle controversie cui affidare la gestione del caso.

Dal momento in cui si presenta il reclamo si avranno 30 giorni per concordare un organismo di risoluzione delle controversie che si occupi del caso.

Se non si è riusciti a trovare in tempo un accordo su un organismo di risoluzione delle controversie o se il professionista ignora il reclamo, si può ricorrere ad un diverso strumento per la risoluzione delle controversie.

Per presentare un reclamo, è necessario prima registrarsi nel sistema.

4.15) Gli *Smart contracts* e gli *Incoterms ICC* 2020

Dal 1° gennaio 2020 è stata pubblicata la nuova edizione degli *Incoterms* da parte della *ICC*.

La medesima ICC ha siglato un accordo con Perlin che è una della più influenti piattaforme di certificazione *Blockchain* per poi elaborare un programma di gestione degli Incoterms.

The International Chamber of Commerce (ICC), *Blockchain development company Perlin and the Dubai Chamber of Commerce and Industry have signed an exclusive partnership for the distribution of innovative blockchain products developed under the newly established Centre of Future Trade based in Singapore.*

The Centre of Future Trade, established by ICC and ***Perlin*** *with the support of Enterprise Singapore, has now signed a major new distribution partner for its technology products with the Dubai Chamber now having exclusive rights to market and distribute innovative blockchain solutions, developed by ICC and Perlin, in the Middle East and Africa.*

"ICC is committed to helping business chambers and enterprises all over the world to access best-in-class technology in an ever-changing and dynamic landscape for global trade," said ICC Secretary General John W.H. Denton AO.

"With the highly respected Dubai Chamber helping to grow awareness for the pioneering technology developed by our Centre of Future Trade, we expect substantial industry adoption in their regions of influence."

Similar to Singapore, Dubai is a major global hub for business and international trade, with a hugely diverse range of commodities and industries moving through the region.

With prime strategic access to thriving markets throughout the Middle East and Africa, the Dubai Chamber is strongly positioned to help ICC and Perlin deploy commercial blockchain pilots.

"We are extremely excited to be working closely with ICC and Perlin to develop and deploy leading-edge blockchain solutions to support our very extensive base of members and regional partners to be at the forefront of trade innovation," said Khalil Haddad, Director of Strategy at the Dubai Chamber.

With recent global launch events in Paris and Rio de Janeiro and more to come, ICC continues to actively support Perlin in spreading awareness and adoption for its blockchain across ICC's 45 million members in over 100 countries.

The overarching goals of the initiatives for blockchain pilots include digital innovation for trade, greatly enhanced efficiencies and more sustainable industries.

"Working with ICC, Singapore Government and extremely active business organisations like the Dubai Chamber, Perlin will help enterprises integrate world-leading blockchain technology into their operations," said ***Dorjee Sun, CEO of Perlin****.*

"This includes helping enterprises of all sizes – from multinationals to micro-, small- and medium-sized businesses across all industries – to better participate in the global economy."

Si riporta un'intervista su queste tematiche effettuata a Mr. Dorjee Sun CEO e fondatore di Perlin

Below is a condensed transcription of ICC's conversation with Dorjee Sun:

TC: What were you doing before you started Perlin and before you became involved in blockchain?

DS: I originally was a tech-entrepreneur. I started my first software company while I was still in University. But about twelve years ago, I became very passionate about climate change and carbon. I ended up raising a facility for rain forest conservation that also sold carbon credits. We ended up raising a US$400 million facility to protect rain forests around the world and we did some of the first carbon deals with clients, such as Rio Tinto and Bank of America Merrill Lynch.

What was fascinating then was when the governments were unable to reach a consensus around what would happen post Kyoto – that was when I started looking at non-governmental instrument's things, like Bitcoin, blockchain, (and other) decentralized consensus mechanisms. So, it was from a very centralised initiative such as carbon credits and intergovernmental agreements on climate change that then lead me into blockchain.

TC: What inspired you to start Perlin?

DS: Perlin is hoping to become what I believe is a requirement for the future regime. If you think about any type of governance, you need to have some sort of monitoring. The power of blockchains is that it uses mathematics and technology and it allows humanity to reach a consensus on a piece of data, without having a central authority dictate to it.

So, if you think about land registry, you need a government to approve that the land you are purchasing is owned by you. If, for example, governments change, there is potentially a conflict of interest, where you could have some of the weaker governances resulting in conflicts over who owns what land. That's you're seeing in a lot of countries. What's fascinating about blockchain is that you can't have these double spin attacks, you can't have people reissue things, unless it has come to a consensus with a majority of the nodes on the network.

What truly inspired me was looking at what arguably was peak centralisation – before the GFC – you really had a lot of consensuses.

Then, after the GFC, you have a very fragmented world, a lot of trade disputes and a lot of conflicts – exiting and brexiting – all of these different types of shifts to soverign states. What blockchain embodies and what I hope for Perlin is that we can create an immutable ledger that records data that then can be seen as the single source of truth. If you are looking for evidence-based policy, you can have this ledger that actually is able to be immutable, that captures scientific readings, and that then can attest to whether something is authentic or not.

As a specific example of why we are working with ICC and working on the ***Incoterms® rules*** *is if you think about trade, now having millions if not billions of sensors, you can actually see if there has been an execution of a trade.*

Whether or not the goods have been shipped, or whether or not the goods have been frozen or overheated – as you can have sensors that monitor temperature.

We are able to use technology where there was previously a lot of guesswork and uncertainty.

That's where the blockchain technology comes in. You are able to transcribe that information onto a blockchain – and because it's public – people know it's never been tampered with or that it's not the private database of a company that may have a vested interest to not necessarily have an immutable source of truth.

TC: *You mentioned ICC's and Perlin's partnership, can you tell me more about this new project and how you think blockchain can help enable the future of Incoterms® rules?*

DS: ***ICC's role in trade has really blown my mind, and it's been such privilege to work with the organization. For those out there who don't know, over the last hundred years ICC has been helping to standardise trade. You don't really realise that until you look at conflicts that happened and fortunately in our lifetime global conflict has not happened.***

If you think about the Incoterms® rules, in 1936 ICC got together and helped standardise at what point was a good when shipped under a Incoterm® rule, or term of contract, was the obligation passed to the buyer and the seller. If you think about these transactions before, I wonder how they coordinated when someone no longer had responsibility over a good. Was it when the shipment was on the dock? You suddenly realise the complexity of this. Coming back, the great privilege that we have is that ICC is rebooting the Incoterms® rules. ICC will often tweak an update for global consensus. ***Incoterms® 2020****, which comes out later this year and will become the regime for which trade contracts will be updated in the future.*

The question we started discussing is what is relevant in 2020 and can we bring it in?

Given blockchain, sensor technology, remote sensing possible with satellites and drones, surely there is a way we can start reducing the paper load.

Some crazy stats showed that a majority of trade documentation would have at least one error in it and I've actually seen internal documentation from some of the big trade companies showing literally tens of thousands of emails being traded just to coordinate.

If we could digitalise, we could improve this process and make it more efficient.

On top of it, just imagine as the cost curve comes down, you are going to have thousands of sensors for a dollar – like sub one cent sensors. These sensors are going to be able to detect not only GPS location, time, temperature, moisture, so just think about it, if you can have all of these sensors transcribing to whether or not a shipment has been transported in the condition contracted.

Now, that brings in ***Smart contracts****.*

A ***Smart contract*** *is like a contract, but with software that is self-executing.*

You know, a couple of weeks ago I got food poisoning by having a rogue oyster, and during my daze, I started thinking about Smart contracts and ledgers.

I thought, what if you could see the journey of the oysters you buy, where they came from, when they were caught, their moisture level, if the temperature was right, when were they vacuum-sealed, do the sensors detect the compression or not?

These are the types of questions that should be determined in the near future, if you could be assured that any good you are buying has been transported under the conditions you have contracted and if not, you could seamlessly self-execute based under ***which Incoterm® rule*** *you have signed, based on the sensors and immutable ledger.*

That would then trigger a settlement.

You would get paid not needing a letter of credit.

What if you could tie into some form of currency or cryptocurrency for payment and settlement.

That is the essence of the supply chain becoming intelligent, becoming on blockchain, and having the Incoterms® rules as Smart contracts with cryptocurrency settlement.

TC: Another important fact would be the affordability of blockchain technology. Is this technology expensive and could micro, small and medium enterprises afford this technology one day?

DS: Not someday…today. I was talking about how this kind of technology would hopefully make trade much more accessible in the future. During the World Chamber Congress in Rio, the Minister explained that 99% of Brasil's economy is small- to medium-sized businesses, yet only 1% of export belonged to small- to medium-sized businesses.

If you look at centralised systems, the fact that you have sub 10 % banked in many developing economies. For example, in India 50% have mobile broadband. Why is the banking rate sub10? – simply because of the overarching burden of centralised systems. You can now create a decentralised wallet with decentralised financial tools. I believe we'll make it no longer that there is a gatekeeper that has to have Basel IV requirements on capital ratios.

I actually think the trend for centralised banking is only going to get more severe in terms of regulations, governance and disclosures. It will be harder and harder for people to bank centrally. Why as a bank would I continue taking risks on tiny loans or small accounts for small to medium-sized businesses? If you can create a blockchain that is cheaper to execute or parametric insurance that automatically pays out. For example, if there is smoke pollution from the haze in Singapore, from the rain forests in Indonesia, then what if the company – let's say it's an al fresco café – it knows its business is going to be affected, it automatically gets paid out.

This means that it does not have to apply for claims, fill out forms…the information is simply grabbed from the government-owned sensors, if the pollution level goes above a certain PSI then they get paid out.

There are all these ways to automate and reduce cost, which is going to make things much more accessible. If you had digital sensors on various forms of the logistics chain, if you also had Smart contracts and a web-enabled mobile app, you could do a sells agreement with ***a Smart Incoterm® rule****. Let's say Facebook's Libra coin suddenly becomes actionable.*

Then you could theoretically do international trade and settlement through Facebook's Messenger without having to touch all of the traditional systems which are currently a little prohibitive.

Coming back, this is an absolute boon for democratising and access, especially for small- to medium-sized businesses, blockchain and decentralised systems allow for peer-to-peer approval rather than having a potentially overburdened, overregulated central authority.

TC: You just mentioned Facebook's Libra coin, there are lots of other companies involved in this space at the moment, what separates Perlin from the pack?

How is Perlin different from other emerging blockchain companies or platforms?

DJ: Every single project gets to choose on which area of the decentralised economy they focus on. From our perspective, we are just really fascinated by trade.

We are based in Singapore, the world's second-biggest trader.

Singapore will most likely become the first in the next years, it facilitates over a trillion dollars of global trade, global trade is around 11 trillion – this is a very substantial amount.

We have been fortunate to work with some of the biggest commodity and trading houses, the government and customs, and we are working with all kind of agencies and organisations on our blockchain initiative.

What differentiates us on a technological level is our Wavelet ledger, which is the fastest benchmarked public blockchain, it can do 31 thousand transactions per second, it's super usable, rather than have our language that you have to learn in order to code Smart contracts there, we made ourselves very compliant with programming languages such as Go, Rust, JavaScript, and if you think about numbers, 11.7 million active developers are coding in JavaScript and these other languages so from this perspective it is very usable.

We also have a consensus mechanism, and we are far more decentralized in terms of the ability for people to rely on our consensus mechanism not being delegated proof of stake like some of the more centralized systems.

Bitcoin was conceived in 2008, then there were multiple waves on innovation, and now in 2019 we are building on the shoulders of earlier innovations, at this point we are cutting edge, and we hope to be for the foreseeable future. From a business and trade perspective, through our ICC partnership we also signed with Dubai and the United Arab Emirates, which is another forward-looking economy, we are working closely with a number of others, and hopefully, we'll be up to bring more trusted nods into the network. Singapore is one of those bases for global reach – particularly for something like a network – blockchain is a fantastic base to be positioned in, especially with strategic support from the government.

TC: Considering the strategic location of Singapore, could you tell me about this new ICC and Perlin initiative to establish the Centre for Future Trade there?

What are your goals for this project?

DS: We co-founded the ICC Centre for Future Trade, and we are collaboratively building it. If you think about the way in which the current industry is evolving, there is a bit of fragmentation, for example, a consortium of banks has created a product for letters of credit, and a competing consortium of banks is creating another letter credit product.

So, it's a bit fragmented and contrary to the wider thought of what's needed for connectivity and network effects, and so the main purpose of the Centre for Future Trade is to unify different fragmented consortiums.

From Singapore's perspective, ICC is the perfect partner to both globalize and push out standards, and Perlin is very fast-moving, developed, focused and also very agnostic. We're taking all of these tools, stitching them together and creating a platform.

The Centre will be focused on interoperable pilots, and try onboard a network effect of parties that can interoperate, we are operating on a synchronized application level. We also do research, for example how to put a price on the shift from paper to digital? How do you price a hybrid version of that? What would the world look like if we did have a coin such as Facebook's Libra?

There are all these different emerging areas, and we see Singapore as a very strategic hub to look at this because a lot of the digital adoption is tremendously strong in Asia – we have a very advanced regional community.

TC: Thank you Dorjee, I really appreciated you taking the time to discuss blockchain and the Incoterms® rules, if you would like to give a final point, the floor is yours.

DS: What is really inspiring about working in the trade space with ICC, even though right now we have trade wars, Brexit, all of these changes in terms of geopolitics, especially in 2020 after the level of Trump politics, what is exciting is that this gives away lots of opportunities, today more than ever we need ICC to standardise.

I am most proud of my environmental work, but what I am really concerned about is how governments have become so sovereign and commercial that there is no multilateral leadership in

terms of SDGs and environmental climate change issues and this is where ICC, with the Chambers Climate Coalition and all the work we are doing on supply chain traceability.

If you imagine a world in 10 years' time with sensors, nanosatellites, drones, with all forms of data collection and that date to be in the blockchain, so it's immutable, then the future should be continuous multidimensional data, using AI and algorithms you can know wheatear something is certified or not and we have real monitoring for evidence-based policy from governments and we'll fix this environmental crisis that's going to lead us to conflict.

The main mission is to think about how do we bring some form of truth and realistic planning and how do we use trade as becoming the anchor point for a sustainable world.

3.16) Cenni di normativa internazionale e comparata

In ambito internazionale molti sono gli Stati che hanno creato una definizione normativa riguardante *lo Smart contract*.

Come si può facilmente immaginare gli **Stati Uniti** hanno provveduto sin da subito ad emanare specifiche norme definitorie in merito a tale fenomeno; in particolare all'interno dello U.S. Code al titolo 15 è stato introdotto *l'Electronic Signatures In Global And National Commerce*[77] che dispone di una norma imperativa e inderogabile rispetto agli *Statutes* dei singoli Stati che attribuisce allo *Smart contract* la stessa valenza giuridica di un contratto redatto in forma cartacea.

Molti degli Stati hanno recepito tale normativa attraverso la possibilità di definizione giuridica di *Smart contract*.

Primo Stato fra tutti ad emanare una specifica definizione è quello **dell'Arizona** che, nel 2017, che definisce gli *Smart contracts* come "*softwares*" basati, a livello di programmazione, su eventi prestabiliti che memorizzano il proprio status e che agiscono in registri distribuiti"[78]; tale definizione molto generale e di ampio respiro è stata recepita anche da altri Stati come quello del **Tennessee** che però ha espanso la definizione in termini operazionali, includendo possibili attività

[77] https://www.law.cornell.edu/uscode/text/15/chapter-96

[78] R. Battaglioni, M.T. Giordano; 2019; Blockchain & Smart contract; pagina 368

come: 1) custodia e trasferimento di asset digitali 2) sincronizzazione di informazioni 3) gestione di attività attinenti all'autenticazione ed all'identità tramite *softwares* applicativi[79].

La definizione di *Smart contract* risulta molto spesso convergente come **Malta** (Malta *Digital Innovation Autority Act*), **Bielorussia** (DPR 8/2017), **Australia** (dove si equiparano gli *Smart contracts* a contratti telematici e conclusi per iscritto, nonché automatici[80]).

Dati i presupposti e le definizioni appena elencate, notiamo dunque come vi sia, nella classificazione giuridica degli *Smart contracts,* una convergenza alla struttura informatica alla base dello strumento, definendo lo stesso a livello minimo come un *software* auto-eseguibile al fine di dar luogo alle prestazioni delle parti, fino ad arrivare all'equiparazione dello stesso al documento contrattuale.

Nonostante ciò la legislazione vigente non lascia intendere come affrontare questioni circa l'applicazione di norme imperative[81] non derogabili dalle parti e che se presenti pregiudicano l'istituto giuridico con l'invalidità del contratto, altra questione non espressa dai legislatori in merito agli effetti dell'invalidità.

[79] https://legiscan.com/TN/text/SB1662/id/1802160

[80] https://www.mondaq.com/australia/new-technology/974460/Smarter-contracts-in-2020

[81] Norma imperativa è la norma proibitiva che, sulla base dell'esigenza di protezione di valori morali e sociali e di quelli fondamentali della comunità giuridica, tende non solo a negare efficacia giuridica alla programmazione negoziale ad essa contraria, ma tende più radicalmente a proibire l'azione programmata

4) *Le Cryptovalute*: profili giuridici

4.1) Storia ed inquadramento

Il protocollo *Bitcoin* (simbolo: ₿, codice: BTC o XBT), la prima delle *cryptovalute* (ora ce ne sono più di 2000 incluso un progetto di *cryptorublo* garantito e controllato dallo Stato Russo, di un Euro digitale elaborato dalla BCE, di una *cryptovaluta* privata pensata da *Facebook – Libra* -, sono acquistabili anche da Bancomat – a Torino il primo in Italia - , esistono già *futures* sui *Bitcoin/ cryptovalute* e le Banche di affari, come JP Morgan, che fino al 2018 vietavano ai propri consulenti di proporli ai propri clienti, ora hanno cambiato idea), **è nato ufficialmente il 3 gennaio 2009**, a seguito della pubblicazione di un *paper* scientifico, a firma Satoshi Nakamoto, intitolato "*Bitcoin*: *A Peer-to-Peer Electronic Cash System*" dell'8 agosto 2008 su "*The Cryptographic Mailing List*" del sito www.metzodowd.com

Satoshi Nakamoto, ha voluto creare un sistema di pagamento *online* che fosse sicuro e indipendente dalle autorità centrali, come per esempio le banche centrali.

La *cryptovaluta* sviluppata da Nakamoto viene eseguita utilizzando un *software open-source* lanciato nel 2009 e scaricabile da chiunque.

Fino alla metà del 2010 Nakamoto ha continuato a collaborare con altri sviluppatori del *software Bitcoin*; dopo questa data ha consegnato il codice sorgente al suo più stretto collaboratore, Gavin Andresen, interrompendo il proprio diretto coinvolgimento.

Per convenzione se il termine *Bitcoin*:

- è utilizzato con la lettera maiuscola significa che ci si riferisce alla tecnologia e alla rete,
- mentre se viene utilizzato con l'iniziale minuscola ci si riferisce alla valuta in sé.

bitcoin è quotato su siti appositi che si chiamano ***Exchenge***, all'interno dei quali è possibile scambiare *bitcoin* con Euro o una qualsiasi altra valuta.

Il *bitcoin* non è classificato come una moneta, bensì come un **mezzo di scambio che**, a differenza delle valute tradizionali:

1) non segue l'andamento della domanda e dell'offerta e
2) non necessita del supporto di un ente centrale.

La moneta *bitcoin* non è quindi creata da una banca centrale (il *cryptorublo* farebbe eccezione se verrà immesso sul mercato e così anche il *cryptoreminbi* di cui si parla anche se a seguito dello scandalo *Evergrande* la Banca Centrale Cinese alla fine di settembre 2021 ha vietato le transazioni in *cryptovalute* – Il sole 24 ore del 25 settembre 2021 pag. 4*)*, **ma viene conservata all'interno di un gigantesco *database* condiviso.**

Ogni partecipante alla rete può contribuire alla *Blockchain* (sulla *Blockchain* si veda il capitolo 1 della presente Guida) di *Bitcoin* ed estenderla.

Per garantire che i soldi appena spesi da un utente non siano riutilizzati per una seconda transazione cioè per evitare il fenomeno del *double-spending* - doppia spesa - cioè la possibilità di spendere una stessa unità di valuta digitale più volte, ad esempio inviando contemporaneamente lo stesso pagamento a due destinatari differenti, Satoshi Nakamoto ha inventato un meccanismo in cui **i controlli** sono **gestiti da una parte terza**, coinvolgendo l'utilizzo della crittografia (sulla crittografia si vedano i paragrafi 1.9 e seguenti della presente Guida)

Queste monete *bitcoins* vengono poi conservate all'interno di un **portafoglio virtuale**, formato da chiave privata e chiave pubblica.

Mentre

- **la chiave pubblica** serve per essere condivisa con tutti in modo che ogni utente sappia dove versare *bitcoin*,

- **la chiave privata** serve per rendere possibile l'accesso a quello specifico portafoglio e, di conseguenza, la gestione delle transazioni al suo interno.

Facciamo un esempio per capirne meglio il funzionamento.

Ipotizziamo due soggetti Sofia e Andrea.

Sofia deve inviare un documento ad Andrea.

Andrea comunica a Sofia la propria chiave pubblica.

Sofia cifrerà il documento da inviare con la chiave pubblica di Andrea.

Il documento viaggerà attraverso il canale di comunicazione e non potrà essere letto da nessuno perché è stato cifrato.

Nel momento in cui il documento arriva ad Andrea egli potrà decifrarlo solo ed esclusivamente con la propria chiave privata.

Schema della crittografia a chiave pubblica (Fonte: nellopetrazzuolotesina.wordpress.com)

La crittografia asimmetrica ha un'altra importante applicazione, cioè la **firma digitale**, in cui la crittografia assume la funzione di metodo di identificazione informatica.

(si veda il capitolo 1 della presente Guida)

La critica principale a *bitcoin* riguarda la **difficoltà a controllare l'utilizzo di questa moneta virtuale,** dal momento in cui **gli operatori che la emettono non ne sono i proprietari** e agiscono in un contesto multinazionale senza l'influenza degli strumenti di politica monetaria delle banche centrali.

Questa è la ragione per cui il Legislatore Italiano l'ha disciplinata in tema di normativa antiriciclaggio.

DIRETTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2018

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 le direttive **2009/138/CE** (*2) «moneta elettronica», il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica;*)

e 2013/36/UE

DEFINISCE «*18)* «***valute virtuali**»: **una 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*»;

La Banca d'Italia in un *Occasional Paper* del **18 marzo 2019** ha avuto modo di precisare che: le *cryptovalute:*

"*non sono moneta legale di stato – fiat money -, depositi o fondi, né una passività di una Istituzione e nemmeno una moneta avente un valore intrinseco – outside money – come l'oro o l'argento".*

Da queste due definizioni si ricava che le *cryptovalute* costituiscono oggetto di diritti e come tali hanno la possibilità economica e giuridica di circolare.

Dopo i *bitcoins* la cryptovaluta più diffusa è *ethereum*

Ethereum

Ethereum è una **piattaforma decentralizzata** creata allo scopo di pubblicare ed utilizzare gli *Smart contracts* (si veda il Capitolo 3 della presente Guida).

Per poter utilizzare questa piattaforma, i contraenti devono pagare l'utilizzo della potenza tramite un'unità di conto chiamata ***ether***.

Quindi anche l'*ether* assume il ruolo di una *cryptovaluta*.

I contratti che utilizzano *Ethereum* sono trattati in maniera completamente sicura e potrebbero essere usati per eseguire un ampio numero di operazioni, dai sistemi elettorali, ai mercati finanziari fino alla regolamentazione della proprietà industriale.

Questa piattaforma fu creata il 30 luglio 2015 da Vitalik Buterin ed è considerata parte di un gruppo di piattaforme *Blockchain* 2.0.

Al contrario di *Bitcoin*, che ha un limite di 21 milioni, *Ethereum* non ha un tetto massimo per il numero di *ether* producibili.

Lo scopo di *Ethereum* è quindi quello di immagazzinare diversi tipi di dati, non solo quelli finanziari e di utilizzarli sfruttando la trasparenza ed immodificabilità della *Blockchain*.

4.2) Natura Giuridica delle Cryptovalute

Dal contratto di permuta al *bitcoin*

4.2.1) Moneta: origine e funzioni

Prima della comparsa della moneta le transazioni economiche venivano effettuate tramite la permuta/baratto, consistente nello scambio di un bene o servizio con un altro.
Per poter essere attuata la permuta implica una coincidenza di bisogni che però non sempre è possibile.
Proprio per questo motivo era necessario trovare una forma alternativa di scambio di beni e servizi. Egiziani, Fenici e Cartaginesi basarono su di esso gran parte dei loro scambi commerciali utilizzando soprattutto il bestiame per la sua abbondanza; la lingua italiana mantiene ancora oggi tracce di questa epoca storica[82].

[82] Es. "Capitale" dal latino *caput* – testa o capo di bestiame oppure il termine "Pecunia" dal latino *pecus* – gregge.

Con lo sviluppo del commercio ed i frequenti spostamenti l'uso del bestiame risultò inadeguato; si giunse quindi ad individuare nei metalli una valida alternativa per caratteristiche quali facile trasportabilità e inalterabilità.
Il primo tipo di moneta metallica, in bronzo e rame, è stato realizzato in Cina intorno al 1000 a.C. mentre nel mondo occidentale ebbe inizio in Lidia intorno alla metà del VII secolo a.C. all'epoca di re Gige il quale impiegò l'elettro, lega naturale di oro e argento, per la monetazione[83].
In Europa l'uso delle monete di metallo ha prevalso per molti secoli fin quando nel 1661 la Svezia non ha emesso le prime banconote.
Da quel momento in poi molti governi europei hanno impiegato le banconote soprattutto per la loro più facile circolazione.

Nel corso della storia la moneta è stata chiamata a svolgere tre funzioni:

1. unità di conto: la moneta viene usata per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro agevolando così le decisioni economiche e gli accordi contrattuali;
2. riserva di valore: la moneta può essere conservata ed utilizzata in un tempo futuro senza che si deteriori in senso fisico o nel suo potere d'acquisto;
3. mezzo di pagamento: la moneta viene utilizzata per l'acquisto di beni e servizi e non può essere rifiutata dal destinatario del pagamento[84] tranne nel caso in cui le parti abbiano stabilito mezzi di pagamento diversi.

4.2.2) Sistema dei pagamenti

Con il termine pagamento in diritto civile si indica in generale sia l'adempimento di un'obbligazione di dare diversa dal danaro sia l'adempimento di **un'obbligazione pecuniaria**.

S'intende il modo di estinzione tipico delle obbligazioni che vengono definite come il vincolo giuridico che si crea tra due o più soggetti, creditore e debitore, in base al quale il debitore si impegna a compiere una prestazione a favore del creditore secondo le regole dell'ordinamento giuridico.

[83] E. De Simone, *Moneta e banche attraverso i secoli*, Franco Angeli, 2002.
[84] In Italia il valore 'liberatorio' del pagamento in moneta è stabilito dall'art. 1277 c.c.

Per adempiere ad un'obbligazione pecuniaria ci si avvale degli strumenti di pagamento[85].

Contante

Costituito da banconote e monete, il contante viene spesso utilizzato per effettuare transazioni di importo limitato tra soggetti fisicamente presenti.
In Italia, dove la moneta legale è l'Euro, le transazioni tra privati di importo superiore a 3.000 euro (la soglia si riduce a 2.000 euro, arrivando a 1.000 euro a partire dal 1° gennaio 2022) devono essere effettuate con strumenti alternativi al contante[86].

Assegno

In Italia si tratta di un titolo di credito (in molti altri Paesi però non ha questa natura giuridica come ad esempio in USA) cartaceo e ne esistono di due tipi: quello bancario e quello circolare.
L'assegno bancario contiene l'ordine scritto impartito da un correntista alla propria banca di pagare a terzi (o a se stesso) una somma di denaro.
L'assegno circolare invece viene emesso dalla banca e consegnato al cliente che ne ha fatto richiesta in favore di un soggetto il cui nome viene riportato sul titolo.

Bonifico

È un ordine di pagamento che viene effettuato da un soggetto, ordinante, indirizzato presso il proprio istituto bancario, affinché quest'ultimo trasmetta una somma di denaro presso una banca controparte, con la richiesta di versare tale somma ad un beneficiario.

Addebito diretto

Si tratta di un servizio con cui un correntista ordina alla propria banca di accettare sul proprio conto corrente gli addebiti provenienti da un determinato creditore.
Normalmente questa modalità viene utilizzata nei casi in cui si debbano effettuare dei pagamenti periodici come ad esempio **il pagamento delle utenze domestiche**.

[85] https://www.bancaditalia.it/compiti/sispaga-mercati/strumenti-pagamento/
[86] Art. 1, comma 899 L.208/2015 – cosiddetta legge di stabilità 2016

Carte di pagamento

Sono delle tessere plastificate, emesse da una banca o da un altro istituto finanziario, dotate di una banda magnetica e/o *microchip* che permettono al titolare di usufruire di diversi servizi finanziari. Vengono anche utilizzate per concludere transazioni di commercio elettronico in internet e possono essere di credito, di debito e prepagate.

La carta di credito consente di poter effettuare sia acquisti presso gli esercenti convenzionati che prelievi di contante presso gli sportelli automatici.

Gli importi spesi vengono addebitati sul conto corrente del titolare in un'unica soluzione o a rate normalmente con cadenza mensile.

Come la carta di credito, quella di debito consente acquisti presso gli esercenti convenzionati e prelievi di contante da sportelli automatici.

Sono previsti però limiti di importo mensili per gli acquisti e limiti mensili e giornalieri per i prelievi in contante.

Al titolare di queste carte i fondi spesi o prelevati vengono addebitati nel momento stesso in cui vengono spesi o prelevati.

La carta prepagata consente di effettuare pagamenti e prelievi dal momento in cui le somme di denaro vengono depositate dal titolare presso l'emittente e non necessitano di un conto corrente di appoggio.

Servizi di pagamento in Internet (*e-payments*) e (*m-payments*)

Vengono utilizzati esclusivamente tramite il circuito internet; i secondi però vengono realizzati tramite telefono cellulare (*Smartphone*) o altro dispositivo mobile.

È previsto l'uso di una carta di pagamento virtualmente inserita nel dispositivo o associata alla *sim card.*

Possono essere effettuati sia pagamenti in presenza (es. bar, metro) che da canale remoto (es. *App-store, Internet shop*); inoltre se il dispositivo lo consente e la carta di pagamento associata è abilitata alla tecnologia *Near Field Communication* (NFC) è possibile pagare anche in modalità *contactless*, semplicemente accostando il dispositivo all'apparecchiatura di accettazione presente nel negozio (POS).

4.2.3) Le monete alternative

La moneta a corso legale, o *fiat*, è uno strumento di pagamento privo di valore intrinseco ma che possiede valore perché esiste un'autorità statale che agisce come se avesse questo valore.
Se una collettività emette, usa e accetta qualcosa come pagamento, automaticamente quel qualcosa acquisisce valore, dato che è riconosciuto come mezzo di scambio.
Fin dal medioevo è scaturita la necessità, da parte di gruppi di persone aventi interessi comuni, di utilizzare, in alternativa o in contemporanea, delle monete diverse da quelle a corso legale per far fronte a problemi come guerre, carenza di liquidità e altro.
Si tratta di monete che non avendo corso legale vengono accettate solo su base volontaria[87].
Ad oggi nel mondo esistono più di 5 mila valute complementari e vari Stati come Francia, Austria, Italia e soprattutto Germania le stanno sperimentando con grande successo.

Qui di seguito alcuni esempi.

1) **Tra il XII e il XVIII secolo in Francia** vennero emessi i **Méreaux**, oggetti realizzati con materiali poveri, da soggetti non autorizzati a battere moneta utilizzati per effettuare determinati acquisti.

2) A Toreke citta belga è stata istituita, negli anni scorsi, come moneta il Toreke per la realizzazione di opere sociali e ambientali tramite la riqualificazione degli spazi urbani e la creazione di un grande giardino comunitario.

3) Mentre l'Epi è nata per sostenere l'agricoltura e l'economia locale[88].

4) **In Italia** invece sta riscuotendo molto successo **il Sardex**, lanciato nel 2010 da cinque imprenditori sardi che hanno creato un Circuito di Credito Commerciale in cui sono le imprese stesse a farsi credito a vicenda in una valuta alternativa.

L'obiettivo è di far girare l'economia risparmiando liquidità.

[87] M. Kennedy, *Il denaro libero da interessi ed inflazione*, Arianna Editrice, Trieste, 2002.
[88] https://www.ilfattoquotidiano.it/2014/04/07/crisi-economica-le-monete-complementari-che-sfidano-lausterita/942155/

Altre 11 regioni italiane hanno replicato con successo il modello nato in Sardegna: Piemonte, Valle d'Aosta, Lombardia, Veneto, Emilia-Romagna, Marche, Umbria, Lazio, Campania, Abruzzo, Molise e vantano circa 5 mila iscritti.

5) Inoltre, possono essere considerate **valute complementari** anche le miglia accumulate dai viaggiatori aerei, i punti dei supermercati o delle stazioni di servizio, i buoni pasto, i punti raccolti con le ricariche telefoniche, ecc.

4.2.4) La Rivoluzione informatica

Nel corso degli anni **Internet** è riuscito a rivoluzionare ogni settore della vita dell'uomo ed anche i sistemi di pagamento e le valute si sono evolute nel tempo sentendo il bisogno di un continuo aggiornamento in linea con le nuove tecnologie.

In questo contesto si inserisce la creazione delle **VALUTE VIRTUALI**.
Come si diceva si tratta di una forma di denaro privato non supportata da alcuna banca centrale ed essendo priva di entità fisica viene creata, memorizzata ed utilizzata su *computer* ed altri dispositivi elettronici come *Smartphone* e *tablet*.

Da questa "filosofia" negli ultimi anni hanno fatto la loro comparsa le ***CRYPTOVALUTE***, una nuova tipologia di moneta legata alle tecnologie informatiche **che utilizza la crittografia per funzionare**.

Le *cryptovalute* nascono per essere **la moneta di Internet** e sono state progettate per sostituire il denaro contante.

Fra le valute virtuali[89] in circolazione, *bitcoin* è quella più conosciuta ed è considerata dai suoi ideatori **un'alternativa alla moneta avente corso legale.**

Risulta quindi fondamentale capire se è possibile considerare questa *cryptovaluta*:

[89] **La BCE ad Ottobre del 2012 ha definito le valute virtuali** come "una forma di moneta digitale non regolata, che viene emessa e controllata dai suoi sviluppatori, utilizzata ed accettata tra i membri di una specifica comunità virtuale", cfr. ECB, *Virtual Currency Schemes*, Ottobre 2012, in https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

- una moneta,
- una moneta elettronica,
- un bene,
- uno strumento finanziario
- o qualche altra cosa.

4.2.5) *Bitcoin/cryptovalute* e moneta

È necessario chiedersi inizialmente se è possibile inquadrare *bitcoin* e le altre *cryptovalute* come moneta.

Parte della dottrina ritiene che la *cryptovaluta* **non sia riconducibile** al concetto di moneta in quanto, secondo la **Teoria statalista, per definire una valuta come "moneta",** gli Stati sovrani debbono aver potere su di essa essendo un'istituzione creata e garantita dallo Stato:

a) **con il corso legale** lo Stato attribuisce alla moneta il potere liberatorio delle obbligazioni pecuniarie e

b) **con il corso forzoso** si ha l'impossibilità da parte del creditore di rifiutarla come mezzo di pagamento.

Quindi in base alla teoria statalista le valute virtuali non possono essere considerate monete dato che nessuno Stato **(si tenga però presente che dal 7 settembre 2021 lo Stato di El Salvador ha introdotto il bitcoin come moneta legale)** le ha riconosciute come moneta avente corso legale e non sono autorizzate, emesse o garantite da alcuna banca centrale.

Le *cryptovalute* **vengono generate da soggetti privati** e il loro utilizzo come mezzo di pagamento presuppone l'accordo delle parti secondo il Principio **di autonomia contrattuale.**

DOMANDA: il pagamento tramite *cryptovaluta* potrebbe rientrare tra le obbligazioni naturali ex art. Art. 2034. c.c.?

Art. 2034 - Obbligazioni naturali.

Non è ammessa la ripetizione di quanto è stato spontaneamente prestato in esecuzione di doveri morali o sociali, salvo che la prestazione sia stata eseguita da un incapace.

I doveri indicati dal comma precedente, e ogni altro per cui la legge non accorda azione ma esclude la ripetizione di ciò che è stato spontaneamente pagato, non producono altri effetti.

Se si esclude il caso recente di El Salvador che ha reso il *bitcoin* moneta di stato penso proprio di sì

Inoltre, secondo la **teoria economica <u>la moneta assolve alle funzioni</u>:**

1) <u>di riserva di valore</u> in quanto la moneta può essere conservata ed utilizzata in un tempo futuro senza che si deteriori nel suo potere d'acquisto,

2) <u>unità di conto</u> in quanto permette di misurare in modo oggettivo il valore dei beni e dei servizi,

3) <u>mezzo di scambio</u> in quanto finalizzata a consentire gli scambi commerciali.

Aggiungo altre motivazioni del perché i *bitcoin* e le *cryptovalute* <u>non</u> si possono considerare moneta:

Secondo la Banca Centrale Europea (BCE)[90] le valute virtuali <u>non</u> riuscirebbero ad assolvere perfettamente alle 3 funzioni sopra descritte:

1) essendo il *bitcoin* caratterizzato allo stato attuale da un elevato livello di volatilità <u>la funzione di riserva di valore non sembra essere soddisfatta</u>;

2) non avendo il *bitcoin* forza legale in nessuno Stato (**eccetto dal 7 settembre 2021 El Salvador**) <u>la funzione di mezzo di scambio dipenderebbe solo da un accordo delle parti</u> e

[90] Cfr. BCE, *Virtual Currency Schemes – a further analysis*, febbraio 2015.

allo stato attuale il numero di transazioni giornaliere evidenzia un livello di accettazione ancora troppo ridotto;

3) infine per quanto riguarda la funzione come unità di conto questa sarebbe compromessa dalle stesse incertezze del mercato dei cambi in quanto gli utilizzatori di *bitcoin* per compiere le loro scelte fanno riferimento alle valute ufficiali.

4.2.6) *Cryptovalute* e moneta elettronica

Il *bitcoin* e le *cryptovalute* non devono essere confuse con il concetto di moneta elettronica.

Secondo la Direttiva n. 2009/128/CE[91] **la moneta elettronica** è "*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica,* ***rappresentato da un credito nei confronti dell'emittente*** *che sia emesso per effettuare operazioni di pagamento (…) e che sia accettato da persone fisiche e giuridiche diverse dall'emittente*".

Da questa definizione possiamo notare che il *bitcoin* ed ogni altra valuta virtuale **non** possono essere considerate moneta elettronica dato che **non è prevista la ricezione di fondi**.

Inoltre **l'articolo 11 comma 2 della stessa direttiva** recita: "*Gli Stati membri assicurano che, su richiesta del detentore di moneta elettronica, gli emittenti di moneta elettronica rimborsino, in qualsiasi momento e al valore nominale, il valore monetario della moneta elettronica detenuta*", questo requisito nell'ambito delle *cryptovalute* non può essere soddisfatto perché tutte le transazioni che vengono effettuate sono irreversibili in quanto "viaggiano" sul "binario" della *Blockchain.*

[91] Direttiva 2009/110/CE del 16/9/2009 concernete l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica.

4.2.7) *Cryptovalute* e moneta complementare

Secondo alcuni autori[92] esiste una certa analogia fra le valute virtuali e le monete complementari dato che quest'ultime come le prime non hanno valore legale, **vengono emesse da privati** e quindi **sono accettate esclusivamente su base consensuale.**

Ciò nonostante esistono delle **differenze**: le monete complementari hanno come principale finalità economica quella di fortificare i legami economici entro una comunità circoscritta geograficamente (esempio Sardex) mentre le valute virtuali sono caratterizzate, grazie alla rete, da una dimensione globale.
La disciplina negoziale prescrive che le monete complementari possano essere detenute entro limitati periodi di tempo e che possano essere utilizzate per finalità di permuta o di scambio di servizi fra i soggetti che aderiscono allo schema; inoltre non possono essere convertite in moneta legale e non si possono eseguire transazioni anonime o non tracciabili.

Da questo è possibile desumere che nonostante ci siano delle caratteristiche in comune le valute virtuali **non** possono essere equiparate alle monete complementari.

4.2.8) *Cryptovalute* come bene?

Avendo escluso la natura di moneta e di moneta elettronica dei *bitcoins* **possiamo chiederci se le *cryptovalute* possono essere considerate dei beni.**

Secondo **l'articolo 810 del Codice civile italiano** "*sono beni le cose che possono formare oggetto di diritti*".

A) Una parte della dottrina ha provato ad inquadrare il *bitcoin* come un bene mobile e soprattutto, essendo privo di materialità, come un bene mobile immateriale/incorporale.

[92] G. Arangüena, *Bitcoin: una sfida per policymakers e regolatori*, in Diritto mercato tecnologia, gennaio/marzo 2014, p. 28.

Come sottolineato da alcuni Autori[93] il *bitcoin* può essere considerato come "una nuova categoria di bene immateriale/incorporale, a sé stante, ma con dei punti di contatto con la proprietà intellettuale".

Anche se il *bitcoin* non può essere completamente equiparato a un prodotto dell'ingegno è pur vero che l'acquisto della proprietà a titolo originario del *bitcoin* deriva da un lato dall'impiego di risorse economiche e dall'altro lato dall'utilizzo di risorse per così dire "intellettuali", essendo **le operazioni svolte da macchine**, che danno origine ad un bene nuovo privo di materialità intrinseca.

Come per le creazioni dell'ingegno la natura di bene immateriale di *bitcoin* non viene meno per il fatto di essere incorporata in un bene fisico: un conto sono i supporti su cui sono salvate e conservate le unità di *cryptovaluta,* un conto è il diritto di disporne.

È possibile quindi identificare un bene immateriale/incorporale anche quando questo venga conservato o si estrinsechi tramite un supporto fisico.

A differenza della proprietà intellettuale in senso classico tuttavia un'unità di *bitcoin* è tipicamente, per la dottrina economica, **un "bene rivale"** dato che non può essere utilizzato nel contempo da più di un proprietario.

B) C'è invece chi sostiene che considerare i *bitcoins* come beni immateriali/incorporali possa creare problemi riguardo la natura dei diritti che su di essi insistono.
I beni immateriali/incorporali sono tipici: il diritto sul bene immateriale/incorporale esiste se esiste una norma che lo riconosce e nel caso dei *bitcoin* una norma non c'è[94].

4.3) *Cryptovalute* e documento informatico

A) È stata proposta in dottrina la ricostruzione della fattispecie quale **documento informatico**, cioè di rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, così come

[93] P.L. Burlone, R. de Caria, *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale*, in IBL Focus, 234, aprile 2014, 4.
[94] R.Vigorita, F. Ilacqua, "*Profili giuridici del Bitcoin: la moneta diventa digitale*", disponibile sul sito http://www.iurisprudentes.it/2016/05/19/profili-giuridici-del-bitcoin-la-moneta-diventa-digitale/

definito **dall'art. 1, c.1, lett. p, D.lgs. n. 82/2005 Codice Amministrazione Digitale**.

In base alle caratteristiche della tecnologia utilizzata dalla *Blockchain*, il *bitcoin* potrebbe essere considerato come un documento informatico portante dati ed informazioni giuridicamente rilevanti e **sottoscritto da una progressione di firme elettroniche attestanti l'avvenuta validazione della propria o dell'altrui legittimazione al perfezionamento di una certa transazione** (cioè, a seconda dei casi, a possedere, avere, spendere, trasferire, acquistare e vendere un determinato bene o servizio, ovvero una determinata quantità di essi).

Conseguentemente "*il bitcoin sarebbe idoneo a garantire, seppure su basi pseudoanonime, la legittimazione e l'adempimento automatico del possessore, in quanto elementi negoziali direttamente incorporati quali dati e rappresentazioni informatiche giuridicamente vincolanti ex ante, e non lasciati al solo (mutevole) giudizio ex post sulla meritevolezza degli scopi economici conseguibili con il loro utilizzo*".[95]

B) Alcuni autori invece sottolineano che "nel caso del *bitcoin* **lo *script* digitale che lo costituisce non rappresenta alcunché**, ma risulta essere semplicemente "un valore" e come tale spendibile per la soddisfazione di interessi del proprietario dello stesso".[96]

4.4 *Cryptovalute* e strumento finanziario/prodotto finanziario?

Ad oggi molti investitori sono stati spinti ad acquistare *bitcoins* non tanto per utilizzarli come mezzo di pagamento nelle transazioni ma con l'obiettivo di ottenere considerevoli profitti dalle oscillazioni del tasso di cambio rispetto alla moneta legale.

Per questo motivo un'ulteriore ipotesi da considerare è quella di **provare a ricondurre i *bitcoins* alla categoria degli strumenti finanziari**.

A) Problema: In base **all'art. 1, comma 2, del D.lgs. n. 58/1998 (TUF**) "*gli strumenti di pagamento non sono strumenti finanziari*": se *bitcoin* lo si considera **solo** come strumento di

[95] G. Arangüena, *Bitcoin: una sfida*, cit., p. 32.
[96] A. Capogna, et al., *Bitcoin: profili giuridici e comparatistici*, cit., p. 44.

pagamento come la moneta legale, non può rientrare in tale categoria[97].

B) Tuttavia - il **Tribunale di Verona** si è espresso sull'acquisto di valuta virtuale tramite una società promotrice finanziaria di una piattaforma di *crowdfunding*.

Il Tribunale ha ritenuto che fosse integrata **la prestazione di un "servizio finanziario" secondo il D.lgs. n. 206/2005 (Codice del Consumo)**.

Ai sensi dell'art. 67-ter, comma 1, lett. b) per "*servizio finanziario*" si intende "*qualsiasi servizio di natura bancaria, creditizia, di pagamento, di investimento, di assicurazione o di previdenza individuale*".
È stato quindi affermato che *bitcoin* sarebbe "*uno strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni online 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*"[98].

Parte della dottrina, partendo da un inquadramento ampio del significato di prodotto finanziario come un prodotto che determina una rendita al suo possessore ed un "guadagno finanziario" ricomprende i *bitcoins* e le *cryptovalute* in questo alveo non limitandone la funzione a solo strumento di pagamento.

Questa opinione fa rientrare i *bitcoins* e le *cryptovalute* all'interno dei **prodotti finanziari definiti dall'art. 1, comma 1, lettera u) del TUF** come "*gli strumenti finanziari e **ogni altra forma di investimento di natura finanziaria**...*".

Il *genus* dei prodotti finanziari è costituito dalla somma di due sottoinsiemi:

1) uno relativo agli strumenti finanziari, tendenzialmente "chiuso", e
2) un altro "aperto" destinato a essere "riempito" ogni volta interpretando e analizzando il caso concreto[99].

[97] P.L. Burlone, R. de Caria, *Bitcoin e le altre cryptomonete,* cit. 3.
[98] Tribunale di Verona, 24 gennaio 2017, n. 195.
[99] G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?* in Diritto dell'informazione e dell'informatica (II), fasc. 3, maggio-giugno 2015, 426.

La CONSOB ha sottolineato che rientrano nella categoria di prodotto finanziario le proposte di investimento che necessitano della presenza di tre elementi:

a) impiego di capitale;
b) aspettativa di rendimento di natura finanziaria;
c) assunzione di un rischio direttamente connesso e correlato all'impiego di capitale.

Come osservato dalla CONSOB "*per configurare un investimento di natura finanziaria, non è sufficiente che vi sia accrescimento delle disponibilità patrimoniali dell'acquirente* (cosa che potrebbe realizzarsi attraverso talune modalità di godimento del bene come ad esempio con la rivendita di un diamante precedentemente acquistato con **la clausola di retrovendita**) *ma è necessario che l'atteso incremento di valore del capitale* impiegato (ed il rischio ad esso correlato) ***sia elemento intrinseco all'operazione stessa***"[100].

Ne consegue che, nel caso in cui l'acquisto di *bitcoin* assuma la funzione di "investimento di natura finanziaria", **la causa concreta dell'acquisto potrebbe far rientrare il *bitcoin* nella nozione di "prodotto finanziario**".

4.5) I vantaggi di *bitcoin* e delle *cryptovalute*

Diversi sono i **VANTAGGI** derivanti dall'uso dei *bitcoins* e delle *cryptovalute*.

Un primo elemento che ne ha consentito il successo e lo sviluppo è sicuramente la **rapidità** con cui i vengono scambiati **soprattutto per le transazioni verso l'estero**.

Gli utilizzatori possono infatti beneficiare:

1) di tempi di verifica e di regolamento della transazione molto più brevi (indipendentemente dalla distanza geografica fra le parti) rispetto ai tradizionali metodi di pagamento sinora utilizzati con i quali possono essere necessari diversi giorni lavorativi affinché l'operazione venga convalidata.

[100] Comunicazione CONSOB n. DTC/13038246 del 6-5-2013 disponibile sul sito http://www.consob.it/documents/46180/46181/c13038246.pdf/e17116af-cbb1-4d3e-b8d1-f921d3ccb0a8

2) Altro vantaggio da considerare è che un'operazione eseguita tramite *cryptovaluta* comporta costi di transazione notevolmente più bassi rispetto ai servizi di pagamento tradizionali, anzi normalmente non viene corrisposta nessuna commissione salvo il caso in cui l'utente voglia corrispondere una *fee* in cambio di una maggiore velocità di conferma.

   L'importo della commissione comunque non dipende dalla quantità di *bitcoin/cryptovaluta* da inviare, ma da altri fattori come congestione della rete, tempistiche di conferma della transazione[101] ecc...
   Tutte le operazioni bancarie hanno dei costi più o meno elevati, ragion per cui una fascia di popolazione economicamente più debole non riesce ad accedere al sistema bancario; il *bitcoin* e le *cryptovalute* invece stante la quasi nullità dei costi possono essere un valido strumento per avvicinare i soggetti economicamente più deboli al mondo della finanza.

3) Un'altra caratteristica positiva derivante dalle *cryptovalute* è che il loro utilizzo facilita le operazioni di *crowdfunding*.
   Gli utenti hanno la possibilità di poter effettuare molte microtransazioni sostenendo costi molto bassi, questo quindi può favorire forme di microfinanziamento utili alle imprese per i loro progetti imprenditoriali (si vedano in tema di ICO i paragrafi 2.1 e 2.2 della presente Guida).

4) Infine rispetto alla moneta a corso legale le *cryptovalute* non possono essere confiscate non essendo soggette al controllo di nessuna autorità centrale[102].

PROBLEMA PRATICO:

è possibile conferire una *cryptovaluta* come capitale sociale di una Spa o di una Srl?

Il Tribunale di Brescia – 18 luglio 2018 e La Corte d'Appello di Brescia - 24 ottobre 2018 non danno questa possibilità in quanto la *cryptovaluta* non sarebbe facilmente individuabile nel proprio valore in quanto soggetto a forte oscillazione e quindi di non chiara "*valutazione economica*" in

[101] https://help.wirexapp.com/hc/it/articles/115000219854-La-commissione-Blockchain-%C3%A8-troppo-alta-Perch%C3%A9-Che-dovrei-fare-
[102] N. Passarelli, *Bitcoin e antiriciclaggio*, 15 novembre 2016 disponibile sul sito http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/bitcoin-e-antiriciclaggio.html

tema di Srl ex art. 2464 secondo comma c.c. inclusa la "procedure di stima" ex artt. 2264 c.c. e 2265 c.c. (art. 2253 c.c.) (Per le Spa si veda anche l'art. 2343 commi terzo e quarto in tema di revisione di stima dei conferimenti e l'art. 2343 ter comma secondo lettera a) e b)).

Nella fattispecie specifica la *cryptovaluta* era stata creata dai soggetti che operavano il conferimento nella Srl ed era negoziata su un *exchange* di poco interesse. (Se la erano suonata e cantata, come si suole dire)

Se invece quella *cryptovaluta* fosse stata diffusa sul mercato e scambiata su piattaforma *exchange* di "pubblico dominio" il ragionamento del Tribunale di Brescia non reggerebbe, perché la *cryptovaluta* avrebbe avuto un tasso di liquidità facilmente accertabile e di "pubblico dominio" **ex art. 1474 secondo comma c.c.**

Le *cryptovalute* commercialmente diffuse, rientrando nella categoria dei beni immateriali/incorporali, si può ipotizzare che siano conferibili come beni in natura dietro opportuna perizia di stima.

L'impostazione data dal Tribunale di Brescia si basava ancora sulla vecchia considerazione che il **capitale sociale** di un'impresa costituisca la garanzia per i creditori sociali, mentre oramai è pacifico che la funzione del capitale sociale sia quella di considerarlo come **uno strumento di produttività** ed i creditori sociali troveranno ristoro dalla **redditività dell'impresa** attuando una **visione economico-dinamica** e non più economico-statica (In ambito economico si valuti in parallelo l'evoluzione storica del concetto di PIL)
In definitiva le *cryptovalute* possono conciliarsi con la suddetta visione produttivistica del capitale qualora possano prontamente essere convertite in valuta avente corso legale in virtù di un tasso di cambio espresso da mercati digitali oppure direttamente scambiate all'interno della catena *Blockchain* per l'acquisto di beni e servizi funzionali all'attività caratteristica dell'impresa.

Articolo 1474
Mancanza di determinazione espressa del prezzo

"*Se il contratto ha per oggetto cose che il venditore vende abitualmente e le parti non hanno determinato il prezzo, né hanno convenuto il modo di determinarlo, né esso è stabilito per atto della*

pubblica autorità [o da norme corporative], si presume che le parti abbiano voluto riferirsi al prezzo normalmente praticato dal venditore.

Se si tratta di cose aventi un prezzo di borsa o di mercato, il prezzo si desume dai listini o dalle mercuriali del luogo in cui deve essere eseguita la consegna, o da quelli della piazza più vicina.

Qualora le parti abbiano inteso riferirsi al giusto prezzo, si applicano le disposizioni dei commi precedenti; e, quando non ricorrono i casi da essi previsti, il prezzo, in mancanza di accordo, è determinato da un terzo, nominato a norma del secondo comma dell'articolo precedente."

4.6) Il funzionamento del Sistema delle *cryptovalute*

A.B.I. – Associazione Bancaria Italiana e *cryptovalute*

Il Comitato esecutivo dell'Associazione Bancaria Italiana il **18 giugno 2020** ha pubblicato delle linee generali della posizione in materia di moneta digitale.

L'ABI ha testualmente affermato: "*Le banche italiane sono disponibili a partecipare a progetti e sperimentazioni di una moneta digitale di Banca Centrale Europea, contribuendo, grazie alle competenze acquisite nella realizzazione di infrastrutture e governance distribuita, a velocizzare la messa in opera di un'iniziativa di livello europeo in una prima nazione.*
Sul tema l'ABI ha istituito dallo scorso anno un gruppo di lavoro dedicato ad approfondire gli aspetti legati a monete digitali e crypto asset.
Di qui le 10 considerazioni condivise dal Comitato esecutivo."

Ecco il decalogo aperto alla possibilità da parte dell'Europa di dotarsi di un euro digitale.

1) La stabilità monetaria e il pieno rispetto della cornice regolamentare europea devono essere preservati in via prioritaria.
2) **Le Banche Italiane** sono già operative su un'infrastruttura di registri distribuiti (*Distributed Ledger Technology* DLT) **con il progetto Spunta**, che è un progetto coordinato da ABI Lab e promosso da ABI volto ad applicare la nuova tecnologia DLT al processo interbancario, **intendono essere parte del cambiamento** introdotto da un'innovazione importante come quella delle monete digitali.

L'applicazione Spunta DLT consente alle banche di individuare rapidamente i disallineamenti nelle transazioni interbancarie condividendo dati comuni in modo sicuro; eseguire controlli e scambi direttamente all'interno dell'applicazione, utilizzare processi e comunicazioni standardizzati per correggere i problemi.

La tecnologia *Smart contract* della soluzione fornisce inoltre alle banche un *feedback* automatico sulle loro transazioni.

I risultati includono un rischio operativo inferiore e processi più rapidi e trasparenti, tutti forniti attraverso un'interfaccia altamente *user-friendly*.

3) Una moneta digitale programmabile rappresenta un'innovazione nel campo finanziario in grado di rivoluzionare profondamente la moneta e lo scambio.

Si tratta di una trasformazione in grado di portare un potenziale valore aggiunto significativo, in particolare in termini di efficienza dei processi operativi e gestionali di qui l'importanza di dedicare attenzione ed energie per sviluppare, rapidamente e con la collaborazione di tutti gli attori del sistema, strumenti utili prima di tutto per lo sviluppo dell'area Euro.

4) È necessario che la moneta digitale ottenga la massima fiducia da parte dei cittadini: a questo scopo, è essenziale che siano rispettati i più elevati standard di conformità alle regole, di sicurezza e di supervisione.
5) In particolare, una *Central Bank Digital Currency* - CBDC, grazie al ruolo fondamentale svolto dalla Banca Centrale, rappresenta lo strumento che più di ogni altro può conciliare le esigenze di innovazione, in coerenza con l'attuale quadro di riferimento di regole, strumenti esistenti e interoperabilità con il mondo analogico.

L'esistenza di un tale strumento potrebbe al contempo ridurre l'attrattività di strumenti di uso comparabile, ma emessi da soggetti privati o (nei casi di completa decentralizzazione) non identificabili, caratterizzati da un profilo di rischio intrinsecamente più elevato.

6) Con l'obiettivo di esplicare al massimo il potenziale trasformativo di questi strumenti è di particolare interesse la possibilità, al momento allo studio, di emettere una *Central Bank Digital Currency* - CBDC - Europea destinata al pubblico, che possa rappresentare una evoluzione del denaro contante.

Grazie al ruolo delle banche, è possibile identificare soluzioni tecniche e modelli di riferimento per preservare le caratteristiche attuali del contante, pur introducendo molti benefici propri del mondo digitale (già propri degli strumenti di pagamento elettronico), come ad esempio la possibilità di non smarrire il proprio denaro e, in questo periodo di forte attenzione al rischio sanitario (Covid 19), di operare in modalità *contactless*.

7) Un lavoro di dettaglio potrà portare a identificare il modello di distribuzione, conservazione e scambio delle monete digitali che meglio contemperi i bisogni di servizio dei clienti, di mantenimento dell'efficacia dei meccanismi di trasmissione della politica monetaria e di conformità regolamentare.
   Certamente, in ciascuno di questi obiettivi, il ruolo delle banche è cruciale.
8) Raggiungere un'elevata facilità d'uso, assicurando al contempo **piena interoperabilità fra il mondo digitale e quello analogico** e un totale livello di circolarità fra tutti gli attori del sistema, rappresenta un fattore di successo della diffusione di questi strumenti.
9) Particolare attenzione va prestata, in funzione delle scelte tecnologiche che verranno adottate, ai profili di tutela dei dati personali dei cittadini.
10) Proiettando nel futuro queste riflessioni, è possibile affermare che la disponibilità di una *Central Bank Digital Currency* - CBDC - potrà abilitare una serie di casi d'uso di grande interesse: favorire la trasmissione di valore tra pari, **agevolando così anche logiche di scambio tra persona e macchina e tra macchina e macchina** e consentire il regolamento delle transazioni transfrontaliere *peer-to-peer*, attenuando il rischio di tasso di interesse, di cambio e di controparte e promuovere, grazie alla caratteristica di programmabilità di queste monete, l'esecuzione di scambi al verificarsi di condizioni predefinite, riducendo in definitiva processi di carattere amministrativo.

Sulla problematica dell'assenza di controllo che sostengono i critici delle *cryptovalute* in realtà un sistema di controllo sia pure per ora solo privato e non pubblico esiste in quanto *Bitcoin* utilizza un ***database* distribuito tra i nodi della rete** (meccanismo della *Blockchain*) che tiene traccia di tutte le transazioni e sfrutta la crittografia per gestire gli aspetti funzionali. (**si veda il capitolo 1 della presente Guida**)

Ogni nodo, cioè ogni dispositivo *hardware* su cui lavora il *software Bitcoin/cryptovalute*, è in grado di comunicare in rete con gli altri dispositivi diventando un soggetto attivo nel processo di gestione della valuta e tanto più numerosi sono i nodi tanto più il concetto di decentralizzazione è significativo.

4.7 Il prezzo del *bitcoin*

Il valore di *bitcoin* è determinato dal mercato, da puri meccanismi di domanda e offerta: un aumento o una diminuzione della domanda determinano di conseguenza un aumento o una riduzione del prezzo della *cryptovaluta*.

L'offerta di *bitcoin* è prestabilita dato che non esiste un'autorità centrale che può modificarne l'emissione.

Dai dati disponibili sul sito ufficiale di *Blockchain*[103] - www.Blockchain.info - possiamo notare che per molto tempo il valore di *bitcoin* è stato pari a zero poi ha incominciato ad andare sulle "montagne russe".

Tutte queste variazioni rendono il *bitcoin* molto volatile così come le altre *cryptovalute* ed in questo scenario numerosi individui possono essere spinti ad acquistare *bitcoin* o le altre *cryptovalute* per scopi speculativi mentre altri, preoccupati dalle informazioni negative riguardanti ad esempio alcuni episodi di furti dagli *exchange*, possono essere spinti a vendere in fretta i *bitcoins* e le altre *cryptovalute* in loro possesso.

4.8) I principali rischi connessi all'uso di *bitcoin/cryptovalute*

Dietro i vantaggi sopra descritti svariati però sono i **RISCHI** che circondano *bitcoin* e in generale tutte le *cryptovalute* in circolazione ed **in particolar modo**:

1) l'estrema volatilità,
2) le finalità illecite,
3) l'anonimato.

Il valore di *bitcoin* nel corso degli anni è stato caratterizzato da una **forte volatilità** anche a causa di una offerta di *cryptovaluta* prestabilita rispetto invece ad una domanda variabile.

Questa estrema volatilità può però innescare il rischio di speculazioni valutarie.

Proprio per questo motivo bisogna prestare molta **attenzione** alle **bolle speculative**.

[103] https://Blockchain.info/it/charts/market-price?timespan=all

ALTRO PROBLEMA da tenere in considerazione riguarda il fatto che a differenza delle operazioni in valuta legale **le operazioni di acquisto, scambio e utilizzo di *cryptovalute* non sono assistite dalle tutele di natura legale e/o contrattuale** che caratterizzano le prime.

Le transazioni che vengono effettuate in *bitcoin* sono **irreversibili**, non sono sostenute né da un contratto né da procedure di reclamo, in più **la vera identità della controparte è anonima**.

La Banca d'Italia ha specificato inoltre, che "*la mancanza di definizioni, di standard legali e di obblighi informativi renderebbe difficile provare in giudizio di aver subito un danno ingiusto*" .
Avverte in più che "*è possibile che l'utilizzo o la conversione di valute virtuali siano soggetti a costi e commissioni non chiaramente indicati*"[104].

Non essendo inoltre soggette a vigilanza l'emissione e la gestione di *cryptovalute* espone i soggetti ad **elevati rischi di condotta fraudolenta, di fallimento o di cessazione di attività da parte delle piattaforme di scambio.**

Questo è quanto accaduto nel 2014 a Mt.Gox, una delle prime e principali piattaforme più utilizzate del *web* per le operazioni di cambio valuta.
In quella occasione circa 750.000 *bitcoins* appartenenti ai clienti della Mt.Gox furono rubati a causa di un attacco informatico.

UN ALTRO RISCHIO deriva dal fatto che le *cryptovalute* archiviate nel *wallet* potrebbero andare perse a seguito di malfunzionamenti o attacchi informatici.

INOLTRE, non esistono delle procedure per poter recuperare la *password* di accesso al proprio portafoglio, quindi nel momento in cui questa viene smarrita la quantità di *bitcoin* presente *nell'e-wallet* diventa irrecuperabile.

L'ASPETTO PIÙ PROBLEMATICO risulta essere però l'anonimato, che non deve essere confuso con mancanza di tracciabilità dato che tutte le transazioni vengono memorizzate sulla *Blockchain* insieme all'indirizzo di chi ha effettuato ogni singola transazione però questi indirizzi sono anonimi.

[104] Avvertenza sull'utilizzo delle cosiddette "valute virtuali", pubblicata da Banca d'Italia il 30 gennaio 2015

L'anonimato, o meglio ancora lo pseudoanonimato, **sta ad indicare che i dati sensibili di una transazione finanziaria non devono essere comunicati affinché venga eseguita la transazione**.

Anche se questo potrebbe essere considerato un punto di forza dato il timore dei consumatori a condividere i propri dati finanziari in rete.

In questo contesto quindi la rete può essere utilizzata per eseguire transazioni connesse ad **attività criminali** rendendo indispensabile l'intervento delle autorità giudiziarie.

Uno degli episodi più gravi legati al *bitcoin* è quello del caso del **portale *Silk Road*.**
Il portale, fin da febbraio del 2011, forniva ad acquirenti e venditori una piattaforma *online* nella quale poter scambiare beni e servizi.

Rispetto agli altri siti però veniva fornito ai clienti un elevato livello di anonimato.

I prodotti che venivano venduti però non erano prodotti "normali": su *Silk Road* venivano commercializzati illegalmente droga, armi, documenti falsi che potevano essere acquistati utilizzando esclusivamente *bitcoin*.

Il fondatore, Ross William Ulbricht sotto lo pseudonimo di Dread Pirate Roberts (DPR), aveva basato il funzionamento di *Silk Road* tramite TOR (*The Onion Router*), sistema di comunicazione anonima per *internet* in grado di nascondere il vero indirizzo IP del computer.

Chiunque possedeva *bitcoins* poteva registrarsi sulla piattaforma e iniziare ad acquistare i prodotti che venivano venduti.
Nell'ottobre del 2013 Ulbricht venne arrestato dalla *Federal Bureau of Investigation* (FBI) ed il portale *Silk Road* venne chiuso.
Ai primi di novembre però ne fu annunciata la riapertura da parte di DPR.
Alla fine di gennaio del 2014 vennero arrestati Robert Faiella e Charlie Shrem, amministratore delegato di *Bit Instant* una società di scambio di moneta virtuale *bitcoin*, accusati di aver venduto oltre un milione di dollari in *bitcoin* agli utenti di *Silk Road*[105].

[105] http://www.repubblica.it/economia/finanza/2014/01/28/news/bitcoin_arresti_traffico_droga-77128457/

Il 29 maggio 2015 Ulbricht è stato condannato all'ergastolo.

4.9) Regolamentazione normativa in Italia ed all'Estero

Nel rapporto dal titolo "*Changes in modus operandi of Islamic State terrorist attacks*" pubblicato nel gennaio del 2016 da parte *dell'Europol*, agenzia finalizzata alla lotta al crimine dell'Unione Europea, si evince che **non vi è alcuna prova riguardante l'uso di *cryptovalute* da parte dei terroristi, contrariamente a quanto affermato da un giornalista il quale dopo una settimana aveva ammesso l'errore.**

Questo quanto scritto nel rapporto: *"(…) There is no evidence however of IS-financing networks in existence. Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement.*"

Nei primi mesi del 2018 però l'*Europol* ha lanciato l'allarme in relazione al presunto riciclaggio messo in atto dai criminali attraverso le *cryptovalute*.

Secondo quanto dichiarato da Rob Wainwright, direttore *dell'Europol* in carica fino al 1° maggio 2018, più di 5,5 miliari di dollari sarebbero stati riciclati attraverso le *cryptovalute* dalle organizzazioni criminali in Europa.

In una intervista alla BBC ha dichiarato che: "*Le cryptovalute non sono governate da un'autorità centrale quindi la polizia non può monitorare tali transazioni.*
E se si stabilisce che sono di natura criminale non ha modo di congelare gli asset a differenza del sistema bancario tradizionale"[106].

Il 9 aprile del 2018 l'operazione *Tulipan Blanca*, coordinata da *Europol* e condotta dalla *Guardia Civil* spagnola con il supporto delle autorità finlandesi e statunitensi, ha portato all'arresto di 11 persone e 137 indagati per il riciclaggio di oltre 8 milioni di euro.

Il tutto si svolgeva in questi termini: i proventi derivanti dalla cocaina venivano convertiti in *bitcoin* in Finlandia, successivamente la *cryptovaluta* veniva cambiata in *pesos* colombiani per poi depositare le somme in conti correnti bancari colombiani[107].

[106] http://www.bbc.com/news/technology-43025787
[107] http://europa.today.it/attualita/riciclaggio-nell-era-bitcoin.html

4.9.a) Italia

In Italia con il **D. Lgs. n. 231/2007** è stata istituita il 1° gennaio del 2008 presso la Banca d'Italia l'Unità di Informazione Finanziaria - UIF - per prevenire e contrastare il riciclaggio e il finanziamento del terrorismo.

A partire da questa normativa il legislatore italiano ha preteso che nel momento in cui la valuta reale prenda la via della *cryptovaluta* – cioè, per esempio, al momento dell'acquisto di *bitcoin* – **deve rimanere traccia reale di chi investe nell'algoritmo** cioè prima che si immerga nel mondo poco tracciabile delle *Blockchain* a espansione continua.

l'Unità di Informazione Finanziaria – UIF - ha il compito di analizzare le operazioni sospette comunicate dagli intermediari finanziari, professionisti e altri operatori, e trasmette la propria analisi al Nucleo speciale di polizia valutaria della Guardia di finanza (NSPV) e alla Direzione Investigativa Antimafia - DIA[108].

L'Unità di Informazione Finanziaria ha pubblicato nel febbraio del 2015 una comunicazione dal titolo "*Utilizzo anomalo di valute virtuali*"[109], con la quale richiede ai destinatari della normativa antiriciclaggio di "*individuare le operatività connesse con valute virtuali, **rilevandone gli eventuali elementi di sospetto***".

Gli Intermediari Finanziari, ma in generale i Prestatori di Servizi relativi all'utilizzo di valuta virtuale dovranno "*valutare con specifica attenzione le operazioni di prelevamento e/o versamento di contante e le movimentazioni di carte di pagamento, connesse con operazioni di acquisto e/o vendita di valute virtuali, realizzate in un arco temporale circoscritto, per importi complessivi rilevanti*".

a) Come si evince dal dettato normativo i destinatari di tali obblighi sono gli **Intermediari Finanziari**.

[108]M. Tupponi (a cura di), *Manuale di diritto commerciale internazionale*, con la collaborazione di G. De Marinis, A. Russo, L. Piccinino, E. Greppi, A. Montefinese, 3ª ed., Giappichelli, Torino, 2019, pag. 7.
[109]https://uif.bancaditalia.it/

b) Ma anche **i Prestatori di Attività Funzionali** – gli *exchanger* - all'utilizzo, allo scambio ed alla conservazione di valute virtuali ed alla loro conversione da/in quelle legali **sono tenuti** all'osservanza degli obblighi di adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette.

Il 30 gennaio 2015, **la Banca d'Italia** aveva reso nota una comunicazione dal titolo "**Valute virtuali**"[110] nella quale si dichiarava che l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali è da considerarsi **un'attività lecita**.

Il documento invitava gli Intermediari Finanziari a valutare con attenzione i rischi indicati dalla *European Banking Authority* – EBA - nel suo *report*.

Quindi in Italia le *cryptovalute* trovano per ora la loro regolamentazione unicamente sotto il profilo del **contrasto al riciclaggio del denaro**.
Con il **D. Lgs. 25 maggio 2017, n. 90**[111], riguardante la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, il legislatore italiano è intervenuto sul tema dell'impiego di **valute virtuali**.
Il decreto introduce in Italia la **IV Direttiva antiriciclaggio entrata in vigore il 4 luglio 2017.**

L'Italia è stato il primo paese in Europa a legiferare sulle *cryptovalute*.

Il D. Lgs. 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, trasferita, archiviata e negoziata elettronicamente*".

Secondo quanto dispone il D. Lgs. n. 231 del 2007, riformato dal D. Lgs. n.90 del 2017, l'art. 1, comma 2, lett. *ff)* definisce che è Prestatore di Servizi relativi all'utilizzo di valuta virtuale "ogni *persona fisica o giuridica che fornisce a terzi**, a titolo professionale**, servizi funzionali all'utilizzo,*

[110] https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf
[111] G.U. n. 140 del 19 giugno 2017

allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale".

I Prestatori di Servizi, **limitatamente allo svolgimento di attività di conversione**, rientrano nella categoria di operatori **non** finanziari, art. 3 comma 5, lett. *i*).

L'art. 8 del D. Lgs. n. 90 del 2017 modifica il D. Lgs. 13 agosto 2010 n. 141 (già modificato dal D. Lgs. 14 dicembre 2010 n.218 e dal D. Lgs. 19 settembre 2012 n. 169): all'art. 17-*bis* del D. Lgs. n. 141 del 2010 viene introdotto il comma 8-*bis*, secondo cui gli obblighi, anche di iscrizione presso il registro degli agenti e dei mediatori, gestito dall'Organismo di vigilanza previsto dall'art. 128-*undecies* del TUB sono estesi ai prestatori di servizi relativi all'utilizzo di valute virtuali di cui all'art. 1, comma 2, lett. *ff*) del D. Lgs. n. 231 del 2007.

Gli ***exchanger*** in quanto Prestatori di Servizi, poiché sono gli operatori o le piattaforme che convertono le *cryptovalute* in moneta avente corso legale, diventano destinatari delle normative antiriciclaggio e devono ottenere una licenza ed essere iscritti in un apposito registro.

Viene previsto inoltre **l'obbligo di adeguata verifica del cliente anche nel caso**:

1. dell'esecuzione di un'operazione occasionale, che comporta la trasmissione o comunque la movimentazione di mezzi di pagamento per un importo pari o superiore a € 15.000;
2. trasferimento di fondi superiore a € 1.000;
3. sospetto di riciclaggio o di finanziamento del terrorismo;
4. dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione.

Allo stato attuale quindi si sta cercando di porre le *exchange* sotto il controllo del Ministero delle Finanze o della Banca d'Italia per verificare cosa avviene al loro interno in modo tale da poter effettuare i controlli antiriciclaggio.

Per quanto riguarda gli aspetti di natura tributaria in Italia si è pronunciata l'Agenzia delle Entrate con la risoluzione numero 72/E del 2 settembre 2016[112] ponendo l'accento sulle operazioni di cambio e la loro imponibilità ai fini IVA, IRAP e dei redditi.

Secondo l'Agenzia le operazioni di cambio tra valute tradizionali e *bitcoin* sono esenti dall'IVA.

La risoluzione fa riferimento alla sentenza della **Corte di Giustizia dell'Unione Europea del 22 ottobre 2015 (Causa C-264/14).**

Secondo i giudici europei le operazioni consistenti nel cambio di valuta tradizionale contro valuta virtuale *bitcoin* e viceversa devono essere considerati assimilabili alle operazioni "relative a divise, banconote e monete con valore liberatorio" di cui **all'art. 135, paragrafo 1, lettera e) della direttiva 2006/112/Ce.**

Dunque è esente IVA il margine che scaturisce dalla differenza tra il prezzo che il cliente è disposto a pagare per acquistare una unità di moneta virtuale e la migliore quotazione del *bitcoin* stesso disponibile sul mercato.

Secondo la risoluzione è considerata un'attività rilevante ai fini delle imposte dirette l'attività di intermediazione di valute tradizionali con *bitcoin* se questa viene svolta in maniera professionale ed abituale.

Quindi sono soggetti a tassazione quei componenti di reddito che derivano dall'intermediazione nell'acquisto e vendita di *bitcoin*.

Per quanto riguarda invece la persona fisica, se questa non svolge attività finanziaria finalizzata all'ottenimento di plusvalenze non deve pagare alcuna imposta.

Però se nel corso di un anno e per almeno 7 giorni consecutivi il valore dei bitcoin posseduti supera la soglia di € 51.645,69 l'Agenzia delle Entrate considera questa attività speculativa e quindi richiede il pagamento delle imposte sulle eventuali plusvalenze.

Le imposte comunque si devono pagare solo quando viene realizzata la plusvalenza, quindi al momento della vendita dei *bitcoins*.

L'aliquota applicata è del 26%.

4.9.b) Regolamentazione internazionale

Le *cryptovalute* da diversi anni sono al centro del dibattito internazionale.

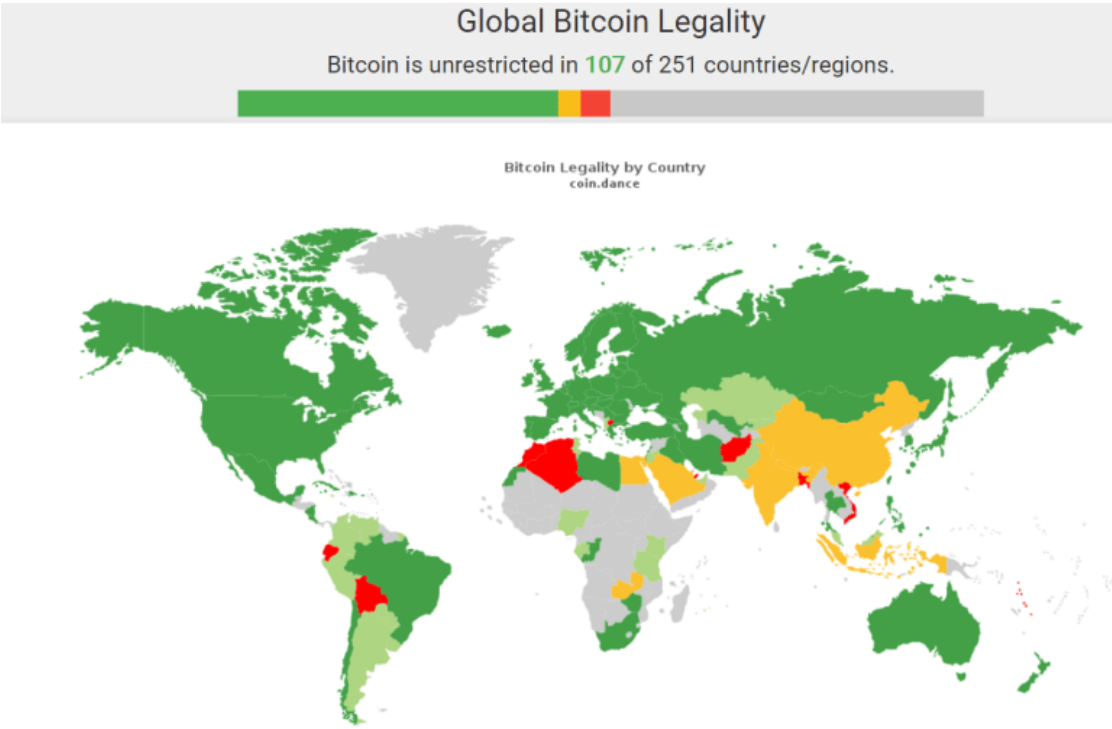
[112] http://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/normativa+e+prassi/risoluzioni/archivio+risoluzioni/risoluzioni+2016/settembre+2016+risoluzioni/risoluzione+n.+72+del+02+settembre+2016/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf

A seguito della loro espansione non tutti i Paesi stanno reagendo allo stesso modo.

Allo stato attuale infatti non esiste una regolamentazione giuridica uniforme sul fenomeno anche perché alcuni Paesi regolano le *cryptovalute*, altri poco e altri ancora le vietano completamente.

È necessario quindi cercare di capire le diverse soluzioni proposte dai singoli Paesi in modo da osservarne analogie e diversità.

La seguente carta tematica mostra le diverse posizioni assunte a livello mondiale sulla detenzione e commercio di *bitcoin*.



Bitcoin: dove è legale, illegale o soggetto a restrizioni (Fonte: www.cryptominando.it)

Il *bitcoin* è:

- legale e neutrale (verde e verde chiaro);
- limitato (giallo);
- illegale (rosso);

- nessuna informazione (grigio).

Unione Europea

La questione *cryptovalute* nel corso degli anni è stata affrontata anche dalle autorità europee le quali hanno cercato di studiare le valute virtuali, cercando di identificare i rischi derivanti dall'uso di tali valute, al fine di mettere a punto delle regole adatte a disciplinare il fenomeno a livello europeo.

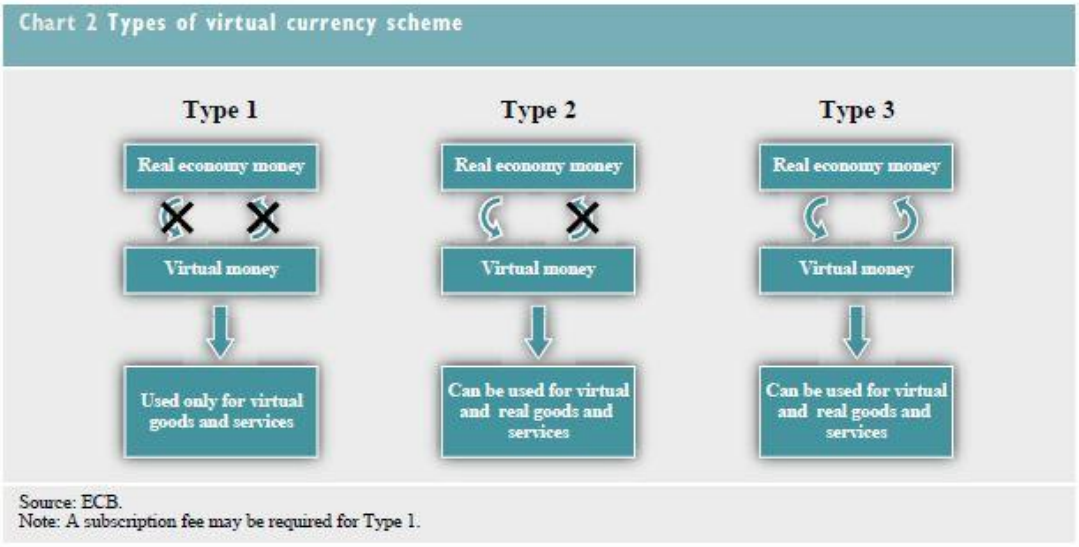
Nell'ottobre del 2012 la Banca Centrale Europea (BCE) ha pubblicato un documento dal titolo "***Virtual Currency Schemes***[113]".

Il testo analizza la nascita delle *cryptovalute* definendo le valute virtuali come un tipo di moneta digitale, non regolamentata, che è controllata ed emessa dai suoi sviluppatori, usata e accettata tra i membri di una specifica comunità virtuale.

Il documento prosegue con la presentazione dei **tre macrotipi principali della valuta virtuale**:

1. **gli Schemi di valuta virtuale chiusi,** dove le valute virtuali non producono interazioni con l'economia reale.
   Sono spendibili unicamente nel contesto della comunità virtuale che le accetta e di solito vengono usate in giochi *on-line*;
2. **gli Schemi di valuta virtuale unidirezionali**, in questo caso le valute virtuali possono essere acquistate con moneta tradizionale ad un determinato tasso di cambio, ma non possono essere riconvertite in valuta reale;
3. **gli Schemi di valuta virtuale con flusso bidirezionale**, dove le valute virtuali possono essere convertite in valute aventi corso legale e viceversa.
   Le cryptovalute appartengono a questo gruppo.

[113] Si veda nota n. 32



Schemi di valuta virtuale (Fonte: www.ecb.europa.eu)

La BCE, sebbene riconosca degli aspetti positivi in termini di innovazione finanziaria generati dalle *cryptovalute*, **sottolinea alcuni potenziali RISCHI di queste valute**:

1. rischio per la stabilità dei prezzi;
2. rischio per la stabilità finanziaria;
3. rischio per la stabilità dei sistemi di pagamento;
4. mancanza di regolazione;
5. il livello di sicurezza è inferiore rispetto alla moneta bancaria, dato che le banche sono sottoposte a requisiti prudenziali e di vigilanza.

Invece tra gli **ASPETTI POSITIVI** riconosciuti la BCE ritiene che se le imprese offrissero la possibilità di pagare con tale alternativa potrebbero trovare il modo per poter aumentare i loro guadagni.

La regolamentazione sperata dalla BCE da un lato fortificherebbe la fiducia in questa moneta ma dall'altro lato andrebbe contro la ragione alla base della sua nascita cioè essere svincolata da un'autorità centrale.

L'Autorità Bancaria Europea (EBA)[114] nel dicembre del 2013 ha diffuso un documento dal titolo "*Warning to consumers on digital currencies*[115]" nel quale si cerca di avvisare il singolo **consumatore** a proposito dei rischi legati all'acquisto, al possesso o allo scambio di monete virtuali come il *bitcoin*.

Il documento dà una **DEFINIZIONE DI MONETA VIRTUALE**: "*A virtual currency is a form of unregulated digital money that is not issued or guaranteed by a central bank and that can act as means of payment*".

Questi alcuni dei **RISCHI** menzionati all'interno del documento:

1. possibilità di perdere il proprio denaro sulla piattaforma di scambio a causa ad esempio di attacchi compiuti da terzi, quindi se una piattaforma di scambio perde denaro o fallisce non esiste nessuna tutela legale specifica volta a coprire tali perdite;
2. possibilità di subire un furto del proprio denaro dal portafoglio elettronico anche se dotato di *password*.

   Inoltre la perdita della *password* comporta la perdita definitiva della valuta virtuale contenuta nell'*e-wallet* dato che non ci sono autorità centrali che registrano le *password* o ne danno di sostitutive;
3. assenza di tutela per l'utilizzo di monete virtuali come mezzo di pagamento nel caso di addebiti non autorizzati o errati.

   In più l'accettazione non è garantita in maniera duratura e può cessare in qualunque momento;
4. possibile abuso delle transazioni in *cryptovalute* per riciclare denaro sporco e svolgere attività criminali essendo dotate di un alto grado di anonimato.

Sempre l'EBA nel luglio 2014 pubblica un ulteriore documento "*Opinion on virtual currencies*" evidenziando **VANTAGGI** e rischi delle valute virtuali.

[114] L'Autorità Bancaria Europea è un'agenzia dell'UE incaricata di attuare un *corpus* di norme standard per regolamentare e vigilare sul settore bancario in tutti i paesi dell'UE. Il suo obiettivo è creare un mercato unico dei prodotti bancari dell'UE efficiente, trasparente e stabile.

[115] Teso integrale su http://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf

Tra i **vantaggi** abbiamo l'inclusione di quei soggetti che non possono accedere ai canali bancari e finanziari a causa di costi e oneri amministrativi elevati e la crescita economica determinata dalla nascita di nuovi attori economici.
Il documento fornisce, a pag.22, un elenco di circa 70 dei potenziali rischi:

Rischi potenziali individuati dall'EBA (Fonte: www.eba.europa.eu)
Fra questi, i rischi identificati con la lettera E, riguardano le autorità di vigilanza.
Il documento mette in guardia le autorità di vigilanza evidenziando i rischi derivanti da una cattiva attività di controllo.
Le autorità, a seconda della scelta di regolamentare o non regolamentare, potrebbero subire danni di natura reputazionale e legale.
Secondo l'EBA i rischi individuati supererebbero i possibili benefici che le valute virtuali potrebbero fornire ai loro utilizzatori.
La BCE nel febbraio del 2015 presenta un nuovo documento "*Virtual Currency Schemes: a further analisys*[116]" dove viene analizzato nuovamente il fenomeno delle *cryptovalute* definendole questa volta come "*a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*"[117].

Da questa nuova definizione fornita **notiamo che la BCE quindi nega alle valute virtuali la natura di moneta** e che non è più presente il termine "non regolamentata" dato che alcune giurisdizioni hanno regolamentato il fenomeno (es. in Germania il *bitcoin* è qualificato come unità di conto).

Nel 2016 è stata pubblicata una prima **Risoluzione del Parlamento europeo**[118] sulle valute virtuali nella quale venivano identificati alcuni aspetti positivi, come abbassamento dei costi di transazione e benefici in termini di inclusione finanziaria, ma anche alcuni timori legati soprattutto all'elevata volatilità delle valute virtuali e al rischio di bolle speculative.

[116] Testo originale https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
[117] Pag. 25 del documento
[118] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0228+0+DOC+PDF+V0//IT

Particolare attenzione viene rivolta alla tecnologia a registro distribuito (*Distributed Ledger Technology*, DLT), che potrebbe essere impiegata per aumentare la condivisione di dati, la trasparenza e la fiducia non solo tra governo e cittadini, ma anche tra operatori del settore privato e clienti.
Proprio per questo motivo la Risoluzione chiede ai paesi dell'UE di adottare un approccio normativo che non vada a soffocare l'innovazione.

Francia

In Francia le plusvalenze generate da *bitcoin* potevano essere considerate profitti aziendali, (*Bénéfices Industriels et Commerciaux* – BIC) in caso di attività costante, oppure profitti non commerciali, (*Bénéfices non Commerciaux* – BNC) per l'attività occasionale, sui quali applicare un'aliquota variabile fino al 45%.

Il Consiglio di Stato francese ha dichiarato[119] che i *bitcoins* possono rientrare solo in una delle categorie previste dall'articolo 516 del Codice Civile francese e cioè beni immobili o beni mobili.
Lo stesso Consiglio ha affermato che il *bitcoin*, in base alle caratteristiche che possiede, deve essere **qualificato come bene mobile**.
Da questo ne deriva che la differenza tra il valore di acquisto e quello di realizzo (nel caso in cui i *bitcoins* detenuti vengano utilizzati per acquistare altri beni) potrà dare luogo a capital gain soggetti alla disciplina applicabile ai beni mobili.
Quindi se le plusvalenze vengono generate nell'ambito di un'attività d'impresa queste rientrano nel reddito commerciale e industriale (BIC) senza conseguenze sul piano fiscale rispetto al regime previgente.
Nel caso di plusvalenze occasionali da parte di persone fisiche queste potranno beneficiare della *flat tax* pari al 19% prevista per i *capital gain*.

È doveroso inoltre ricordare che il governo francese con l'ordinanza n° 2017-1674 dell'8 dicembre 2017 è stato il primo in Europa ad introdurre delle norme che favoriscono l'utilizzo del sistema della *Blockchain* nella registrazione dei titoli finanziari (azioni e obbligazioni) emessi dalle società.

[119] https://www.lemonde.fr/argent/article/2018/04/26/le-conseil-d-etat-change-la-fiscalite-sur-les-gains-generes-par-les-bitcoins_5291137_1657007.html

Sempre la Francia insieme ad altri Stati europei sta lavorando per cercare di redigere una normativa comune con la quale provare a regolamentare al meglio il tema delle *cryptovalute*.

Una occasione importante per poter trattare dell'argomento poteva essere il G20, tenutosi in Argentina nel mese di marzo 2018.
I partecipanti però non sono riusciti a giungere a una proposta condivisa e secondo quanto dichiarato dal governatore della banca centrale argentina Federico Sturzenegger le autorità internazionali riunite al G20 hanno bisogno di altri dati e di monitorare più a lungo il fenomeno per fornire delle "proposte specifiche" circa un eventuale quadro normativo condiviso[120].

Germania

Nel 2013 l'Autorità Federale di Supervisione Finanziaria (*Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin*) ha pubblicato un documento[121] nel quale viene affermato che i *bitcoins* sono unità di conto inclusi nella categoria degli strumenti finanziari ai sensi della legge bancaria tedesca (c.d. Kreditwesengesetz o KWG).
Chi utilizza *bitcoin* o altre *cryptovalute* come strumento di pagamento o le accetta a contropartita di beni e servizi, non necessita di alcuna autorizzazione specifica da parte della BaFin.
Invece nel caso in cui vi sia acquisto o vendita di *bitcoin* per conto terzi su scala commerciale è necessaria una licenza ai sensi della legge bancaria tedesca (KWG), in quanto attività sottoposta a regolamentazione e vigilanza.

Quindi se una società agisce come intermediario nelle transazioni di *cryptovalute*, *exchange*, oppure svolge attività di *mining* non può sfuggire alla necessità di richiedere una licenza alla BaFin.

Da un punto di vista **fiscale** dobbiamo distinguere il diverso trattamento imposto tra privati e imprese.

Per i privati gli scambi in *cryptovalute* che danno origine ad una plusvalenza sono considerati transazioni speculative e quindi sono soggetti all'articolo 23 della legge fiscale.

[120] https://www.soldionline.it/analisi-scenario/bitcoin-e-g20-un-occasione-persa
[121] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html

Questa però prevede che siano esenti da tassazione se vengono detenute per più di un anno.
Facciamo **un esempio** per capire meglio: se il 10 febbraio 2021 ho acquistato un *bitcoin* per € 2.000 e il 30 novembre l'ho venduto a € 11.000 sulla differenza, quindi € 9.000, devo pagare una imposta sui guadagni.
Invece se io avessi tenuto il *bitcoin* acquistato il 10 febbraio 2020 oltre il 10 febbraio 2021, l'imposta sul guadagno sarebbe stata soppressa.
Tale approccio ci fa subito notare una diversa trattazione tra Germania ed ad esempio gli Stati Uniti dove *l'Internal Revenue Service* (IRS) considera *bitcoin* come una proprietà e ogni acquisto effettuato utilizzando *bitcoin* è pertanto ritenuto tecnicamente una vendita di proprietà e quindi soggetto all'imposta sulle plusvalenze.
Nel caso le *cryptovalute* vengano vendute prima vi è solo una esenzione standard pari a € 600.
In compenso sono detraibili le minusvalenze.
Per quanto riguarda invece le imprese il reddito prodotto dal trading di *cryptovalute* è tassato come reddito di impresa.

Svizzera

Mentre molti paesi stanno cercando di predisporre complesse regolamentazioni o imporre divieti parziali all'uso delle *cryptovalute*, in Svizzera l'Autorità di sorveglianza dei mercati finanziari (FINMA) ha emanato un manuale per gli operatori finanziari nel quale viene spiegato come le norme in vigore possono essere **applicate anche al mercato delle *cryptovalute*** permettendo a questo settore di continuare ad evolvere[122].
Questo però non vuol dire che le leggi svizzere attuali siano sufficienti per tenere sotto controllo il nuovo mercato dato che attualmente il diritto civile svizzero contempla i beni materiali, come le automobili, e i beni immateriali, come i diritti d'autore.
Con la *Blockchain* e le *cryptovalute* sorge un "nulla giuridico", **perché si fondano su algoritmi**, ossia un qualcosa che ancora non è preso in considerazione dal diritto svizzero.
Sarà quindi opportuno aggiungere degli adeguamenti.
Anche gli operatori del settore richiedono l'introduzione di un più chiaro quadro giuridico.

Dal 1° luglio 2016 a Zugo l'amministrazione comunale ha deciso di adoperare il *bitcoin* come moneta per pagare le tasse comunali.

[122] https://www.swissinfo.ch/ita/economia/rivoluzione-digitale_cryptovalute--chance-o-rischio-per-la-piazza-finanziaria-svizzera-/44157444

I cittadini quindi possono regolare i loro conti con l'amministrazione pubblica anche attraverso la *cryptovaluta* per un importo massimo di 200 franchi.
Si tratta del primo comune al mondo che dà la possibilità di pagare le tasse in *bitcoin*.
Stessa direzione è stata seguita a sud della Svizzera dal comune di Chiasso.
Da gennaio 2018 anche qui si possono pagare le imposte comunali tramite *bitcoin* fino a 250 franchi.
Di recente inoltre è stata fondata la *Capital Markets and Technology Association* (CMTA)[123], un'organizzazione il cui scopo è quello di realizzare norme e strumenti per promuovere l'utilizzo della tecnologia *Blockchain*.

Russia

Cambio di rotta da parte della Russia sul tema *cryptovalute* che inizialmente aveva dichiarato di volerle vietare perché considerate un mezzo idoneo per riciclare denaro e finanziare il terrorismo. Adesso però la situazione sembra essere cambiata perché le *cryptovalute* e in particolare il *bitcoin* sono cresciute in tutto il mondo.

La legge riconosce ai cittadini russi il diritto a possedere *cryptovalute* e la possibilità di scambiarle contro valute fiat - rubli o altre valute digitali.

Questa operazione però deve avvenire tramite *exchange* che rispettino le leggi russe in tema di intermediazione finanziaria (Legge Federale N.39-FZ del 22 aprile 1996) ovvero che siano società di *trading* ai sensi della normativa russa (Legge Federale N.325-FZ del 21 novembre 2011 "Sul *trading* organizzato").

I cittadini russi quindi potranno vendere o comprare le *cryptovalute* solo tramite *exchange* che abbiano sede stabile in Russia.

Per quanto riguarda il portafoglio digitale (*wallet*), in base a quanto stabilito dalla legge, questo potrà essere aperto solo dopo l'identificazione del soggetto che richiede di aprirlo in conformità con

[123] http://www.cmta.ch/wp-content/uploads/CMTA-Press-release-EN_FR_DE_1191538_1.pdf

la Legge Federale H.115-FZ del 7 agosto 2001 "Sul riciclaggio di profitti derivanti da attività criminali e sul finanziamento del terrorismo".

Il governo russo, inoltre negli ultimi mesi sta lavorando alla creazione di una propria *cryptovaluta*: il ***cryptorublo***.
Secondo quanto riferito da Sergey Glazev, consigliere economico del presidente Putin, si tratterebbe dello stesso rublo ma scambiato attraverso il sistema *Blockchain* potendone così tracciare i movimenti.
Essendo emessa dallo stato la nuova moneta non potrà essere "minata"[124].
A questo punto però sorge spontanea una domanda: il *cryptorublo* può davvero essere considerato una *cryptovaluta*? A parere di chi scrive, come già detto, il *cryptorublo* andrebbe a violare uno dei principi cardine delle *cryptovalute* poiché queste sono nate per essere decentralizzate quindi con l'obiettivo di non essere regolate né da banche né da governi centrali.

Riguardo alla tassazione tutte le transazioni che verranno eseguite con il *cryptorublo* saranno tassate del 13%.

USA

Nel 2012 il *Federal Bureau of Investigation* (FBI) ha pubblicato un documento dal titolo "*Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*"[125].
Il documento descrive i diversi livelli di rischio per le attività illegali eseguite tramite *bitcoin*.

L'FBI valuta con livello di rischio basso l'utilizzo dei *bitcoins* per **riciclare denaro**, mentre l'area riguardante il finanziamento del terrorismo e il furto di fondi è quella che preoccupa maggiormente l'FBI classificandola come l'area con il più alto livello di rischio.
Nel 2013 il *Financial Crimes Enforcement Network* (FinCEN) pubblicò una guida nella quale venivano fornite indicazioni per l'applicazione del *Bank Secrecy Act* (BSA approvato nel 1970)[126] alle valute virtuali[127].

[124] https://es.cointelegraph.com/news/breaking-russia-issuing-cryptoruble
[125] http://cryptome.org/2012/05/fbi-bitcoin.pdf
[126] Si tratta di una norma che obbliga le istituzioni finanziarie ad assistere le Agenzie Governative Statunitensi a prevenire e contrastare il riciclaggio di denaro.
[127] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

Nella guida FinCEN le valute virtuali non vengono equiparate alle valute a corso legale, ma è necessario capire quali siano gli operatori soggetti agli obblighi del *Bank Secrecy Act*:

- **l'utente** che ottiene moneta virtuale per l'acquisto di beni o servizi non è *Money Service Business* (MSB) quindi non è soggetto agli obblighi del *Bank Secrecy Act*
- mentre **le figure di scambiatore e amministratore diventano *Money Service Business*** nel momento acquistano o vendono moneta virtuale convertibile per qualsiasi motivo.

Al contrario nel 2014 *l'Internal Revenue Service* (IRS), l'Agenzia delle Entrate negli USA, decise di considerare le valute virtuali come una proprietà quindi tutte le volte che viene effettuata una transazione in *cryptovaluta* bisogna registrare l'importo e nel caso in cui si riscontri un guadagno questo deve essere soggetto a tassazione[128].

Finora comunque il governo federale degli Stati Uniti ha lasciato ai singoli stati la possibilità di introdurre i propri regolamenti.

Stato del Texas

Nell'agosto del 2013 il giudice Amos Mazzant nella causa SEC v. Shavers[129] ha stabilito che i *bitcoins* sono una forma di moneta e per questo devono sottostare alle leggi USA sulla valuta.

L'imputato Trendon Shavers è il fondatore di *Bitcoin Saving & Trust* (BTCST).

Nel mese di agosto del 2012 le attività di BTCST sono state chiuse e la SEC ha accusato il fondatore di portare avanti una frode basata sullo schema Ponzi[130].

Secondo la SEC Shavers aveva raccolto circa 700 mila *bitcoins* pari a oltre 4,5 milioni di dollari.

Egli però sosteneva che non essendo *bitcoin* moneta nessuna transazione di denaro era avvenuta.

Il giudice Mazzant però ha stabilito che i *bitcoins* possono essere usati come una moneta.

Possono essere utilizzati per acquistare beni o servizi solo ove vengano accettati come moneta e possono essere cambiati come qualsiasi altra moneta.

Quindi *bitcoin* è una moneta o forma di denaro e gli investitori che hanno voluto investire in BTCST hanno effettuato un investimento di denaro.

---

[128] https://www.ilbitcoin.news/il-folle-trattamento-fiscale-delle-cryptovalute-negli-usa/

[129] https://h2o.law.harvard.edu/cases/4293

[130] Da Wikipedia "Lo schema Ponzi è un modello economico di vendita truffaldino che promette forti guadagni alle vittime a patto che queste reclutino nuovi "investitori", a loro volta vittime della truffa."

Stato dell'Arizona

L' 8 febbraio 2018 il Senato dell'Arizona aveva approvato la legge *SB 1091* con la quale veniva consentito ai cittadini di pagare le tasse statali in *cryptovalute*.

Il Dipartimento delle Entrate, una volta ricevuto il pagamento in *cryptovaluta*, avrebbe dovuto convertire entro 24 ore le *cryptovalute* in dollari statunitensi.

La stessa legge era passata poi all'esame della Camera dei Rappresentanti dove però è stata oggetto di alcuni emendamenti.

In particolare, la Camera ha proposto che il Dipartimento delle Entrate avesse la possibilità di "valutare" forme di pagamento alternative che usano sistemi elettronici *peer-to-peer*.

Tuttavia però, secondo documenti pubblici, la Camera dei Rappresentanti ha approvato la legge il 30 aprile ma con un testo diverso rispetto all'originale approvato dal Senato[131] nel quale non vengono menzionate in alcun modo le *cryptovalute*.

Il problema è che nell'arco delle 24 ore, tempo a disposizione del Dipartimento delle Entrate per convertire la *cryptovaluta* in dollari, il pagamento effettuato dal contribuente in *bitcoin* poteva subire variazioni in aumento o in diminuzione rispetto al momento di pubblicazione da parte del Dipartimento ed in questa situazione lo Stato sarebbe stato costretto a rimborsare il contribuente per la differenza o a richiedere l'integrazione[132].

Sempre in Arizona il 3 aprile del 2018 è stato approvato un disegno di legge relativo alle *Blockchain*.

La normativa *HB 2603*, approvata[133] dal Governatore Doug Ducey, consente alle imprese di archiviare e condividere dati su registri distribuiti.

Stato della Georgia

Come l'Arizona anche lo Stato della Georgia, con la **proposta di legge** 464 del 21 febbraio[134] ad opera dei senatori Michael Williams e Joshua McKoon, ha avanzato la possibilità di accettare per il pagamento delle tasse le *cryptovalute*.

---

[131] https://legiscan.com/AZ/text/SB1091/id/1791279

[132] https://assodigitale.it/cryptovalute/legge-tasse/arizona-boccia-cryptovalute-come-sistema-pagamento-tasse/

[133] https://legiscan.com/AZ/text/HB2603/id/1718691

[134] https://legiscan.com/GA/text/SB464/id/1739174

Il disegno di legge afferma che: "*The commissioner shall accept as valid payment for taxes and license fees any cryptocurrency, including but not limited to Bitcoin, that uses an electronic peer-to-peer system*".
Viene inoltre stabilito che i pagamenti effettuati in *cryptovaluta* dovranno essere convertiti in dollari statunitensi entro 24 ore dal ricevimento degli stessi.

Nel luglio del 2015 il Dipartimento dei Servizi Finanziari dello Stato di New York (DFSNY) ha pubblicato un regolamento[135] sulle *Virtual Currencies* rivolto a quelle imprese impegnate in attività con le monete virtuali.
Queste imprese per poter operare devono essere in possesso di una licenza, la BitLicense.

Stato di New York

Come precisa il regolamento alla lettera q) di pagina 6 nella nozione di "*virtual currency business activity*" rientrano le seguenti attività:

- ricezione o trasmissione di valuta virtuale;
- conservazione, custodia o controllo di valuta virtuale per conto di altri soggetti,
- l'attività professionale di acquisto e vendita di valuta virtuale;
- la prestazione del servizio di cambio valuta virtuale in valuta avente corso legale e viceversa;
- l'emissione, l'amministrazione e il controllo di valuta virtuale.

Queste attività devono comunque riguardare un soggetto che sia residente, domiciliato o che sta conducendo affari nello Stato di New York.
Le imprese devono verificare l'identità dei loro clienti, devono monitorare e notificare al Dipartimento le transazioni che eccedono i $ 10.000 al giorno per persona e le operazioni sospette di riciclaggio, evasione fiscale o altre attività criminali.
Per richiedere la licenza l'impresa deve pagare una tassa di iscrizione pari a $ 5.000 e la domanda di licenza potrà essere accettata o negata entro 90 giorni dalla presentazione della stessa.

[135] https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

Questo progetto però è risultato troppo restrittivo e molte imprese infatti non sono più attive a New York.

Ad oggi infatti solo cinque organizzazioni hanno ricevuto la licenza[136].

Il legislatore di New York sta attualmente considerando un nuovo disegno di legge, presentato il 14 febbraio 2018[137], che istituirebbe una *task force* per studiare la *cryptovaluta*.

La *task force*, composta da 9 membri nominati dal governatore, presidente temporaneo del Senato, presidente dell'assemblea, sovrintendente del dipartimento dei servizi finanziari e dal direttore dell'ufficio dei servizi di tecnologie dell'informazione, avrà il compito di analizzare l'impatto della designazione delle "zone di empowerment economico" per l'estrazione di *cryptovalute* al fine di comprendere i requisiti di idoneità della località, il potenziale impatto di tale designazione sulla forza lavoro di quella località ed eventuali minacce alla sicurezza informatica.

Nel caso in cui la proposta venisse accettata la *task force* dovrà presentare entro un anno i risultati al governatore e al corpo legislativo.

Canada

Il 19 giugno 2014 il Parlamento del Canada ha approvato *Bill C-31*[138], la prima legge nazionale sull'uso dei *bitcoins*.

La legge prevede che sia le imprese che hanno una sede commerciale in Canada sia le società che hanno una sede di attività fuori dal Canada ma che offrono servizi a persone o entità in Canada, e comunque solo per operazioni che superano la soglia di $ 10.000, sono destinatari delle norme sull'Antiriciclaggio e Antiterrorismo previste dal *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA).

Messico

Nel marzo 2018 un disegno di legge diretto a favorire lo scambio delle *cryptovalute* è stato approvato dalla Camera del Governo[139].

[136] https://en.wikipedia.org/wiki/BitLicense

[137] http://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=A09862&term=2017&Summary=Y&Actions=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y&Text=Y&Chamber%26nbspVideo%2FTranscript=Y

[138] http://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/third-reading

[139] https://www.reuters.com/article/us-mexico-fintech/mexico-financial-technology-law-passes-final-hurdle-in-congress-idUSKCN1GD6KX

Scopo del disegno di legge è cercare sia di promuovere la stabilità finanziaria che prevenire il riciclaggio di denaro offrendo alle imprese *Fintech* una maggiore regolamentazione riguardo alle *cryptovalute*, ai metodi di pagamento ed al *crowdfunding*.
Verrà inoltre consentita la condivisione delle informazioni degli utenti da parte delle istituzioni finanziarie purché gli utenti siano d'accordo.
Questa proposta di legge, elaborata in termini generici, sarà seguita nei mesi successivi da normative secondarie più dettagliate.

Australia

In Australia le valute digitali subiscono un diverso trattamento: bisogna infatti fare una distinzione:
1) fra transazioni dirette a un investimento o a un'attività commerciale e
2) transazioni per uso personale.

Nel caso in cui l'acquisto sia orientato ad un investimento le plusvalenze che vengono realizzate devono essere tassate.

Discorso diverso va fatto nel caso in cui l'acquisto dei *bitcoins* sia diretto ad esempio all'acquisto di un bene per uso personale, come ad esempio una lavatrice, e quindi non rilevante a fini impositivi.

A monte di tutto questo c'è la tutela dal rischio di attività fraudolente.
Nel mese di aprile del 2018 nuove normative antiriciclaggio sono state emanate.
L'AUSTRAC[140] (*Australian Transaction Reports and Analysis Centre*), l'agenzia governativa che si occupa insieme ad altri organi istituzionali di studiare e contrastare minacce di tipo finanziario (tra cui riciclaggio, evasione fiscale e finanziamento del terrorismo), ha messo in atto nuove leggi per i fornitori di *Digital Currency Exchange* (DCE).
Per cercare di minimizzare il rischio che i criminali possano utilizzare i DCE per riciclare denaro o per finanziare il terrorismo, i fornitori di servizi di *cryptovalute* con un'attività commerciale ubicata in Australia devono registrarsi presso AUSTRAC e attuare procedure di segnalazione e controllo delle identità.
Gli *exchange* dovranno rispettare quattro regole fondamentali per poter operare a norma di legge:

[140] http://www.austrac.gov.au

- adottare e mantenere un programma per combattere il riciclaggio di denaro ed il finanziamento del terrorismo;
- identificare e verificare l'identità dei propri clienti;
- riferire all'AUSTRAC qualsiasi attività sospetta e transazioni che comportano somme di denaro contante per un valore di $ 10.000 o superiore;
- mantenere certi registri per almeno sette anni.

Cina

Il rapporto tra Cina e *bitcoin* è sempre stato molto difficile.

La PBOC (Banca Popolare della Cina) con un rapporto del 5 dicembre del 2013 ha proibito a banche e istituzioni finanziarie di detenere ed effettuare transazioni in *cryptovalute*.

La banca centrale ha spiegato che, anche non costituendo una minaccia al sistema finanziario cinese, l'utilizzo può comunque comportare alcuni rischi come ad esempio favorire le organizzazioni criminali a riciclare gli introiti delle loro attività illegali.

Il divieto però non riguarda i privati i quali sono liberi di utilizzare la moneta virtuale come meglio credono.

Nonostante ciò secondo un report della banca Goldman Sachs la Cina movimentava l'80% della moneta virtuale nel 2015[141].

A settembre del 2017[142] i regolatori cinesi hanno imposto il blocco di tutti gli *exchange* cinesi per cercare di limitare, quanto più possibile, le attività criminali.

Nonostante il blocco la popolazione cinese ha continuato ad utilizzare le *cryptovalute* usando *exchange* esteri.

[141] www.financemagnates.com
[142] https://www.ilbitcoin.news/la-cina-blocca-ufficialmente-le-cryptovalute/

Per questo motivo le autorità hanno cercato di bloccare l'accesso ai siti internet di questi *exchange* ma con scarsi risultati.

Nello stesso periodo la Cina ha dichiarato illegali le ICO (*Initial Coin Offering*), il sistema di raccolta fondi basato sulle *cryptovalute*.

In realtà però non si tratterebbe di un divieto ma di una sospensione temporanea.
Questo è quanto affermato in un'intervista[143] da Hu Bing, ricercatore presso l'*Institute of Finance and Banking*[144].
La sospensione deriverebbe dalla necessità per il governo di valutare il potenziale degli ICO in un ambiente controllato, attraverso un programma di licenze.
In pratica si verrebbe a creare un programma di licenze simile a *BitLicense* del Dipartimento dei Servizi Finanziari dello Stato di New York.
Come detto a seguito dello scandalo *Evergrande* la Banca Centrale Cinese alla fine di settembre 2021 ha vietato le transazioni in *cryptovalute* – Il sole 24 ore del 25 settembre 2021 pag. 4

Giappone

Il Giappone è allo stato attuale uno dei paesi in cui le *cryptovalute* risultano essere più diffuse che in altre parti del mondo.

Il governo giapponese il 1° Aprile 2017 ha approvato una legge con la quale il *bitcoin* viene riconosciuto come metodo legale di pagamento[145].

Si tratta della prima legge al mondo che riconosce *bitcoin* e le altre valute digitali come forma di pagamento.

La legge approvata legalizza gli *exchange* con requisiti patrimoniali, di sicurezza informatica e procedure operative migliori e più sicure.

[143] http://finance.chinanews.com/shipin/2017/09-06/news730639.shtml
[144] Organizzazione di ricerca accademica sostenuta dal governo cinese.
[145] http://www.gavrilobtc.it/oggi-il-giappone-legalizza-il-bitcoin-come-metodo-di-pagamento-01042017/

Questi sono obbligati a registrarsi presso il *Financial Services Agency* (FSA) giapponese, ovvero l'ente governativo che regola i mercati finanziari, il quale rilascerà le licenze operative agli *exchange*.

La licenza applica alcuni requisiti operativi per gli scambi, inclusi elevati standard per la sicurezza in rete, la verifica delle identità dei clienti ed il controllo che gli scambi di *cryptovalute* non siano utilizzati per il riciclaggio di denaro sporco.

Nel corso dei mesi comunque si sono verificati casi in cui l'Agenzia per i servizi finanziari ha bloccato le attività di alcuni cambio valute virtuali a causa del fatto di aver operato senza licenza.

Sempre nel 2017 un altro disegno di legge è stato approvato: si tratta della riforma fiscale che elimina l'imposta sulla vendita di *bitcoin*, entrato in vigore il 1° luglio[146].

[146] https://nextgenerationcurrency.com/e-ufficiale-il-giappone-ha-eliminato-limposta-su-bitcoin/

5) BIG DATA

5.1) Nozione e funzione dei *Big Data*

In statistica e informatica, la locuzione inglese ***Big Data* ("grandi masse di dati")**, o in italiano "megadati", indica genericamente una raccolta di dati informativi così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore o conoscenza.
Il termine è utilizzato dunque in riferimento alla capacità (propria della scienza dei dati) di analizzare ovvero estrapolare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati, grazie a **sofisticati metodi statistici e informatici di elaborazione**, allo scopo di scoprire i legami tra fenomeni diversi aventi possibili correlazioni e prevedere quelli futuri.

Le peculiarità dei *Big Data* possono essere schematizzate per semplicità nelle ***Six V of Big Data***, ovvero degli aggettivi che efficacemente riescono a sintetizzare le caratteristiche più importanti di tali strumenti, ed abbiamo:

1. ***Variety***: con varietà si intende la natura dei dati presenti all'interno del database, distinguendo dati di tipo strutturato, e non strutturato come foto, video, audio, PDFs, etc. dove, questi ultimi, rendono maggiormente difficoltosi processi come *storing, mining and analyzing data*[147].

2. ***Volume***: il volume rappresenta una caratteristica peculiare dei Big Data in quanto essi inglobano al loro interno una quantità mastodontica di dati in aumento continuo attraverso un flusso continuo ed ininterrotto.

3. ***Velocity***: il termine velocità è correlato ad una duplice situazione, la prima definita dal flusso di informazioni in entrata proveniente da diverse fonti come *mobile device, business processes, sensor, social media, application logs*, la seconda da *how fast the data is produced and processed to meets the demands.*

[147] Joshi, Ramesh C., Gupta, Brij B; *Security, Privacy, and Forensics Issues in Big Data* (2019), pagina 26.

4. ***Variability***: la variabilità dei dati nel corso del tempo è strettamente relazionata all'interpretazione ed elaborazione degli stessi, questo comporta quindi l'utilizzo degli stessi attraverso un analisi profonda che comprende l'inclusione del contesto e del momento di riferimento.

5. ***Veracity***: la veridicità del dato è un elemento qualitativo di grande importanza per l'utilizzo dei Big Data, poiché un'informazione non veritiera o molto poco accurata non potrà essere utilizzata in analisi, altrimenti porterebbe a delle distorsioni di valutazione.

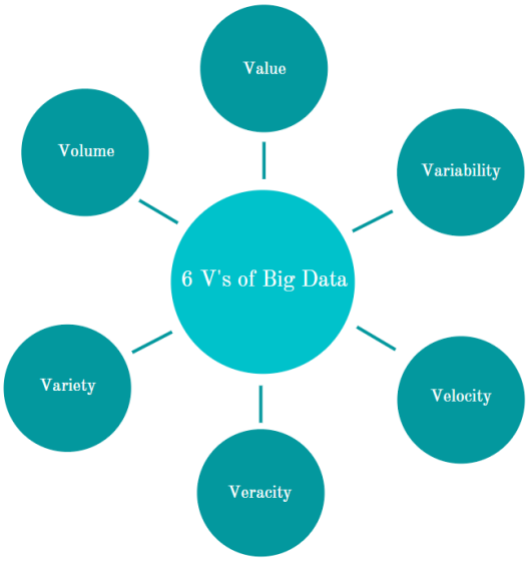


Figura 18 - Le sei V dei *Big Data*

6. ***Value***: ultimo, ma non per importanza, **il valore** è la caratteristica più complessa delle sei, in quanto essa rappresenta il reale utilizzo dei dati presenti all'interno dei database. Il valore dei dati cresce in base alla potenza, velocità e precisione dei processi di elaborazione dei dati grezzi in informazioni utili e accurate che permettono il porre in essere azioni con il miglior focus possibile sull'obiettivo da perseguire. *Qui sono le metodologie di Big Data Analytics ad essere fondamentali, attraverso il loro utilizzo un'impresa può estrarre valore, ovvero prendere decisioni più informate, tempestive e consapevoli, dal vasto mondo dei Big Data.*

I *Big Data* sono *l'asset* fondamentali **dell'economia dell'informazione**.
Gli agenti economici che costituiscono il c.d. ciclo dei *Big Data* (o catena del valore), sono:

1) Imprese,
2) consumatori e
3) autorità del settore pubblico

all'interno del quale sono individuate:

5.2) Le attività che conferiscono valore ai dati:

1. la raccolta,
2. l'archiviazione,
3. l'analisi ed organizzazione,
4. l'utilizzo dei dati.

A ogni attività tipica delle fasi della **catena del valore** corrisponde un **mercato dei *Big Data***, caratterizzato da qualità economiche ed attori differenti.

In ogni anello della catena del valore, inoltre, sono presenti **limiti all'accesso ai *Big Data*** più o meno insormontabili, che determinano l'insorgere di vantaggi competitivi in capo alle imprese operanti in ciascun passaggio della catena del valore.

Saranno presi in esame i distinti ***Big Data submarkets***; in particolare se ne analizzeranno le caratteristiche economiche e si individueranno **i limiti giuridici all'accesso** propri di ogni fase della catena del valore.

Ci si concentrerà anche sui soggetti coinvolti nei passaggi del *Big Data cycle*.

Si tenga presente che a Bologna nella sede dell'ex Manifattura Tabacchi prenderà vita tra la fine del 2021 e l'inizio del 2022 il *Big Data Technopole*, uno dei maggiori centri di elaborazione dati d'Europa.

Si ricorda che il concetto di **CATENA DEL VALORE** è stato teorizzato dall'economista **Michael E. Porter** in un saggio del 1985.

Con questa espressione gli studiosi dell'economia fanno riferimento alla sequenza delle attività strategicamente rilevanti mediante le quali l'impresa genera, nelle fasi di produzione del bene o erogazione del servizio le informazioni ottenute dai beni e dai servizi stessi che l'impresa mette a disposizione dei consumatori e delle imprese operanti sul mercato.

Maggiore è il valore aggiunto conseguito in ogni "anello", maggiore è il vantaggio competitivo che l'attore economico ottiene sul mercato.

5.2.a) La raccolta dei dati

La raccolta dei dati (*data capture o data collection*) **costituisce la prima fase della catena del valore dei *Big Data*.**

I *Big Data* provengono da una **molteplicità di fonti** (*data sources*), cioè da entità che pongono in essere il dato e lo immettono nel mercato al pari delle altre risorse.

È evidente che conferire ordine al caos delle fonti è un'operazione poco agevole, poiché la produzione di dati avviene su larga scala e in diversi contesti e tocca realtà imprenditoriali di ogni settore, salvo nei casi in cui la documentazione dell'impresa sia tenuta in via manuale o in formati analogici.

Si è scelto di esaminare la produzione dei *Big Data* facendo riferimento a una classificazione di carattere soggettivo, basata sulle peculiarità del *data provider* – fornitore di dati: le fonti si distinguono a seconda che quest'ultimo sia **una persona fisica o una persona giuridica** abbia **personalità di diritto privato o pubblico**.

a) In caso di Entità di **diritto privato**, le principali **fonti dei *Big Data*** da cui attingono i soggetti economici comprendono:

1) i dati, in stato grezzo, direttamente o indirettamente forniti dagli utenti-consumatori in Rete,

2) i dati interni delle imprese,

3) quelli forniti dalle imprese che vendono i dati sul mercato (c.d. ***data brokers***);

b) in caso di Entità **di diritto pubblico**, si tratta dei **c.d. *public data***, fra i quali sono compresi gli *open data*, o *open government data* (OGD), cioè i dati raccolti e messi a disposizione dagli enti del settore pubblico per il riutilizzo anche a fini commerciali.

La raccolta è svolta principalmente mediante:

1) **i *log files***, che registrano le attività degli utenti e sono prodotti automaticamente dalla fonte di produzione, oppure mediante

2) i **c.d. *web crawlers***, programmi che consentono la registrazione e l'indicizzazione di pagine web.

Anche l'accesso alle banche dati delle pubbliche amministrazioni avviene *online*, attraverso i portali presenti sui siti web delle stesse.

Ingenti quantità di dati sono acquisite mediante l'utilizzo di oggetti interconnessi a una rete **(c.d. *Internet of Things*, IoT).**

Tali dati, che sono di diverso genere (si tratta di dati geografici, ambientali, o generati dagli elettrodomestici *Smart*, o ancora mediante tecnologie *wearable*) sono raccolti in tempo reale e si riferiscono a coordinate spazio-temporali precise,

3) infine, alcuni dati sono **raccolti *offline*** in vari modi: si pensi ai sondaggi e ai "programmi fedeltà" (*loyalty programs*) dei supermercati.

Da questa breve analisi si deduce che consumatori e imprese possano essere parte integrante della catena del valore dei dati, giacché essi da un lato possono essere coloro cui il dato si riferisce, dall'altro i soggetti che producono il dato.

Le limitazioni all'accesso ed il potere di mercato sono parzialmente affievoliti dalle attività economiche di soggetti intermediari, come i ***data brokers***, che si procurano e rivendono i dati sul mercato (di cui parleremo diffusamente al paragrafo 5.3.a).

I dati degli utenti sono particolarmente vantaggiosi per gli inserzionisti che li utilizzano per intercettare le preferenze ed i comportamenti dei primi e, sulla base di questi, migliorare le strategie di marketing individuando contenuti pubblicitari mirati per ciascun consumatore (c.d. pubblicità comportamentale, o *behavioural targeting*).

Nella catena del valore dei ***Big Data***, alla fase

1) dell'acquisizione segue quella
2) dell'archiviazione (*storage*), che consiste nell'immagazzinamento e
3) dell'analisi e dell'organizzazione (*sorting*) dei *datasets*, infine quella
4) dell'utilizzo.

L'organizzazione dei dati non è solo l'attività più importante svolta dagli elaboratori, ma anche una delle ragioni per cui i computer sono nati.

5.2.b) Archiviazione dei dati

Più problematici, invece, sono i profili riguardanti **la sicurezza**, i costi energetici dell'immagazzinamento dei *Big Data* e i costi di transizione dovuti al passaggio da una tecnologia a un'altra (c.d. *switching costs*).

Con lo sviluppo del ***Cloud Computing***, inoltre, i costi dell'archiviazione dei dati si sono ulteriormente abbattuti.

Il ***Cloud***, infatti, consente alle imprese e agli utenti finali dei servizi l'efficace immagazzinamento e l'accesso ai dati forniti mediante un diretto collegamento alla Rete.

La sicurezza dei sistemi di immagazzinamento dei dati

Problemi giuridici legati alla *privacy*

I sistemi di **archiviazione** dei ***Big Data***, e soprattutto quelli basati sul *Cloud*, pongono serie **problematiche giuridiche**, legate alla ***privacy*** informazionale ed alla protezione dei dati dei consumatori e, soprattutto, alla **sicurezza della conservazione dei dati**.

Si ritiene comunemente che la questione più spinosa in tema di sicurezza sia la **minaccia di intrusione nei sistemi di memoria da parte di soggetti terzi**, quali ***hackers* e governi stranieri**.

I limiti dell'approccio tradizionale al tema della sicurezza e le nuove esigenze dettate dall'avvento dei *Big Data* hanno determinato nuovi problemi e sviluppi in tema di ***cybersecurity***, fondata su un modello di valutazione dei rischi (*risk assessment*) già noto ad altri settori.

La soluzione *risk-based*, a differenza di quella tradizionale, **è integrata** nella **catena del valore dei *Big Data***: i rischi legati alla sicurezza sono le conseguenze negative dovute a eventi incerti e imprevisti dei benefici sperati nello sfruttamento economico del ciclo dei *Big Data*.

L'Unione Europea con il **Regolamento UE 2016/679 - GDPR** ha innovato notevolmente **il quadro legislativo** in tema di **protezione dei dati personali**, imponendo obblighi e **limiti all'archiviazione dei dati personali** e, in particolare, prevedendo lo svolgimento della valutazione dei rischi.

Il grande giro di affari riguardante l'utilizzo dei *Big Data*, soprattutto da soggetti la cui forza contrattuale risulta elevata, ha portato l'Unione Europa ad emettere una legislazione ad hoc a tutela e garanzia della privacy attraverso **il Regolamento 2016/679 noto come GDPR (General Data Protection Regulation)** che, come espresso dalla Commissione Europa, rappresenta un *passo essenziale per rafforzare i diritti fondamentali dei singoli nell'era digitale e agevolare le attività economiche rendendo chiare le regole per le imprese nel mercato unico digitale.*
Il Regolamento in questione, sostitutivo della Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) e aggiornato dalla rettifica pubblicata in GUUE il 23/05/2018, pone dei pilastri normativi finalizzati ad adeguare l'Europa digitale in materie di protezione dei dati personali eliminando la forte frammentazione e diversificazione in materia dei Paesi membri.

Tra le novità del seguente testo normativo abbiamo i seguenti punti di maggiore interesse:

1) **Portabilità dei Dati**: tale diritto dell'utente è disciplinato dall'**articolo 20 del GDPR**, che permette all'interessato (soggetto a cui sono collegati i dati di riferimento), di richiedere, al titolare del trattamento (o *data controller*[148]), i propri dati personali ed inviarli ad un altro titolare senza impedimenti.

[148] https://protezionedatipersonali.it/titolare-del-trattamento

Impedimenti però che potrebbero verificarsi nel caso di adozione di standard differenti degli operatori che non permetterebbero la portabilità dei dati personali tra le diverse piattaforme di riferimento.

2) **Principio di *Accountability***: tale principio, introdotto attraverso l'**articolo 35 del GDPR**, è volto alla *minimizzazione dei rischi di violazione dei diritti individuali per il tramite dei Big Data*[149] attraverso, da parte del titolare del trattamento, una valutazione preventiva, o una serie di esse, sulla sicurezza e protezione dei dati personali dei soggetti interessati e della loro elaborazione finale; tali valutazioni dovranno, come da normativa, riguardare tutti i dati relativi a profilazioni che comporteranno effetti giuridici, categorie particolari di dati personali (**art. 9 paragrafo 1 del GDPR**) e dati di sorveglianza in larga scala su zone pubbliche.

   Tali valutazioni interessano inoltre una serie di tipologie di trattamento dei dati che sono individuate dalle preposte Autorità di controllo.

   L'obbligo scaturente nei confronti del titolare del trattamento però *non si esaurisce nella fase "progettuale" nell'utilizzo dei Big Data; opportune misure devono essere poste in essere per monitorare con sistematicità l'efficacia delle soluzioni predisposte, affinandole se necessario, e verificare la qualità del processo posto in essere*[150].

3) **Codici di condotta**: l'**articolo 40 del GDPR**, per facilitare il rispetto del precedente punto, ha introdotto la possibilità di predisporre ed adottare dei codici di condotta da parte di associazioni di categoria (o altri organismi) che rappresentano i responsabili del trattamento.

   Tra i maggiormente significativi abbiamo il Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali che riguarda i soggetti operanti nel settore di attività di informazione commerciale e che pone vincoli ferrei sulla certezza, affidabilità e aggiornamento delle informazioni in possesso, sui requisiti di natura tecnica legate alla protezione dei dati in possesso dei fornitori aderenti e sulla garanzia di esercizio dei propri diritti alla *privacy* dei soggetti interessati[151].

4) **Registro delle attività di trattamento dati**: importante inclusione all'interno del **GDPR all'articolo 30**, esso rappresenta un importante strumento per garantire *l'accountability* –

[149] AGCM – AGCOM - CPDP, 2020, Indagine conoscitiva sui Big Data, pagina 66.
[150] AGCM – AGCOM - CPDP, 2020, Indagine conoscitiva sui Big Data, pagina 67.
[151] Anna Cataleta, A. Longo, R. Natale, 2020, GDPR: Tutto ciò che c'è da sapere per essere in regola.

responsabilità - del titolare del trattamento dei dati personali, attraverso la redazione di un registro (digitale o cartaceo), per tutte le imprese con almeno 250 dipendenti, contenente una serie di informazioni circa le informazioni critiche del trattamento delle *categorie interessate e delle categorie di dati personali, finalità del trattamento, soggetti preposti alla protezione dei dati, trasferimenti dei dati personali, e ove possibile le misure di sicurezza tecniche ed organizzative adottate*[152].

5) **Designazione del DPO**: il DPO, ***Data Protection Officer*** è un soggetto che, secondo la normativa del **GDPR, sezione 4 (art. 37, 38, 39**), dev'essere designato all'interno dell'entità aziendale di riferimento; in particolare la sua nomina è obbligatoria per:

a) Enti pubblici: quando il trattamento dei dati è effettuato da un'autorità pubblica o da un organismo pubblico, ad eccezione per gli organi giurisdizionali nell'esercizio delle loro funzioni;

b) Imprese private: quando la core activities del titolare del trattamento dei dati (o responsabile del trattamento) consista in *trattamenti che richiedono il monitoraggio su larga scala*[153] e/o quando consista in *trattamenti su larga scala di informazioni sensibili e/o di dati relativi a condanne penali o reati*.

In sintesi, vi dovrà essere l'adozione della figura del DPO per tutte quelle realtà che, in ambito privato, hanno come attività principale la profilazione e/o il trattamento di dati giudiziari o di salute su larga scala attraverso dispositivi interconnessi o la creazione di campagne di marketing mirate, programmi fedeltà, profilazione creditizia o assicurativa su larga scala.

Oltre al rispetto essenziale del principio di *accountability*, principio dove il titolare e i responsabili del trattamento dovranno garantire, per tutto il processo che riguarda il trattamento dei dati, il rispetto della conformità di trattamento ed il miglior sistema di protezione, con annesse prove atte a documentarla.

L'adozione del DPO, nei casi in cui essa è obbligatoria o su base volontaria, risulta un prezioso valore aggiunto in termini qualitativi e di sicurezza in merito ai dati oggetto del trattamento.

[152] https://protezionedatipersonali.it/registro-dei-trattamenti

[153] GDPR con relative Rettifiche, 2016-2018, Regolamento 2016/679, Parlamento UE e Consiglio, art. 37.

In particolare, il **Responsabile della Protezione dei Dati Personali**, cioè il ***Data Protection Officer* (DPO).**

In capo al **GDPR** c'è l'obbligo di nominare il **Responsabile della Protezione dei Dati Personali**, cioè il **Data *Protection Officer* (DPO).**

Il *Data Protection Officer* è una figura professionale obbligatoria per tutti i 27 Stati dell'Unione Europea, il cui compito è quello di **valutare e gestire il trattamento dei dati personali, con lo scopo di far rispettare le normative europee in materia di *privacy*.**

Questa persona non solo deve avere ampie competenze in campo informatico, ma anche in ambito giuridico, di valutazione del rischio e di analisi dei processi.

I compiti del DPO identificati, seppur non in modo esaustivo, dalla normativa di riferimento, sono diversi, ovvero:

1. **Art. 39.1.a**: informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal Regolamento;
2. **Art. 39.1.b**: sorvegliare l'osservanza del Regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dei dati nonché sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
3. **Art. 39.1.c**: fornire pareri, se richiesti, alla redazione della Data Protection Impact Assessments (c.d. DPIA menzionato all'art. 35 del GDPR) e sorvegliarne lo svolgimento;
4. **Art. 39.1.d**: fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali[154];
5. **Art. 36 e 39**: fungere da punto di contatto tra titolare ed Autorità Garante in termini di documentazione, nel caso in cui precedentemente al trattamento dei dati il titolare consulti l'autorità di controllo in merito alla valutazione dell'impatto sulla protezione

[154] https://www.garanteprivacy.it/home/autorita

dei dati (**art. 35**) ed essa raggiungesse un rischio elevato in assenza di misure adottate dal titolare al fine di mitigare quest'ultimo.

6. Controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. Data Breach Notification Management).

L'articolo 37 del Regolamento però lascia spazio a diversi **dubbi**, infatti non sono specificate quali debbano essere le qualità professionali necessarie per essere DPO.

Ulteriore elemento di complessità è dato **dall'articolo 38**, che specifica che il DPO non deve trovarsi in nessuna situazione di conflitto di interessi, con la conseguenza che un DPO non possa essere rappresentato dal responsabile aziendale dell'ICT (*Information Communication Technology)*. Per la stessa motivazione, non può essere nominato DPO né l'amministratore delegato, il responsabile operativo, il responsabile sanitario o finanziario, il direttore di marketing e neppure il direttore delle risorse umane.

a) Sempre **nell'articolo 37 del Regolamento** viene definito che la nomina del DPO è obbligatoria quando il trattamento dei dati "*venga effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali nell'esercizio delle proprie funzioni*".

In particolare il ***Data Protection Impact Assessment*** - DPIA, menzionato al punto 3 del precedente elenco e previsto all'art. 35 del GDPR, può essere descritto come un procedimento che mira a *descrivere un trattamento di dati […] per valutarne i relativi rischi e apportare misure idonee ad affrontarli*[155]; essa è uno degli strumenti principali per il rispetto del principio di responsabilizzazione (accountability) ed il rispetto delle prescrizione dell'RGPD - Regolamento Generale sulla Protezione dei Dati.

Tale procedura è di responsabilità del Titolare del Trattamento, ma può essere affidata ad un altro soggetto (DPO) ed è:

1) **Obbligatoria**: quando può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, e più specificatamente secondo l'art. 29, quando riguardano trattamenti valutativi, di

[155] GDPR con relative Rettifiche, 2016-2018, Regolamento 2016/679, Parlamento UE e Consiglio, art. 35.

scoring, con effetti giuridici, monitoraggio sistematico, combinazione di insieme di dati derivanti da due trattamenti differenti o titolari distinti; dove quest'ultimo caso rappresenta la fattispecie dei *Big Data*.

Altra importante categoria all'interno dell'obbligatorietà è anche quella dove il trattamento dei dati potrebbe impedire ad un soggetto l'esercizio di un suo diritto o l'utilizzo di un servizio (es. screening per l'accensione di un finanziamento), in questo caso all'emergere anche di una delle due fattispecie menzionate precedentemente la DPIA risulta necessaria.

2) **Non Obbligatoria**: quando non vi è un elevato rischio per diritti e libertà dei soggetti e per tutte quelle casistiche definite dalle Linee Guida del Gruppo ex art. 29, ovvero: casi in cui si ha una natura o una finalità molto simile ad un trattamento in cui già è stata svolta la DPIA o rientrano nelle fattispecie escluse dall'obbligatorietà e ne risulta solo facoltativa.

Un altro meccanismo finalizzato ad una miglior protezione dei dati personali da parte dei titolari del trattamento o dei responsabili del trattamento è stabilito dall'**articolo 42 e seguenti del GDPR**: esso è volto alla **creazione di possibili schemi di "certificazione"** volti a dimostrare il rispetto delle conformità previste dal Regolamento in termini di misure tecniche ed organizzative (**art. 24, 25, 32**) ed è di natura volontaria.

La certificazione in questione però *non è una prova della conformità, ma rappresenta piuttosto un elemento che può essere utilizzato per dimostrare la conformità […] illustrando le modalità con cui vengono soddisfatti i criteri e come si intende soddisfarli nel caso in cui non siano soddisfatti*[156].

Con il termine "**certificazione**", per chiarezza interpretativa, possiamo intenderla secondo il significato datogli dall'ISO (Organismo Internazionale di Standardizzazione) ovvero "rilascio, da parte di un organismo indipendente di un'assicurazione scritta che il prodotto, servizio o sistema in analisi soddisfa dei requisiti specifici".

Con il termine "sigillo" o "marchio" menzionato all'interno del GDPR si intende invece l'esito positivo risultante alla fine del meccanismo di certificazione.

La certificazione in questione può essere rilasciata, secondo l'**art. 42 del GDPR**, da due soggetti, ossia:

[156] Garante per la protezione dei dati personali, Linee guida Europee, 2019, pagina 317.

1) da un **Organismo di Certificazione Accreditato**: organo differente dall'autorità di controllo che è proprietario dello schema di certificazione approvato precedentemente dall'autorità di controllo e che ha, come ruolo, quello di rilasciare, rinnovare o di revocare le certificazioni, comunicando la decisione ex-ante all'autorità di controllo (**art. 43, paragrafo 1**).

   I criteri di certificazione adottati dall'organismo accreditato sono poi a loro volta periodicamente riesaminate dall'autorità di controllo per verificarne la coerenza[157].

2) dall'**Autorità di Controllo**: dove, a differenza degli organismi accreditati e sotto il rispetto delle decisioni nazionali in materia di accreditamento, essa può optare per diverse linee di azione ovvero rilasciare essa stessa la certificazione in relazione al proprio schema, delegare ad altri soggetti il processo di valutazione del rispetto del proprio schema o affidare a terzi il compito della valutazione e del rilascio della certificazione.

   Le diverse opzioni dell'autorità di controllo devono però trovare conciliazione con la massima indipendenza esercitabile, al fine di evitare conflitti di interesse nell'esercizio delle funzioni di indagine ed esecuzione ad essa preposti.

   b) **nell'articolo 37** è definito che anche imprese private necessitino della nomina del DPO.
      Il requisito richiesto è che l'attività principale del Titolare del Trattamento dei dati "*consista in trattamenti richiedenti il monitoraggio sistematico su larga scala*" oppure "*riguardino il trattamento, su larga scala, di informazioni sensibili o di dati relativi a condanne penali e a reati*".

Accountability **– Responsabilizzazione**

Il GDPR introduce il **principio** di ***accountability* - responsabilizzazione**, in base al quale il Titolare del Trattamento dati – DPO - deve sia seguire una serie di principi contenuti negli **articoli 5 e 6**, ma anche assicurarsi della dimostrabilità della sua corretta condotta.

I dati personali devono quindi essere trattati rispettando i seguenti **principi**:

1) liceità, correttezza e trasparenza del trattamento;
2) limitazione della finalità del trattamento e minimizzazione dei dati (cioè condividere solo quelli strettamente necessari);

[157] GDPR, articolo 43, paragrafo 2, lettera c.

3) esattezza e aggiornamento dei dati, compresa la opportuna cancellazione dei dati che risultino inesatti;
4) limitazione della conservazione;
5) integrità e riservatezza.

5.2 c) Analisi ed Oganizzazione dei dati

Il ruolo dei *Big Data analytics*

Due sono i principali obiettivi cui mira un'impresa con le attività di *analytics*:

a) capire le preferenze dei consumatori

b) prevedere i trends del mercato.

Le informazioni che ne risultano:

1) **possono essere cedute a terzi, oppure**

2) **essere utilizzate dall'impresa stessa.**

Riguardo al lato della domanda, gli algoritmi comportano taluni costi per i consumatori.

L'**utilizzo *contra legem*** di **procedimenti automatizzati per l'analisi dei *Big Data*** provoca esternalità negative nei confronti di soggetti terzi, nel senso che «*la loro curva di indifferenza (o di utilità) è affetta da comportamenti di altri individui, al di fuori dai consueti meccanismi dello scambio di mercato*».

Tali ricadute, che **nel mondo giuridico** sono riconducibili alla **nozione civilistica delle immissioni** (*nuisances*), comprendono quattro fattori differenti.

1) Anzitutto, alcuni soggetti possono rimanere esclusi dai rapporti con il resto della società sulla base dei dati analizzati mediante l'uso di algoritmi. VIOLAZIONE DELLA PARITA' DI DIRITTI

In altre parole, si pongono **problematiche legate alla discriminazione dei consumatori interessati dalle operazioni algoritmiche.**

2) In secondo luogo, l'utilizzo di algoritmi può provocare danni alla reputazione di talune categorie di consumatori, tracciandone profili identitari distorti.

3) In terzo luogo, l'accumulo dei dati degli utenti e la classificazione di questi ultimi in base alla valutazione dei rischi connessi alla persona **può precludere l'accesso a determinati servizi**.

4) Infine, **le decisioni prese mediante l'uso di algoritmi sono poco trasparenti**, e un'adeguata comprensione di queste richiede la collaborazione degli operatori e delle imprese che hanno elaborato le modalità di funzionamento dell'algoritmo.

5.2.d) L'utilizzo dei dati: inclusa la vendita dei dati

L'uso dei ***Big Data*** costituisce **l'ultimo anello della catena del valore**.

Tale fase inerisce a due attività fondamentali.

Il detentore dei dati, infatti, può decidere:

1) di utilizzare le informazioni ai propri fini allo scopo di operare scelte strategiche sul mercato

2) oppure cedere le informazioni a terzi.

La compravendita dei *Big Data* è molto diffusa nel settore dei ***data brokers***, che ricavano i dati da una pluralità di fonti, li aggregano e li vendono ai propri clienti.

Le principali barriere all'entrata nel mercato dell'utilizzo dei dati hanno natura contrattuale.

Fino a qualche anno fa, il soggetto che acquisiva i dati poteva imporre limiti di natura contrattuale alla portabilità dei dati personali dell'utente, cioè al trasferimento degli stessi a un altro soggetto titolare del trattamento, pur non essendo molto diffuso nella pratica.

L'utente era costretto a sopportarne costi di transizione (*switching costs*) e, se questi ultimi erano troppo elevati, gli era precluso il passaggio ad un altro titolare del trattamento (effetto *lock-in*).

Limiti al trasferimento dei dati

Nelle riforme della **normativa europea** in materia di **protezione dei dati personali**, il legislatore europeo ha introdotto una nuova situazione giuridica in capo all'interessato.

Il **Regolamento UE 2016/679 - GDPR**, infatti, prevede che il DIRITTO ALLA PORTABILITÀ (quindi di trasferire) DEI DATI sia esercitato senza impedimenti da parte del primo titolare, qualora il trattamento si effettui con mezzi automatizzati.

In senso contrario, il soggetto che utilizza i dati può limitarne il proprio uso.

Ciò avviene, nella prassi, per chi opera in un segmento di mercato in cui la *privacy* e la custodia dei dati dei consumatori sono assai rilevanti.

N.B. Tali limiti hanno natura contrattuale, giacché l'obbligo - "di non fare" - di astenersi dal concedere i dati dell'utente a terzi grava sull'utilizzatore in forza di un accordo stipulato con l'utente stesso.

Vi sono poi **ulteriori limiti** di carattere giuridico all'utilizzo dei *Big Data*:

- da un lato, l'utilizzo dei dati personali da parte dei soggetti titolari del trattamento incontra limiti nella Normativa Europea della Protezione dei Dati – GDPR di cui abbiamo parlato;
- dall'altro, nel 2017 la Commissione ha emanato una Comunicazione in materia di proprietà dei dati compresi i dati non personali.

5.3) I rischi derivanti dalle attività tipiche dei *Big Data Submarkets*.

Nel perseguimento del profitto, le imprese svolgono attività di utilizzo dei dati personali che hanno un ovvio rovescio della medaglia per i soggetti i cui dati vengono utilizzati.

I rischi più rilevanti sono:

1) la perdita dei dati e i furti di identità (*identity fraud*);
2) la raccolta, la condivisione e l'utilizzo di dati in modalità non accordate o non previste;
3) gli usi impropri dei dati dei consumatori, che originano contatti indesiderati da terzi (c.d. *nuisance contacts* - come e-mail e chiamate da terzi sconosciuti);
4) l'uso discriminatorio dei dati personali.

In conclusione, **quella dei consumatori** è una categoria di soggetti che richiede forme di tutela giuridica efficaci ed elevate dal momento che le attività di raccolta e trattamento dei dati incidono sul loro **diritto alla *privacy* e alla protezione dei dati personali.**

5.4) I *Data Brokers*

La società dell'informazione è costituita da **consumatori** che utilizzano le tecnologie dell'informazione e della comunicazione (ICTs) per interagire fra loro e accedere a prodotti che rendono più semplice la vita quotidiana.

In tali interazioni, **gli utenti rilasciano ingenti quantità di dati personali**, dal cui sfruttamento le imprese attive nei ***Big Data Submarkets*** traggono enormi profitti.

Sono società di *data brokers* per esempio, Acxiom, Experian e Datalogix, società statunitensi leader del settore del ***data brokerage*** e sono presenti in diversi Paesi membri dell'Unione Europea.

Le piattaforme digitali utilizzano le informazioni dei consumatori iscritti per distinguere gli annunci degli inserzionisti in base alle preferenze personali.

Oltre a utilizzarle internamente, le imprese che raccolgono e archiviano i dati in prima battuta possono **cederli a terzi dietro corrispettivo**.

In questo senso nell'era dei *Big Data* **le informazioni personali** divengono beni oggetto di transazioni economiche fra una pluralità di attori, accrescendo notevolmente le possibilità di accumulo di capitale da parte delle imprese.

a) Alcuni agenti economici operano come intermediari fra gruppi di soggetti.

b) Altri attori economici sono specializzati nella vendita dei dati dei consumatori acquisiti da altri: si tratta dei c.d. *data brokers*.

Partiamo dall'inquadramento giuridico di un *Broker*

La figura del *broker* può essere facilmente confusa con quella del mediatore.

Qual è dunque la differenza tra *broker* e mediatore?

Il *BROKER* è una figura professionale in grado di reperire informazioni significative sui mercati e può agire anche per conto, ma non in nome di una delle due parti in causa: vale a dire da un lato l'acquirente e dall'altro il venditore oltre che acquisire dati da un altro *data broker* o da imprese che raccolgono dati per rivenderli.

Il MEDIATORE, invece, è colui che cerca di coniugare gli interessi di entrambe le parti.

DEFINIZIONE operativa: **un *Data Broker* è** «*a company or business unit that earns its primary revenue by supplying data or inferences about people gathered mainly from sources other than the data subjects themselves*».

Da questa definizione, si desumono tre elementi fondamentali:

1. Anzitutto, i *Data Brokers* offrono sul mercato una tipologia particolare di beni (i dati dei consumatori) o di servizi (*data analytics* sulla base di tali dati);

2. in secondo luogo, conducono tale attività in via principale, traendone i maggiori guadagni;

3. in terzo luogo, non acquisiscono gli *input* produttivi direttamente dai consumatori, ma li attingono da fonti diverse da questi ultimi (per esempio, imprese, siti, autorità del settore pubblico, *online stores*, piattaforme digitali ecc.).

N.B. Da quest'ultimo profilo emerge che soggetti come Google, Apple, Facebook, eBay non sono compresi nella categoria dei *data brokers*, giacché acquisiscono i dati degli utenti direttamente, in assenza di un soggetto interposto.

I soggetti che forniscono i *Big Data* come input produttivo ai *data brokers* acquisiscono i dati dai consumatori sia *offline* (si pensi, per esempio, ai dati catastali raccolti dalle autorità del settore pubblico) sia *online* (come i dati delle vendite negli *stores* digitali, le preferenze musicali, le informazioni personali inserite dagli utenti al momento dell'iscrizione a un sito ecc.).

Chiaramente, un *Data Broker* può procurarsi i dati da un altro *Data Broker*.

Le esternalità negative derivanti dalle attività dei "venditori di informazioni" hanno una causa principale e comune: la mancanza di trasparenza, che emerge sotto un duplice profilo:

1) In primo luogo, i consumatori non hanno adeguata consapevolezza del fatto che i *Data Brokers* monetizzino i propri dati personali: secondo uno studio il 64% delle persone intervistate non sa che un supermercato può vendere ad altre imprese le informazioni sulle preferenze di acquisto dei consumatori.

Di conseguenza, questi ultimi subiscono una perdita asimmetrica del loro diritto alla *privacy* (*asymmetrical loss of privacy*), dal momento che le società di *data brokerage* conducono attività di compravendita dei dati **in assenza di consapevolezza del pubblico degli utenti**, nel silenzio di un quadro legislativo poco chiaro **anche se con l'entrata in vigore del GDPR nel 2016 si è in parte regolamentata la materia.**

La maggior parte dei consumatori ignora addirittura l'esistenza dei *Data Brokers* stessi e, quindi, la possibilità di cancellazione o correzione delle proprie informazioni prevista nei portali presenti nei siti web degli *information sellers*.

Alcuni *Data Brokers* prevedono che gli interessati possano chiedere il **c.d. *opting out***, cioè l'esclusione dei dati a loro riferiti dalle operazioni di trattamento.

2) In secondo luogo, emerge un ulteriore profilo problematico: **il c.d. *aggregation effect* (attività di profilazione).**

I *Data Brokers* possono compiere **attività di profilazione senza il consenso dei soggetti interessati** mediante l'aggregazione dei numerosi dati acquisiti dalle diverse fonti: «*while each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life*».

In conclusione, il settore dei *Data Brokers* deve parte della sua crescita dimensionale negli ultimi anni a una regolamentazione poco stringente sulla base della quale i soggetti economici conducono le proprie attività senza limiti sostanziali, idonei alla tutela efficace della *privacy* degli interessati.

Spesso le soluzioni di tutela prospettate dai *data brokers* ai consumatori sono disponibili solo ex post, cioè «*after their data has been bought, aggregated, and sold*».

Questo comporta che il livello di protezione delle informazioni degli interessati sia assai scarso, poiché, pur innestandosi una richiesta di informazioni, i dati possono essere già stati trattati e ceduti a terzi.

Si rammenti che secondo il **Diritto Europeo, il consumatore** è «*qualsiasi **persona fisica** che, nei contratti oggetto della presente direttiva, agisca per fini che non rientrano nel quadro della sua attività commerciale, industriale, artigianale o professionale*» (**art. 2 n. 1 Direttiva 2011/83/UE**

del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori, G.U. n. L. 304 del 22/11/2011).

5.5) I limiti giuridici all'accesso ai dati personali: trattamento e uso

diritto alla *privacy* (USA e UE)

La storia del **diritto alla *privacy***, a ben vedere, è la storia del suo travagliato rapporto col progresso tecnologico.

Questa considerazione si basa sul fatto che, a differenza di altri istituti giuridici, il diritto alla *privacy* vanta una varietà di concezioni differenti, che legislatori e commentatori di periodi storici diversi hanno avanzato al fine di conciliare le istanze di tutela della personalità degli individui con l'inesorabile innovazione tecnologica.

In questo senso, la *privacy* ha dovuto fare i conti con diversi "riposizionamenti tecnologici" che ne hanno cambiato il significato e la portata.

In questo senso tre sono i fatti tecnologici che hanno segnato un mutamento di paradigma nel diritto alla *privacy*:

1. la diffusione delle prime macchine fotografiche,
2. l'impiego di *databases* per l'accumulo di dati personali,
3. il successo del web 2.0 **la rete del *world wide web (www)***, cui si collega, in tempi più recenti, la raccolta di quantità smisurate di dati (*Big Data*) da parte di compagnie private che operano nel settore delle comunicazioni *online*.

Il celebre articolo "*The Right to Privacy*" degli avvocati bostoniani Samuel Warren e Louis Brandeis, pubblicato nel 1890 *sull'Harvard Law Review*, è considerato all'unanimità l'atto di fondazione teorica del moderno diritto alla *privacy*.

In principio, dunque, il diritto alla *privacy* si configura come diritto a essere lasciati indisturbati (*right to be let alone*), secondo "il criterio del recinto proprietario".

Secondo i due avvocati statunitensi l'estensione della logica dello *jus excludendi alios* risiede nei cambiamenti politici, economici e sociali, per i quali le minacce di intrusione non concernono:

a) solo la sfera proprietaria delle cose corporali,

b) bensì coinvolgono anche altri beni, quale la riservatezza del singolo, ritenuti egualmente meritevoli di tutela a fronte di novità tecnologiche che coinvolgevano più intensamente la vita dei consociati.

Il processo di acquisizione e trattamento dei dati diviene «*invisibile, perché immanente alle azioni quotidiane e attuato in forma continuativa, discreta e disponibile in tempo reale*».

5.5.a) Il modello statunitense e quello europeo

Il diritto alla *privacy* negli **Stati Uniti** ha conosciuto uno sviluppo assai complesso, che è il frutto delle interazioni di giurisprudenza, dottrina e dato legislativo.

Si possono individuare talune linee-guida di evoluzione della materia.

Occorre distinguere, infatti, fra:

a) il diritto di origine giurisprudenziale (*case law*) e

b) il diritto positivo degli *statutes*, cioè delle leggi che regolano il diritto alla *privacy* a livello federale e statale.

Il primo osservabile è il *judge-made law* (principio dello *stare decisis*).

All'interno di esso, si trova, da una parte, l'operato dei giudici dei singoli Stati Federati, che accordano una tutela basata sul *tort law*, e, dall'altra, quello della Corte Suprema Federale.

Anzitutto, in seguito alla teorizzazione di Warren e Brandeis, la *privacy* si è sviluppata all'interno del *tort law*, che, mutatis mutandis, corrisponde approssimativamente alla categoria giuridica degli illeciti civili del civil law (per esempio gli artt. 2043 e ss. del codice civile italiano).

a) In **ambito europeo** il legislatore ha configurato la *privacy* come diritto fondamentale cioè come diritto della personalità;

b) negli **Stati Uniti**, **invece**, la tutela di tale situazione giuridica si è configurata essenzialmente come una propaggine dei diritti del consumatore e, quindi, come diritto disponibile, che può essere

trasferito secondo la volontà ed il consenso dell'interessato nei limiti degli accordi col titolare del trattamento.

Come abbiamo visto la tutela dei dati personali **nella U.E.** è disciplinata dal **Regolamento UE 2016/679 - il c.d. Regolamento Generale sulla Protezione dei Dati, General Data Protection Regulation, o GDPR**, che sostituisce la precedente Direttiva 1995/46/CE.

La Carta dei diritti fondamentali dell'Unione Europea include, fra le libertà fondamentali, la tutela dei dati degli interessati, annoverandone alcuni contenuti:

1. il principio di lealtà,
2. il principio finalistico,
3. quello consensualistico,
4. il diritto di accesso e di rettifica dei dati da parte della persona interessata (art. 8 par. II).

Si tenga presente che con la sentenza *Schrems* II la Corte di Giustizia dell'U.E. il 16 luglio 2020 ha dichiarato che l'accordo tra U.E. ed U.S.A. sulla garanzia dei dati personali trasferiti dalla UE in U.S.A. – il *Privacy shield* del 2016 – non assicurando un adeguato sistema di tutela delle informazioni pari a quello richiesto dal GDPR è stato considerato non più applicabile ed il trasferimento dei dati dei cittadini europei verso gli U.S.A. va bloccato.

La fattispecie riguardava la gestione di dati che la sede europea di Facebook in Irlanda inviava, senza tutte le tutele che il GDPR offre al cittadino europeo e per tal motivo gli è stato inibita questa attività nei confronti di un cittadino austriaco.

5.5.b) U.S.A.

Nell'ordinamento nordamericano prevale un sistema di governance della *privacy* che si differenzia *dall'hard government* affidato all'operato legislativo delle istituzioni pubbliche.

Questa tendenza è indice di «*an intense worry about the risks of state coercion and bumbling, combined with relative insensitivity to the ramifications of private power*».

I mezzi di auto-regolamentazione si basano sui ***Fair Information Practices Principles*** (FIPPs, o semplicemente *Fair Information Practices*, FIPs), cioè **cataloghi di pratiche commerciali e linee-**

guida di "informazione leale" che regolano il controllo e la gestione delle informazioni personali agli interessati.

Occorre prendere in esame i contenuti dei principi di **informazione leale** alla luce dei recenti sviluppi tecnologici.

I FIPs - *Fair Information Practices* - si basano sul **principio dell'"informativa e consenso",** per il quale il trattamento dei dati personali è legittimo se la persona interessata, informata delle ragioni e delle condizioni del trattamento, concede il proprio consenso al titolare del trattamento.

Pertanto, gli interessati sono muniti di un certo grado di controllo sui propri dati, «*and through this control people for themselves can decide how to weigh the costs and benefits of the collection, use, or disclosure of their information*».

I titolari del trattamento sono tenuti a fornire i termini del trattamento dei dati (*privacy policies*) e, solitamente, meccanismi di ***opting out***, cioè di esclusione dal trattamento di talune tipologie di dati personali.

Tuttavia, il **principio dell'"informativa e consenso**" mostra tutti i suoi limiti nella società dei *Big Data* per due ordini di motivi:

1) gli uni di natura conoscitiva,
2) gli altri di carattere strutturale.

Anzitutto, di solito gli interessati non forniscono il consenso sulla base di scelte informate.

a) Spesso gli utenti non leggono le lunghe *privacy policies*, oppure, se provano a leggerle, non ne hanno una comprensione adeguata.
b) Se consapevoli dei meccanismi di *opting out*, in pochi casi optano per tale possibilità.

Si tenga presente che i FIPPs hanno **ispirato la legislazione europea** in materia di protezione dei dati, cioè la Direttiva 95/46/CE ed ora **il Regolamento UE 2016/679 – GDPR** che l'ha sostituita**.**

5.5.c) Unione Europea

L'accesso ai dati personali nel Regolamento U.E. 2016/679 - GDPR

Come abbiamo visto a differenza degli Stati Uniti, **l'Unione Europea** si è dotata di un **sistema di tutela generale in materia di *privacy* informazionale.**

N.B. La protezione giuridica dei dati personali si estende a **ogni ambito di sfruttamento, sia commerciale sia non commerciale**, e si articola in ogni fase del ciclo di vita dei dati, dalla produzione, alla raccolta e al trattamento degli stessi.

Interventi normativi settoriali non mancano nell'Unione Europea, ma operano come «*backup used to increase the specificity of regulatory norms stemming from the initial statutory framework*».

La minuziosa disciplina europea **RAPPRESENTA UN UNICUM A LIVELLO MONDIALE** cui si sono ispirati alcuni legislatori di altre parti del mondo.

5.6) I limiti al trattamento dei dati personali

Gli artt. 5 e 6 del Regolamento disciplinano i principi del trattamento dei dati personali includendo quelli **dell'integrità** e della **riservatezza** ed estendendo le condizioni di liceità del trattamento.

CAPO II Principi

Articolo 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono:

*a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);*

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente

*all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);*

*c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);*

*d) esatti e, se necessario, aggiornati; devono essere adottate tutte **le misure ragionevoli** per cancellare o rettificare **tempestivamente** i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);*

*e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);*

*f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).*

*2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).*

Articolo 6 - Liceità del trattamento

*1. **Il trattamento è lecito solo se** e nella misura in cui **ricorre almeno una delle seguenti condizioni**:*

*a) l'interessato ha **espresso** il **consenso** al trattamento dei propri dati personali per una o più **specifiche** finalità;*

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, ***il titolare del trattamento tiene conto, tra l'altro:***

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Fra questi principi che pongono limiti alle attività di trattamento dei dati personali si annoverano:

1. **Il principio della minimizzazione**, che prevede che i dati personali siano «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»,
2. **il principio della limitazione della finalità**, per il quale «*i dati personali sono […] raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*»,
3. **il principio di liceità del trattamento**, stabilito dall'art. 6 par. I del Regolamento.
4. Riguardo al **principio del consenso**, e, in particolare, ai problemi inerenti al meccanismo dell'"informativa e consenso" si è già parlato in precedenza al paragrafo 5.5.b.

5.6.a) Il principio di minimizzazione

comporta un duplice adempimento del titolare del trattamento *«I dati personali sono […] trattati in maniera da **garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali» (**art. 5 par. I lett. f Regolamento**).*

È necessario circoscrivere la raccolta e il trattamento dei dati allo stretto necessario rispetto alla finalità del trattamento, **e cancellarli** dai sistemi di memoria **una volta che si sono raggiunte tali finalità.**

Il titolare del trattamento, inoltre, non può svolgere il trattamento dei dati secondo finalità diverse da quelle per le quali l'interessato ha prestato il proprio consenso.

È chiaro che un siffatto principio pone seri problemi di legittimità della raccolta e del trattamento dei *Big Data*, giacché risulta radicalmente incompatibile col modello di *business* dei *data brokers*.

Per limitare fenomeni di elusione della disciplina, il legislatore ha disciplinato le **condizioni del consenso** in maniera più particolareggiata (**art. 7 del Regolamento**).

Articolo 7 - Condizioni per il consenso

*1. Qualora il trattamento sia basato sul consenso, **il titolare del trattamento** deve essere in grado di dimostrare che **l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.***

*2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, **la richiesta di consenso** **è presentata in modo chiaramente distinguibile dalle altre materie**, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.* PERCHE' NORMA IMPERATIVA

*3. L'interessato ha il diritto di **revocare il proprio consenso** **in qualsiasi momento**. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima*

di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

*4. **Nel valutare se il consenso sia stato liberamente prestato**, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.*

L'Art. 4 n. 1 del Regolamento **definisce il dato personale** come:

*«qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».*

Fuori dalle ipotesi di finalità statistiche, **il Regolamento** consente ai titolari di sottoporre i dati personali a trattamenti che prescindono dalle finalità iniziali, dal consenso dell'interessato e dalle norme previste in atti legislativi dell'Unione o degli Stati membri che limitano gli obblighi e i diritti degli interessati conformemente alle ragioni elencate all'art. 23 par. I del Regolamento.

Articolo 23 - Limitazioni

*1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può **limitare**, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:*

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:

a) le finalità del trattamento o le categorie di trattamento;

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;

e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;

g) i rischi per i diritti e le libertà degli interessati; e

h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

La compatibilità non è in sé stessa, **ma dev'essere verificata dallo stesso titolare del trattamento.**

In tale controllo, si deve tenere conto di una pluralità di elementi, fra cui:

a. il nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b. il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c. la natura dei dati personali;

d. le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e. l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

5.6.b) il diritto alla trasparenza, accesso e rettifica

Il principio di trasparenza, previsto **all'art. 5 del Regolamento** «*impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*»

Si pensi, per esempio, al trattamento svolto per finalità statistiche come disciplinato dall'art. 5 del Regolamento.

Il **diritto di accesso** (art. 15 del Regolamento) e gli **obblighi informativi dei titolari del trattamento** (artt. 13 e 14 del Regolamento) sono corollari del principio di trasparenza.

Articolo 15 - Diritto di accesso dell'interessato

*1. **L'interessato** ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di **ottenere l'accesso ai dati personali e alle seguenti informazioni**:*

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

*d) quando possibile, **il periodo di conservazione dei dati personali** previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;*

*e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento **la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali** che lo riguardano o di **opporsi** al loro trattamento;*

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

*h) l'esistenza di un processo decisionale automatizzato, compresa la **profilazione** di cui all'articolo 22, paragrafi 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.*

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante

mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Articolo 16 - Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la ***rettifica*** ***dei dati personali inesatti*** *che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.*

Articolo 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, ***il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni****:*

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento ***l'accesso*** *ai dati personali e la* ***rettifica*** *o la* ***cancellazione*** *degli stessi o la* ***limitazione*** *del trattamento dei dati personali che lo riguardano o di* ***opporsi al loro trattamento****, oltre al* ***diritto alla portabilità dei dati;***

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di ***proporre reclamo*** *a un'autorità di controllo;*

e) se la comunicazione di dati personali è un ***obbligo legale o contrattuale*** ***oppure un requisito necessario per la conclusione di un contratto****, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;*

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 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.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

*1. Qualora i dati **non** siano stati ottenuti presso l'interessato, **il titolare del trattamento fornisce all'interessato le seguenti informazioni:***

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

e) il diritto di proporre reclamo a un'autorità di controllo;

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 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.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere

riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

5.6.c) Il diritto alla limitazione ed alla cancellazione dei dati

Oltre al diritto di rettifica e di integrazione, l'interessato può richiedere al titolare del trattamento operazioni che conferiscono all'interessato un controllo ancora più intenso dei dati personali.

L'interessato, infatti, non ha un mero diritto di accesso ai dati, ma può pure disporre di questi, **obbligando il titolare a interrompere il trattamento (diritto alla limitazione) o a cancellare i dati personali (diritto alla cancellazione).**

L'interessato ha diritto di chiedere **la limitazione del trattamento** dei dati personali (**art. 18 del Regolamento**), cioè il «contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro».

Articolo 18

Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

*a) l'interessato **contesta** l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;*

*b) il trattamento è **illecito** e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;*

*c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, **l'esercizio o la difesa di un diritto in sede giudiziaria;***

*d) l'interessato si è **opposto** al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.*

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il diritto alla cancellazione, meglio conosciuto come **"diritto all'oblio"** o *right to be forgotten*, è previsto **all'art. 17 del Regolamento**.

Articolo 17

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento ***la cancellazione*** *dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare* ***senza ingiustificato ritardo*** *i dati personali, se sussiste uno dei motivi seguenti:*

a) i dati personali ***non sono più necessari*** *rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*

*b****) l'interessato revoca il consenso*** *su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;*

c) l'interessato ***si oppone*** *al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;*

d) i dati personali sono stati ***trattati illecitamente****;*

e) i dati personali devono essere cancellati per adempiere ***un obbligo giuridico*** *previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;*

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a ***cancellarli****, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.*

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla ***libertà di espressione e di informazione****;*

b) per l'adempimento di ***un obbligo giuridico*** *che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*

c) per motivi di ***interesse pubblico*** *nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;*

d) a fini di ***archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*** *conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o*

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Nell'esigenza individuale di **limitare la diffusione dei dati personali** stanno le radici del **diritto alla cancellazione**: **l'oblio digitale** consente agli interessati di tutelare l'auto-determinazione informazionale, della quale i dati personali, alla stregua di "tracce del passato", sono un'importante componente.

Se il trattamento dei dati personali continua nonostante l'esercizio di tale diritto, l'attività del titolare del trattamento diviene **illecita**: non a caso, le dette ipotesi in cui l'interessato può esercitare **il diritto all'oblio** riflettono tutte le situazioni di illiceità del trattamento previste dal **Regolamento**.

5.6.d) Il Diritto alla portabilità dei dati

Il legislatore ha previsto un ulteriore limite alle attività di (ri)uso dei dati personali: **l'interessato ha il diritto di trasferire e ottenere i propri dati in formato digitale.**

Tale situazione giuridica è stata denominata **diritto alla portabilità dei dati personali**, ed è prevista **all'art. 20 del Regolamento U.E. 2016/679.**

Articolo 20

Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ***ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:***

a) il trattamento si basa sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

*b****) il trattamento sia effettuato con mezzi automatizzati****.*

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

La ratio della norma sta nel **rafforzamento del controllo dell'interessato sui propri dati personali.**

Il legislatore, inoltre, ha specificato che il diritto alla portabilità non pregiudica il diritto alla cancellazione.

6) La disciplina dell'accesso ai dati personali nella U.E.

Il **diritto dell'U.E.** si basa sulla tutela della protezione dei dati come diritto fondamentale, per il quale l'informazione personale trova tutela in ogni stadio del suo ciclo di vita.

Nell'Unione europea, le autorità di controllo istituite ai sensi **dell'art. 51 del Regolamento U.E. 2016/679** hanno il potere di ingiungere al titolare del trattamento di interrompere il trattamento illecito e conformare i trattamenti alle disposizioni del Regolamento in una determinata maniera ed entro un dato termine;

Articolo 51 - Autorità di controllo

*1. **Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di controllare l'applicazione del presente regolamento** al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione («autorità di controllo»).*

2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.

3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.

4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

Articolo 82 - Diritto al risarcimento e responsabilità

1. ***Chiunque*** **(NON SOLO L'INTERESSATO)** *subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di* ***ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.***

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

5.8) La cosiddetta *group privacy*: ad esempio, società, associazioni, enti pubblici anche se il dato letterale della norma sembra escluderlo

Per lungo tempo, **il diritto alla privacy** è stato concepito come **posizione giuridica esclusivamente individuale.**

In questo senso, anche il testo del **Regolamento U.E. 2016/679** chiarisce che lo stesso «*stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati»* e che «*protegge i diritti e le libertà fondamentali delle persone fisiche*».

Ciò non significa, tuttavia, che l'esigenza di trasparenza del trattamento dei dati, al pari dell'esigenza di riservatezza, non possa coinvolgere anche soggetti collettivi, intesi sia come enti, sia come insiemi di persone fisiche accomunate da un'identità culturale o da convinzioni e interessi comuni, prive di un'indipendenza formale riconosciuta sul piano giuridico: com'è stato fatto opportunamente notare, nessun principio giuridico preclude all'estensione della nozione di "soggetto interessato".

Il Regolamento U.E. 2016/679 va in questa direzione, innovando notevolmente il quadro legislativo precedente e dando la possibilità agli interessati di agire in giudizio collettivamente (CLASS ACTION).

Il par. I dell'art. 80, infatti, stabilisce che "*l'interessato ha il diritto di dare mandato a un **organismo, un'organizzazione o un'associazione senza scopo di lucro**, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di **proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79*** [diritto di proporre reclamo, diritto al ricorso giurisdizionale nei confronti dell'autorità di controllo e nei confronti del titolare del trattamento e del responsabile del trattamento] *nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82"*.

Il par. II aggiunge che "*gli Stati membri possono prevedere che l'organismo, organizzazione o associazione non-profit di cui al par. I, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare il diritto di proporre reclamo o ricorso giurisdizionale nei confronti dell'autorità di controllo, qualora ritenga che i diritti di cui un interessato gode a norma del Regolamento siano stati violati in seguito al trattamento.*"

N.B. Il legislatore europeo ha adottato misure che rispondono a esigenze di tutela della rappresentanza delle persone interessate mediata dall'operato di tali organizzazioni, ma, a differenza della giurisprudenza statunitense, **non** ha stabilito norme a tutela della *privacy* informazionale di enti collettivi in quanto tali.

La formulazione **dell'art. 80 del Regolamento** è in linea con la visione individualistica cui si ispira l'intera disciplina della tutela della protezione dei dati personali: **sia il par. I sia il par. II del presente articolo** fanno riferimento alla posizione di un singolo interessato, la cui tutela in sede giudiziaria è affidata a un'organizzazione atta a far valere il suo diritto individuale.

Tentando di sintetizzare, **nel Regolamento U.E. 2016/679** si registra una duplice tendenza:

1) da un lato, i soggetti del diritto alla protezione dei dati personali in senso stretto sono le **persone fisiche**;

2) dall'altro, le persone fisiche possono essere **rappresentate in giudizio da organizzazioni senza scopo di lucro**, ai sensi **dell'art. 80 del Regolamento U.E. 2016/679**.

La portata **dell'art. 33 del Regolamento U.E. 2016/679** si addice meglio alle problematiche in questione.

Il par. I prevede che il titolare del trattamento debba effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali «*quando un tipo di trattamento, **allorché prevede in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle **persone fisiche***».

Tale forma di verifica dell'impatto è richiesta, in particolare, per i casi previsti dal **par. III del detto articolo 80**, fra cui rientra «*la 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***».

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà ***delle persone fisiche****. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

5.9) Gli algoritmi utilizzati per elaborare i dati

La parola algoritmo deriva dal nome di "al-Khwarizmi", importante matematico arabo del nono secolo d. C.

Al-Khwarizmi è famoso per averci insegnati i cosiddetti numeri arabi: la sua opera "(Libro) di al-Khwarizmi sui numeri indiani" fu tradotta in latino come "*Algorismi de numero Indorum*". Fu su questo libro che l'Europa intera imparò ad usare il sistema di notazione decimale posizionale.

Le procedure che permettevano di effettuare calcoli in notazione decimale divennero così note come "Algorismi" o "Algoritmi" e più tardi lo stesso termine fu applicato in generale alle procedure di calcolo necessarie per ottenere un determinato risultato.

L'area della **soggettività giuridica** si è accresciuta con l'evolversi dell'informatica in quanto sulla scena è apparso l'agente elettronico (*software, e persons, computer, robot*) capace di elaborare decisioni algoritmiche autonome e di conseguenza agire nella realtà giuridica.

Ovviamente se tale soggettività giuridica non rientra tra le persone fisiche potrà rientrare solo tra le persone giuridiche o tra altre entità.

Il problema giuridico emerge in quanto tali elaborazioni complesse portano ad individuare il concetto di **intelligenza artificiale** che però spesso nel suo operare concreto si distacca dal controllo umano compresi i suoi creatori.

Da ciò la DOMANDA: in caso di violazione di legge chi ne risponde?

A) C'è chi sostiene che si potrebbe parlare di persona giuridica elettronica affermando che i robot e gli strumenti elettronici di per sé sarebbe i responsabili.

Si veda anche la **Risoluzione del Parlamento Europeo del 16 febbraio 2017** con la quale il Parlamento ha invitato la Commissione a formulare una proposta di direttiva che individui norme civilistiche idonee a regolare in modo coerente ed uniforme, su tutto il territorio dell'U.E., gli aspetti e le problematiche connesse all'impiego della robotica e delle intelligenze artificiali – *Artificial Intelligence*.

PROBLEMA: con quale patrimonio si risarcirebbe il danno poiché il *robot* è di per sé privo di un patrimonio?

PROBLEMA:

1) come si definirebbero i criteri soggettivi di dolo e colpa applicati ad un *robot*?

2) Se si facesse riferimento ad una responsabilità oggettiva porsi il problema della soggettività del *robot* sarebbe inutile.

B) Altri sostengono che i responsabili siano chi li utilizza e ne trae beneficio (*accountability*)

C) **Si tenga presente che esiste anche una terza ipotesi più articolata** in quanto normalmente i *software* sono creati dai programmatori, semmai in *equipe,* i quali però spesso seguono le

direttive di un *management* aziendale oppure addirittura, per ragioni tecniche, danno risultati solo probabilistici che poi verranno successivamente elaborati a loro volta.

Se le **fonti dei *Big Data*** raccolgono dati scorretti che vengono passati all'elaborazione:

- Su chi grava la responsabilità civilistica se si creano danni o comunque violazioni di norme se i computer sono in rete?
- E se il meccanismo della rete è collocato all'interno di una procedura di ***Blockchain***?

(in dottrina si parla anche di responsabilità suddivisa *pro quota*)

- I *software* possono essere considerati dei rappresentanti degli esseri umani che li hanno creati o che li utilizzano, se questi compiono attività giuridiche?
- Si può ritenere di introdurre il concetto di uomo – macchina come di un nuovo soggetto giuridico "misto"?

Alcuni Autori parlano di "Ente di fatto digitale".

Si attua una comunicazione giuridica diretta all'esterno quindi determinando conseguenze rilevanti per il diritto.

Da ciò deriva che è importante comprendere come i soggetti che si relazionano con il *software* e la macchina percepiscono tale relazione. **Teoria dell'Affidamento** (artt. 1389 e 1390 c.c.) prevalente rispetto a quella della colpa.

Se **il programmatore delega all'algoritmo la scelta** se prendere una decisione od un'altra in caso di responsabilità derivante dalla scelta operata essa dovrà essere imputata:

A) all'algoritmo che ha materialmente operato la scelta oppure

B) al programmatore che non ha scelto ed ha delegato alla macchina/algoritmo? (*machine learning* – algoritmi *black box*)

Nel caso di uno *Smart contract*:

- dove una persona fisica o giuridica – creditore - delega l'esecuzione del contratto?
- su chi ricade l'eventuale responsabilità legale?

Si può considerare il *software* e l'algoritmo su cui si basa come un ausiliare/commesso (art. 2049 c.c.) dell'utilizzatore del *software*/creditore?

Non risulta semplice accertare il momento della causalità e della colpevolezza.

Si potrebbe ipotizzare che il binomio uomo/macchina sia un tutt'uno dove le responsabilità sia contrattuali che extracontrattuali potranno essere imputate, a seconda delle prove, solo all'uomo, solo alla macchina (che acquisterebbe una "personalità informatica") od ad entrambi uomo e macchina.

Alcuni autori sostengono che si potrebbe pensare ad un'attività d'impresa societaria ex art. 2247 c.c. il cui conferimento è un fare/svolgimento di servizi.

Si tenga presente che le problematiche uomo/macchina dovranno essere affrontate in futuro in **un'ottica processuale** e di emissione di una **sentenza**.

I *software* sono algoritmi ossia flussi di informazioni rappresentate in linguaggio matematico.

Gli algoritmi comportano normalmente un **problema di mancanza di trasparenza**, cioè di **OPACITÀ** (*opacity*), su cui occorre soffermarsi ulteriormente.

L'opacità degli algoritmi è riconducibile a tre ordini di problemi:

1. l'inaccessibilità,

2. l'incomprensibilità tecnico-formale e

3. l'incomprensibilità sostanziale.

In primo luogo, gli algoritmi sono coperti da meccanismi di tutela proprietaria (**per esempio**, il segreto industriale) che limitano l'accessibilità alle informazioni sul loro funzionamento.

Tale opacità "volontaria" comporta un primo **ostacolo** alla conoscenza del processo decisionale condotto mediante l'algoritmo, poiché, per esempio, **secondo il Regolamento U.E. 2016/679**, il diritto di accesso previsto **dall'art. 15** «*non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale*» **e quindi la titolarità dell'algoritmo.**

In secondo luogo, se anche tali informazioni fossero accessibili, solo un numero ristretto di individui, dotati di determinate qualifiche tecnico-professionali (**per esempio**, gli ingegneri informatici e i programmatori), sarebbe in grado di leggere e capire il linguaggio dei codici sorgente e gli schemi matematici che compongono gli algoritmi e ne determinano il funzionamento.

Si pone, quindi, un **problema** di comprensibilità del funzionamento degli algoritmi per la maggior parte delle persone.

In terzo luogo, l'incomprensibilità sostanziale concerne il funzionamento degli algoritmi più complessi, che hanno la capacità di modificare e correggere i procedimenti di calcolo sulla base dei *datasets* forniti (*machine learning*). «*The internal decision logic of the algorithm is altered as it 'learns' on training data. Handling a huge number especially of heterogeneous properties of data […] adds complexity to the code*».

Ne consegue che i risultati (*output*) dei procedimenti di analisi mediante algoritmi di questo genere sono imprevedibili e ignoti agli agenti umani.

Perciò, anche se le informazioni sul funzionamento dell'algoritmo sono accessibili, rimane il problema di capirne le modalità decisionali.

DOMANDA: quale è l'approccio dell'Unione Europea e quale il dibattito intorno al "diritto alla spiegazione" in tema di algoritmi?

Come visto in precedenza **il Regolamento U.E. 2016/679 – GDPR -** prevede:

1. precisi obblighi in capo ai titolari del trattamento e, simmetricamente,
2. una serie di diritti dell'interessato al trattamento dei propri dati.

Fra i diritti dell'interessato, taluni autori hanno riconosciuto la previsione di un **"diritto alla spiegazione"** (*right to explanation*) del funzionamento del processo decisionale automatizzato, con il quale il legislatore europeo intende fronteggiare l'opacità degli algoritmi.

Le possibili fonti di **diritto alla spiegazione in tema di algoritmi** si trovano:

1. nelle "misure di salvaguardia" previste al par. all'art. 22,

par. I dell'art. 22 del Regolamento U.E. 2016/679:

1. 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.

A questa regola derogano le **eccezioni** previste al paragrafo seguente, che operano come **"clausole di disinnesco" della norma in questione.**

2. negli obblighi di informazione stabiliti dagli artt. 13 e 14;
3. nel diritto di accesso ai sensi dell'art. 15.

Gli artt. 13 e 14 del Regolamento U.E. 2016/679 impongono obblighi informativi in capo al **titolare del trattamento**.

Fra gli altri, **il titolare del trattamento** deve comunicare all'interessato «*l'esistenza di un processo decisionale automatizzato,* ***compresa la profilazione*** *[…], e, almeno in tali casi, informazioni*

significative sulla logica utilizzata anche dagli algoritmi, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato».

Questa spiegazione si colloca **prima del processo decisionale**, nel momento in cui i dati sono raccolti per essere sottoposti al trattamento, e **riguarda il funzionamento del sistema algoritmico**.

Si pongono **problemi** rispetto alla **qualità delle informazioni** cui l'interessato accede: la diffusione dei codici sorgente e le descrizioni tecniche dettagliate **non soddisfano** le esigenze di trasparenza dell'interessato, a meno che costui non sia un soggetto qualificato a livello professionale.

Un **diritto alla spiegazione** si può desumere dal **diritto di accesso** previsto **all'art. 15 del Regolamento U.E. 2016/679.**

L'esercizio del diritto di accesso, a differenza degli obblighi previsti dagli artt. 13 e 14, implica un'istanza dell'interessato al titolare del trattamento che non è soggetta a termini di decadenza.

Stando a questa ricostruzione, **all'interessato potrebbe essere garantito** un **diritto alla spiegazione ex ante ed ex post,** a seconda del momento in cui è formulata la richiesta.

Par. II dell'art. 22 del Regolamento U.E. 2016/679, "*la norma del par. I **non** si applica nel caso in cui la decisione:*

*a) **sia necessaria per** la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*

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".

Per evitare **che il par. I** sia eluso nella prassi ricorrendo al consenso dell'interessato, il legislatore europeo ha stabilito che, nelle sole ipotesi sub a) e c), **il titolare del trattamento** debba attuare «*misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*».

Per ovviare ad entrambi i problemi, alcuni autori hanno proposto l'istituzione di meccanismi di verifica (*auditing*) da parte di autorità indipendenti (*trusted auditors*) che, pur mantenendo il segreto

industriale nell'interesse degli utilizzatori, agiscono per il pubblico interesse, spiegando il funzionamento dell'algoritmo in termini comprensibili anche a soggetti non dotati di competenze tecnico-professionali.

5.10) La "proprietarizzazione" dei dati personali nel Regolamento U.E. 2016/679

Nella U.E. non si arriva a riconoscere un vero e proprio regime proprietario sulle informazioni personali.

Tuttavia, nell'economia dell'informazione si riscontra la marcata tendenza, in ambiti commerciali, di considerare le informazioni personali alla stregua di **beni alienabili dotati di valore economico**.

Tali proposte non sono state esenti da critiche da una parte della dottrina che hanno ritenuto che lo schema di **tutela proprietaria applicato alla *privacy* informazionale** e lo sdoganamento degli scambi commerciali dei dati, compromettano i diritti delle persone interessate.

Occorre quindi capire se nell'**Ordinamento Europeo**, in cui non è previsto un regime proprietario dei dati personali, sono presenti almeno i germi di diritti dominicali in capo ai diversi attori.

Per una comparazione si tenga presente che in **U.S.A.** alcuni **autori** hanno teorizzato un **diritto di proprietà dei dati personali**.

5.11) Paragone con il diritto d'autore ed il diritto di licenza

Nella tradizione europea la protezione dei dati personali detiene il rango di diritto fondamentale: la sua formulazione trova spazio nella Carta dei diritti fondamentali dell'Unione Europea (art. 8) accanto al rispetto della vita privata e familiare (art. 7) e nel Trattato sul Funzionamento dell'Unione Europea (art. 16 TFUE).

Sul versante europeo, veri e propri diritti di proprietà sui dati personali sono difficilmente configurabili, dal momento che «*it is [not] possible to avoid human rights issues when discussing data protection matters.*

This conclusion is especially relevant when the data protection rights come into conflict with other interests, such as freedom of contract or free alienability of personal data for economic gain».

Ciononostante, in seno al recente dibattito sulle questioni di appartenenza dei dati (*data ownership*), taluni autori hanno intravisto in alcune regole del **Regolamento U.E. 2016/679** i germi di una tutela di matrice proprietaria, benché il legislatore europeo non abbia adottato la terminologia tipica del diritto di proprietà.

In particolare, questa tendenza si riscontra in tre punti particolari della disciplina.

1) **il par. I dell'art. 6 del Regolamento** prevede che il trattamento è lecito se l'interessato ha fornito il proprio consenso e in una serie di altre ipotesi.

Questo significa che il titolare dell'*entitlement* è, di norma, la persona interessata.

In particolare, l'interessato non può cedere il proprio diritto sui dati personali.

In base a questo assunto, quindi, la disciplina europea prevede una rigida regola-base di inalienabilità (*inalienabilities*), per la quale l'*entitlement* non può essere trasferito nemmeno se sussiste il consenso dell'alienante (l'interessato) e dell'acquirente (titolare del trattamento).

L'interessato assume la medesima posizione dell'autore di un'opera in cui il contenuto del diritto d'autore ha un duplice contenuto:

a) oltre ai diritti economici,

b) sono previsti i c.d. diritti morali (o personali).

Tali situazioni giuridiche soggettive sono irrinunciabili e intrasmissibili, e proteggono l'opera in quanto emanazione della personalità dell'autore.

La posizione forte della persona interessata è avvalorata dalla previsione del Diritto di Limitazione ex **art. 18 del Regolamento** e del Diritto alla Cancellazione, previsto all'**art. 17 del Regolamento**.

Infatti, se il trattamento diviene illecito per il venir meno di una delle condizioni previste dal **par. I dell'art. 6 del Regolamento**, l'interessato ha diritto di chiedere che i dati non siano più oggetto del trattamento o che siano cancellati.

Questo sistema di tutela assomiglia ad un Regime di Licenze, per il quale «*a data user may essentially receive a "license" to use the subject's data, since the data subject has temporarily waived her right to exclude it from using her information*».

Al contempo, però, l'interessato mantiene la Titolarità del Diritto sui Propri Dati Personali.

Tuttavia, l'interessato può cedere talune prerogative al titolare del trattamento.

L'interessato può consentire che i dati personali siano raccolti e sottoposti al trattamento alle condizioni previste al **par. I dell'art. 6 del Regolamento**.

In particolare, le attività del titolare del trattamento sono legittime se **l'interessato consente al trattamento o in altre ipotesi** e fra queste, **il legislatore europeo** ha previsto che il trattamento è legittimo se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

La formulazione di questa norma ricalca il principio espresso dal par. I dell'art. 17 della Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE) in materia di **limiti del diritto di proprietà**, per il quale «*nessuna persona può essere privata della proprietà se non per causa di pubblico interesse, nei casi e nei modi previsti dalla legge*».

2) In secondo luogo, il **diritto di protezione dei dati** si configura **come** un **diritto assoluto**, nel senso che crea **obblighi erga omnes** in capo al titolare del trattamento e ai terzi.

Si consideri di nuovo il Diritto alla Cancellazione.

Secondo il **par. II dell'art. 17 del Regolamento il titolare del trattamento** che ha reso pubblici i dati personali ed è obbligato a **cancellarli**, tenendo conto della tecnologia disponibile e dei costi di attuazione e deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di **cancellare** qualsiasi link, copia o riproduzione dei suoi dati personali.

Tale aspetto della disciplina risponde chiaramente a **logiche proprietarie**, giacché «*it creates a burden that "runs with" the data subject's information. Rather than conceiving of privacy protection as purely in personam, the […] Regulation instead grounds these rights in the data itself*».

3) Infine, taluni rimedi previsti nel **Regolamento U.E. 2016/679** sono chiaramente ispirati a ***property rules***, per cui l'interessato ha una tutela forte nei confronti di tutti i consociati.

Questa protezione giuridica consiste in **provvedimenti di inibitoria** delle attività di trattamento che violano il **Regolamento** e in sanzioni punitive dell'autorità.

Secondo il dettato legislativo, le Autorità Nazionali di Controllo previste **dall'art. 51 del Regolamento** hanno poteri "correttivi", cioè possono:

Articolo 51 - Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di controllare l'applicazione del presente regolamento al fine di ***tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione («Autorità di controllo»)****:*

1) ***ingiungere*** *al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del Regolamento;*

2) ***imporre*** *una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;*

3) ***ordinare*** *la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;*

4) ***infliggere*** *una sanzione amministrativa pecuniaria ai sensi dell'art. 83.*

Articolo 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se ***infliggere una sanzione amministrativa pecuniaria*** *e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:*

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

5.12) I limiti giuridici all'accesso ai dati non personali: proprietà e regolamentazione

Anzitutto, è necessario distinguere preliminarmente due situazioni qualitativamente diverse cui l'espressione "**dati non personali**" si riferisce.

In primo luogo, vi sono **i cc.dd. "beni digitali",** quali files musicali, ebook, documenti di testo ecc.

Sui **beni digitali**, esiste una **tutela giuridica del diritto d'autore**, e **il legislatore europeo** ha preso in considerazione l'introduzione di nuove norme in materia di diritto dei contratti concernenti tali beni.

In secondo luogo, nella nozione rientrano anche i grandi *datasets* raccolti, analizzati e (ri)utilizzati dai soggetti economici, che comprendono quantità incalcolabili di dati non personali prodotti da dispositivi (***machine-generated data***), «*created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real*».

Occorre poi tener presente che **il livello di protezione dei dati è strettamente connesso alla distinzione di tre piani della nozione di informazione**:

1) **il piano semantico**, cioè quello del significato (**per esempio**, alla successione di note e alla progressione armonica di un brano musicale; **per esempio**, la protezione dei dati personali, il segreto commerciale e il brevetto);

2) **il piano sintattico**, cioè quello dei *bits*, dei segni e dei codici, rappresentati nel sistema numerico binario (ad **esempio**, il file mp3 dello stesso brano musicale) cioè i dati nel loro formato digitale;

3) **il piano fisico-strutturale**, inerente all'infrastruttura, al supporto o al dispositivo che contiene i dati o, in senso più ampio, ai dati rappresentati dalla struttura di una cosa materiale (per **esempio**, il CD o la penna USB in cui è immagazzinata la traccia musicale; il diritto di proprietà sul supporto contenente le informazioni, quale un CD di un album musicale).

I dati trovano diverse modalità di protezione giuridica per ciascuno di questi livelli.

5.12.a) Alle radici di un dibattito essenzialmente europeo.

I beni digitali: dal diritto dei contratti alla proprietà normativa a tutela dei consumatori

Come sempre si è fatto nello sviluppo di questa Guida partiamo dal dato normativa ed in particolare dalla **Direttiva (UE) 2019/770 del Parlamento Europeo e del Consiglio del 20 maggio 2019** relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

Le autorità europee hanno dimostrato un notevole interesse verso una tutela giuridica più adeguata dei beni digitali in taluni interventi concernenti il diritto dei contratti dei **consumatori** all'inizio del secondo decennio del Duemila.

Con la **Direttiva U.E. 2019/770**, il legislatore europeo ha conferito un minimum di armonizzazione alle normative interne degli Stati membri riguardanti i **diritti dei consumatori**, stabilendo «*norme standard per gli aspetti comuni dei contratti a distanza e dei* ***contratti negoziati fuori dei locali commerciali***».

Nel testo normativo, una disciplina speciale riguarda i contratti di fornitura di "contenuto digitale".

Il dettato legislativo configura tali contratti come un *tertium genus* rispetto al contratto di vendita e al contratto di servizi, e prevede norme specifiche in materia di obblighi di informazione pre-contrattuale e di diritto di recesso.

In base alla **Direttiva**, il diritto esclusivo dell'autore di distribuire gli esemplari di un'opera incontra un limite nel c.d. **principio dell'esaurimento** (*exhaustion doctrine*, meglio conosciuta negli Stati Uniti come *first-sale doctrine*), per il quale il titolare del diritto **non può impedire la rivendita delle copie dell'opera messe in commercio** col suo consenso dopo che ha proceduto alla prima vendita o al primo trasferimento della proprietà di tali esemplari all'interno del territorio europeo.

In altri termini, l'acquirente della prima copia, divenuto proprietario di quest'ultima, non ha bisogno dell'autorizzazione dell'autore per alienarla in un secondo momento.

Tale principio è il frutto della coordinazione della tutela del diritto d'autore col principio di libera circolazione delle merci, considerato prevalente in questo caso.

I giudici europei, applicando il principio dell'equivalenza *offline-online*, hanno esteso la dottrina dell'esaurimento agli ambienti digitali, prevedendo che il principio possa applicarsi anche ai casi di scaricamento (*download*) delle copie digitali di un programma per elaboratore (*software*) da

Internet, se autorizzato dal titolare del diritto, anche a titolo gratuito. (Sentenza *Used Soft* della Corte di Giustizia dell'Unione Europea)

Benché la sentenza si occupi specificamente di programmi per elaboratore, fra gli autori è prevalsa l'opinione che il **principio dell'esaurimento "digitale"** possa ragionevolmente estendersi anche alle copie di altre tipologie di opere creative, quali brani musicali, *ebooks* ecc.

Più controversa è la configurabilità di tale precetto rispetto ai **servizi di fornitura del contenuto dell'opera**:

A) secondo alcuni, attenendosi al testo della **Direttiva**, occorre escludere la fornitura di un servizio *online* dal campo di applicazione della **dottrina dell'esaurimento**;

B) tuttavia, così facendo, si perdono di vista le recenti evoluzioni tecnologiche, e si limita notevolmente la portata del principio in questione a modelli di business che saranno presto surclassati.

Comunque la rivendita di una copia digitale dell'opera creativa comporta talune problematiche.

A differenza di un prodotto su un supporto fisico, **un *file* deve essere copiato per essere ulteriormente ceduto**, ma ciò non comporta la contestuale eliminazione del prodotto dal dispositivo del primo acquirente.

Perciò, la creazione di un'ulteriore **copia** può ledere il diritto esclusivo di riproduzione dell'autore dell'opera.

Tuttavia, negli ambienti digitali, venendo meno la differenza fra l'opera originale e quella riprodotta, la **copia di un *file*** è un elemento tecnologico accessorio e necessario perché il prodotto in questione possa circolare liberamente nel mercato.

Perciò, **nel bilanciamento delle esigenze dell'autore e dei consumatori, il sacrificio delle prime è necessario a garantire il buon funzionamento del mercato.**

Il diritto di proprietà del licenziatario sulla copia digitale si estende ai **dati non personali** che la costituiscono.

La Corte però non si è spinta a riconoscere un generale diritto di proprietà dei dati che possa estendersi a contesti diversi da quello delle opere creative in formato digitale, quali le questioni di appartenenza dei ***Big Data***, su cui ora, però, occorre soffermarsi.

Molti dati sono generati senza il diretto intervento di un operatore umano (*machine-generated data*) mediante i sensori degli oggetti *Smart* interconnessi dell'Internet delle Cose e, dopo essere sottoposti ad analisi, diventano informazioni di valore e sono riusati dalle imprese.

Le imprese scambiano i *datasets* di grandi dimensioni come veri e propri beni commerciabili (*assets* o *commodities*) mediante **strumenti contrattuali**.

Rispetto alle prassi di sfruttamento e controllo dei *datasets*, **i commentatori europei** hanno tentato di capire se i regimi di tutela esistenti forniscano un **qualche forma di protezione agli attori che controllano i *datasets*.**

L'allocazione dei diritti di accesso e di riuso dei *datasets* avviene mediante **strumenti contrattuali (per esempio contratti di licenza, di vendita – si veda l'art. 1470 c.c. che parla di "altri diritti")**, ma le soluzioni normative esistenti nel diritto dei **contratti** non appaiono sufficienti a garantire il buon funzionamento del mercato: «*where the negotiation power of the different market participants is unequal, market-based solutions alone might not be sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations*».

Le imprese che cedono i *datasets* ad altri attori economici di solito inseriscono negli accordi **clausole contrattuali che ostacolano o impediscono il riutilizzo dei dati per scopi diversi da quelli previsti nel contratto.**

5.12.b) I *Big Data* e allocazione giuridica dei "nuovi" beni immateriali

Nella società dell'informazione i ***datasets* di grandi dimensioni** sono considerati **beni commerciabili.**

È necessario soffermarsi maggiormente sulla portata di tale affermazione, approfondendo:

- la nozione di bene,

- le implicazioni in materia di diritti esclusivi.

Secondo una distinzione tradizionale, i beni si dividono in **beni materiali e beni immateriali**.

a) **I beni materiali** comprendono le **risorse tangibili e corporee**, che sono assoggettate in modo pacifico alle regole del diritto di proprietà "fisica" civilistica, lo strumento di tutela giuridica di carattere reale e assoluto per eccellenza.

b) **I beni immateriali**, la cui teorizzazione più risalente si deve al giurista tedesco Josef Kohler (n. 1849 – m. 1919), includono le creazioni intellettuali, quali le invenzioni, i segni distintivi e le opere dell'ingegno.

La protezione giuridica dei beni immateriali consiste nell'istituzione di un monopolio nello sfruttamento del bene che risponde alla tutela dominicale dei beni materiali. Si tratta della tecnica giuridica della **c.d. privativa (o esclusiva**), che, come il diritto di proprietà delle cose materiali, **è un diritto reale e assoluto**.

A seconda del bene che si desidera proteggere, esistono differenti privative:

- **Il Brevetto**: protegge le invenzioni nuove ed originali di un prodotto o di un procedimento atto ad essere applicato in campo industriale. La durata prevista è di 20 anni ed inizia dal momento in cui viene presentata la domanda negli appositi uffici.

- **Il Marchio**: rappresenta una nuova parola, figura o segno atto a distinguere prodotti o merci al fine di identificarli, individuando l'impresa produttrice; la durata è di 10 anni rinnovabile.

- **Il Modello di utilità**: protegge i nuovi modelli atti a conferire caratteri di novità, miglioramenti a macchine o parti di esse. La protezione prevista dalla legge è di 10 anni.

- **Il Modello o disegno**: protegge i nuovi disegni o i modelli che grazie ad una particolare forma, linee, colori o altri elementi permettono di conferire al prodotto stesso un elemento di innovazione. La durata è di 5 anni, rinnovabile per 5 volte.

- **La Topografia di un circuito a semiconduttori**: protegge una serie di disegni che, rappresentano lo schema tridimensionale di cui si compone un circuito a semiconduttori e tale protezione dura 10 anni.

- **Nuova varietà vegetale**: protezione prevista per le nuove scoperte nel campo vegetale. La durata della protezione è di 20 anni, elevata a 30 anni per particolari specie e piante.

• **Il Diritto d'autore: tutela le opere dell'ingegno di carattere creativo, compresi i programmi per elaboratore.** Dopo la morte dell'autore il diritto dura ulteriori 70 anni.

La tendenza alla creazione di nuove entità intangibili (fra cui rientrano i *datasets* di grandi dimensioni – *Big Data*) che generano utilità e soddisfano interessi di natura patrimoniale dei soggetti che vi accedono e ne hanno il controllo non ha ancora trovato un'adeguata risposta in sede parlamentare e istituzionale.

I "nuovi" beni immateriali (o beni immateriali atipici), infatti, sono (ancora) privi di una protezione giuridica espressamente riconosciuta dal legislatore, o «comunque non [sono] riconducibili al catalogo tradizionale dei diritti di privativa».

Al pari di quello dei diritti reali sulle cose materiali, il sistema degli istituti di **proprietà intellettuale** è organizzato secondo il principio del ***numerus clausus***, per il quale, da un lato, i diritti di esclusiva sono figure tipiche, cioè tassativamente predeterminate, e, dall'altro, «gli interessi su entità diverse dalle cose e privi di un riconoscimento normativo (diretto o analogico) godono di una tutela limitata e caratterizzata dall'assenza di esclusività», **non essendo applicabile l'interpretazione analogica o estensiva.**

Tuttavia, a differenza del sistema che governa i diritti reali, il **principio di tipicità** ha una portata più limitata nell'ambito della proprietà intellettuale.

N.B. Nell'ambito della proprietà intellettuale il principio di tipicità si riferisce esclusivamente ai diritti "primari" sulle entità intangibili, e non anche ai diritti "secondari" (o meglio, frazionari) **di sfruttamento economico**, che i consociati trasferiscono mediante lo strumento duttile della **licenza** a prescindere dall'esistenza di un istituto di privativa.

Le considerazioni sollevate sono necessarie a inquadrare le questioni di appartenenza dell'oggetto di trattazione, cioè **i *datasets* costituiti da dati non personali**.

Si cercherà di capire quale sia il grado di protezione accordata dai regimi di tutela esistenti agli **agenti economici** che controllano e gestiscono i *datasets* inclusi i *Big Data*.

In particolare taluni regimi esistenti a livello europeo potrebbero accordare tutela sui *datasets* di grandi dimensioni – *Big Data*.

Essi sono:

a. il diritto d'autore, che potrebbe essere rilevante per la protezione dei singoli dati di *datasets- Big Data*;

b. la tutela giuridica delle banche dati prevista dalla Direttiva 96/9/CE;

c. la tutela giuridica del segreto commerciale, stabilita dalla Direttiva (UE) 2016/943;

d. la tutela brevettuale;

e. la tutela della proprietà privata fisico-civilistica.

5.12.b.1) Il diritto d'autore

La tutela del diritto d'autore potrebbe riguardare i singoli dati costituenti un *dataset - Big Data* se si opera un'estensione oggettiva della nozione di opera dell'ingegno.

Nell'ordinamento interno degli Stati membri dell'U.E. la nozione di opera protetta, pur non univoca, è «*sufficientemente ampia ed elastica da potere tener conto dell'evoluzione della tecnica e delle forme espressive*».

Il diritto d'autore conferirebbe una **tutela** sul piano semantico – linguistico **ai singoli dati**.

1) Tuttavia, **il requisito di originalità dell'opera** limita l'applicazione della protezione autorale alle sole informazioni create da una **mente umana.** Mentre i dati inclusi in un *Big Data* arriverebbero anche da macchine.

2) **I dati** non strutturati (*raw data*) **raccolti mediante processi automatizzati e quelli generati mediante i sensori degli oggetti dell'Internet delle Cose non sono compresi** nella tutela di diritto d'autore.

5.12.b.2) La tutela giuridica delle banche dati: la Direttiva 96/9/CE

La Direttiva 96/9/CE ha introdotto un regime armonizzato di protezione giuridica delle **banche dati** che potrebbe accordare un grado di tutela ai soggetti controllori dei *datasets* - *Big Data*.

Occorre dapprima soffermarsi sulla disciplina prevista nel dettato normativo e, in seguito, configurarne l'applicabilità agli scenari dei ***Big Data*.**

Secondo **la Direttiva 96/9/CE,** una **banca dati (*database*)** è «*una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo*».

Questa formulazione appare notevolmente ampia, accogliendo non solo le raccolte di elementi digitali, ma anche le banche dati non elettroniche.

La Corte di Giustizia dell'Unione europea (CGUE) ha confermato questa impostazione, asserendo che la definizione di banca di dati ai sensi **dell'art. 1, n. 2, della Direttiva 96/9/CE** concerne qualsiasi raccolta di opere, dati o altri elementi, separabili gli uni dagli altri «*senza che venga per questo intaccato il valore del loro contenuto, e che comporti un metodo o un sistema, di qualunque natura esso sia, che consenta di ritrovare ciascuno dei suoi elementi costitutivi*».

Articolo 1 - Campo d'applicazione

*1. La presente direttiva riguarda la tutela giuridica delle **banche dati**, qualunque ne sia la forma.*

*2. Ai fini della presente direttiva per «**banca dati**» si intende una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo.*

*3. La tutela della presente direttiva **non si applica** ai programmi per elaboratori utilizzati per la costituzione o il funzionamento di banche di dati accessibili grazie a mezzi elettronici.*

Articolo 2 - Limitazioni del campo d'applicazione

La presente direttiva si applica fatta salva la normativa comunitaria concernente:

a) la tutela giuridica dei programmi per elaboratore;

b) il diritto di noleggio e di prestito a taluni diritti connessi al diritto d'autore in materia di proprietà intellettuale;

c) la durata di protezione del diritto d'autore e di alcuni diritti connessi.

I giudici degli Stati membri hanno variamente interpretato l'oggetto della tutela giuridica prevista dalla Direttiva.

Per esempio, in Italia, **il Tribunale di Torino**, seguendo la linea adottata dalla Corte Suprema degli Stati Uniti nel famoso caso Feist, **ha negato** la protezione accordata dal diritto d'autore agli elenchi telefonici.

Il dettato normativo prevede un duplice binario di tutela giuridica:

- l'una di diritto d'autore (cap. II della Direttiva 96/9/CE),
- l'altra di diritto sui generis (cap. III della Direttiva 96/9/CE).

Il diritto d'autore riguarda i ***databases*** che «per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore».

Questo è l'unico criterio a stabilire l'assoggettabilità di una banca dati alla tutela del diritto d'autore.

Tali *databases* sono oggetto dell'esclusiva intellettuale «in quanto tali» **ex art. 3**, essendo una species particolare di opera collettiva.

L'aggiunta dell'espressione "in quanto tali" è spiegata meglio nel **par. II dello stesso art. 3 della Direttiva 96/9/CE,** per il quale tale tutela concerne la struttura dei *databases*, ma «*non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto*».

Capitolo II - diritto d'autore

Articolo 3 - Oggetto della tutela

"1. A norma della presente direttiva, ***le banche dati*** *che* ***per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore*** *sono tutelate in quanto tali dal diritto d'autore. Per stabilire se alle banche dati possa essere riconosciuta tale tutela non si applicano altri criteri.*

2. La tutela delle banche dati in base al diritto d'autore prevista dalla presente direttiva ***non*** *si estende al loro contenuto (*cioè ai dati in essa contenuti*) e lascia impregiudicati i diritti esistenti su tale contenuto."*

L'indipendenza della tutela giuridica della struttura dagli elementi che costituiscono la banca dati si riflette sulla valutazione del requisito di originalità della banca dati.

Secondo la CGUE, la scelta e la disposizione del materiale **elaborato nei *databases*** devono costituire «*un'espressione originale della libertà creativa del suo autore*», e tale valutazione non dipende dall'impegno intellettuale e dal know-how destinati alla creazione di detti dati, ma unicamente dagli **sforzi creativi di assemblaggio del database.**

L'autore del *database* è «*la persona fisica o il gruppo di persone fisiche che l'ha creata o, qualora la legislazione dello Stato membro interessato lo consenta, la persona giuridica individuata da tale legislazione come titolare del diritto*»; inoltre, se il *database* è frutto della collaborazione fra più soggetti, i diritti esclusivi appartengono congiuntamente a ciascuno di questi.

Gli art. 5 e 6 della Direttiva 96/9/CE prevedono nello specifico, rispettivamente, il contenuto del diritto di cui all'art. 3 e le eccezioni e limitazioni all'esclusiva.

Articolo 5 - Atti soggetti a restrizioni

L'autore di una banca di dati *gode, per quanto concerne la forma espressiva di tale banca dati* ***tutelabile mediante il diritto d'autore****, del diritto esclusivo di eseguire o autorizzare:*

a) la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsivoglia forma;

b) la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica;

c) qualsiasi forma di distribuzione al pubblico dell'originale o di copie della banca di dati. La prima vendita di una copia di una banca di dati nella Comunità da parte del titolare del diritto o con il suo consenso esaurisce il diritto di controllare all'interno della Comunità le vendite successive della copia; (PRINCIPIO DELL'ESAURIMENTO)

d) qualsiasi comunicazione, presentazione o dimostrazione in pubblico;

e) qualsiasi riproduzione, distribuzione, comunicazione, presentazione o dimostrazione in pubblico dei risultati delle operazioni di cui alla lettera b).

Articolo 6 - Deroghe relative agli atti soggetti a restrizioni

1. ***L'utente legittimo di una banca di dati o di una copia di essa*** *può eseguire tutti gli atti elencati all'articolo 5 che gli sono necessari per l'accesso al contenuto della banca di dati e l'impiego normale di quest'ultima senza l'autorizzazione dell'autore della banca di dati. Se l'utente legittimo è autorizzato a utilizzare soltanto una parte della banca di dati, il presente paragrafo si applica unicamente a tale parte.*

2. Gli Stati membri hanno la ***facoltà*** *di prevedere limitazioni dei diritti* ***di cui all'articolo 5 nei casi sequenti:***

a) allorché si tratta di una riproduzione per fini privati di una banca di dati non elettronica;

b) allorché l'impiego ha esclusivamente finalità didattiche o di ricerca scientifica, sempreché si indichi la fonte, nei limiti di quanto giustificato dallo scopo non commerciale perseguito;

c) allorché si tratta di impieghi per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale;

d) allorché si tratta di altre deroghe al diritto d'autore tradizionalmente contemplate dal diritto interno, fatte salve le disposizioni delle lettere a), b) e c).

3. Conformemente alla convenzione di Berna sulla tutela delle opere letterarie e artistiche, il presente articolo non può essere interpretato in modo da consentire che la sua applicazione arrechi indebitamente pregiudizio ai legittimi interessi del titolare del diritto o entri in conflitto con il normale impiego della banca di dati.

La seconda tipologia di tutela **ex art 7 -** prevede che **i costitutori/creatori delle banche dati** per le quali «*il conseguimento, la verifica e la presentazione […] [del contenuto] attestino un* ***investimento rilevante*** *sotto il profilo qualitativo o quantitativo»* **abbiano il diritto di** *«vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini qualitativi o quantitativi*».

Questa protezione sui generis, a differenza del diritto d'autore, ha una durata più limitata, estinguendosi «*trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data del completamento*» della banca dati.

L'investimento dev'essere rilevante, cioè deve consistere nell'impegno di mezzi finanziari, tempo, lavoro ed energie del costitutore.

La CGUE, nei casi *Fixtures Marketing e British Horseracing Board*, ha specificato ulteriormente la nozione di investimento introducendo come criterio di valutazione quello che conferisce al *database* una disposizione sistematica o metodica del materiale contenuto e un'organizzazione dell'accessibilità individuale degli elementi (fase di presentazione-organizzazione della banca dati).

Il contenuto del diritto sui generis è più limitato rispetto a quello previsto in capo al titolare del diritto d'autore. ex art 7

Inoltre, al diritto di distribuzione compreso nel concetto di reimpiego si applica **il principio dell'esaurimento**.

CAPITOLO III - DIRITTO «SUI GENERIS»

Articolo 7 - Oggetto della tutela

*1. **Gli Stati membri attribuiscono al costitutore di una banca di dati il diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa**, valutata in termini qualitativi o quantitativi, **qualora** il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo.*

2. Ai fini del presente capitolo:

*a) **per «estrazione»** si intende il trasferimento permanente o temporaneo della totalità o di **una parte sostanziale del contenuto di una banca dati** su un altro supporto con qualsiasi mezzo o in qualsivoglia forma;*

*b) **per «reimpiego»** si intende qualsiasi forma di messa a disposizione del pubblico della **totalità** o **di una parte sostanziale del contenuto della banca di dati** mediante distribuzione di copie, noleggio, trasmissione in linea o in altre forme. La prima vendita di una copia di una banca dati nella Comunità da parte del titolare del diritto, o con il suo consenso, esaurisce il diritto di controllare la rivendita della copia nella Comunità.* PRINCIPIO DELL'ESAURIMENTO.

Il prestito pubblico non costituisce atto di estrazione o di reimpiego.

3. Il diritto di cui al paragrafo 1 ***può essere*** *trasferito, ceduto o essere oggetto di licenza contrattuale.*

4. Il diritto di cui al paragrafo 1 si applica a prescindere dalla tutelabilità della banca di dati a norma del diritto d'autore o di altri diritti. Esso si applica inoltre a prescindere dalla tutelabilità del contenuto della banca di dati in questione a norma del diritto d'autore o di altri diritti. La tutela delle banche dati in base al diritto di cui al paragrafo 1 lascia impregiudicati i diritti esistenti sul loro contenuto. CIOE' SUI DATI CONTENUTI.

5. ***Non*** *sono consentiti l'estrazione e/o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca dati che presuppongano operazioni contrarie alla normale gestione della banca dati o che arrechino un pregiudizio ingiustificato ai legittimi interessi del costitutore della banca di dati.*

Analogamente ai *databases* protetti dal diritto d'autore, **la Direttiva 96/9/CE non** prevede alcuna protezione per i singoli dati che compongono il *database* oggetto di tutela sui generis, scelta giustificata dal fatto che «*the legislator wanted to keep the (semantic) information in the public domain*».

Specularmente alle disposizioni del par. I dell'art. 7 della Direttiva 96/9/CE, **l'art. 8** prevede che **l'utente legittimo** possa estrarre e reimpiegare le parti **non** sostanziali della banca dati, valutate in termini qualitativi e quantitativi.

Articolo 8 – Diritti e obblighi dell'utente legittimo

1. ***Il costitutore di una banca dati messa in qualsiasi modo a disposizione del pubblico non*** *può impedire all'utente legittimo della stessa di estrarre e reimpiegare parti* ***non*** *sostanziali, valutate in termini qualitativi o quantitativi, del contenuto di tale banca dati per qualsivoglia fine. Se l'utente legittimo è autorizzato a estrarre e/o reimpiegare soltanto una parte della banca dati, il presente paragrafo si applica solo a detta parte.*

2. L'utente legittimo di una banca dati messa in qualsiasi modo a disposizione del pubblico non può eseguire operazioni che siano in contrasto con la ***normale gestione della banca di dati*** *o che* ***arrechino un eccessivo pregiudizio ai legittimi interessi del costitutore della stessa****.*

3. L'utente legittimo di una banca dati messa in qualsiasi modo a disposizione del pubblico non può arrecare pregiudizio al titolare del diritto d'autore o di un diritto connesso relativo ad opere o prestazioni contenute in tale banca.

Nondimeno, la lesione del diritto sui generis avviene anche nel caso in cui l'estrazione o il reimpiego riguardino parti non sostanziali del contenuto, purché siano ripetuti e sistematici e presuppongano operazioni contrarie alla normale gestione della banca dati o arrechino un pregiudizio ingiustificato ai legittimi interessi del costitutore della banca di dati.

La previsione di un **diritto sui generis sulle banche dati** a livello europeo ha sollevato aspre **critiche**.

In particolare, taluni commentatori hanno ravvisato in tale tutela giuridica un potenziale anticoncorrenziale, dal momento che il costitutore-investitore della banca dati, pur per un periodo di tempo limitato, «*paradoxically obtains the strongest scope of protection available from any intellectual property regime except, perhaps, for the classical patent paradigm itself*».

Le banche dati il cui costitutore/creatore è l'unico soggetto ad avere accesso (le cc.dd. *sole-source databases* o *single-source databases*) pongono problematiche di distorsione della concorrenza ancora più serie.

La tutela giuridica sui generis di tali *databases* si può tradurre in un forte monopolio.

Per evitare conseguenze pregiudizievoli, **i giudici europei** hanno adottato **un'interpretazione restrittiva della nozione di "investimento sostanziale".**

Il costitutore della banca dati non gode della tutela giuridica sui generis se gli investimenti per la costituzione di tali *databases* sono relativi solo alla «creazione dei dati costitutivi» della *databank* (cioè alla produzione di tali risorse), e non anche al conseguimento e all'acquisizione dei dati da altre fonti.

Come affermato nella **sentenza *Horseracing***, «*il fine della tutela, conferita dal **diritto sui generis**, introdotta dalla direttiva è infatti di incentivare la creazione di sistemi di memorizzazione e di gestione di **informazioni esistenti**, e **non** la creazione di elementi che possano essere successivamente raccolti in una banca di dati*».

Ne consegue che le **banche dati *sole-source* non** rientrino nel campo di applicazione della **Direttiva 96/9/CE,** dal momento che gli investimenti del costitutore **si limitino** alla produzione degli elementi della banca dati.

Tale impostazione interpretativo, in linea con **l'art. 102 TFUE**, impedisce ai titolari del diritto di avere un vantaggio competitivo insormontabile dagli altri agenti economici, rappresentato da un «*near-absolute downstream information monopoly in derivative information products or services*».

Più recentemente sono riemerse nuove questioni relative alle **banche dati *single-source.***

La CGUE, nel caso Ryanair, pur non modificando l'orientamento adottato in precedenza, ha specificato che le eccezioni e le limitazioni al diritto d'autore e al diritto sui generis si applicano alle sole banche dati protette da tali istituti giuridici.

In particolare, se **la banca dati** non gode né della tutela giuridica di diritto d'autore, né di quella di diritto sui generis, l'autore-costitutore della stessa **non è soggetto ai limiti** previsti dal **par. I dell'art. 6, dall'art. 8 e dall'art. 15 della Direttiva 96/9/CE.**

Articolo 15 - Inderogabilità di talune disposizioni

*Qualsiasi disposizione contrattuale **in contrasto** con l'articolo 6, paragrafo 1 e con l'articolo 8 è nulla e priva di effetti.*

Perciò, tale soggetto gode di **piena libertà contrattuale** e può imporre a terzi notevoli restrizioni all'accesso al materiale del *database* nei limiti stabiliti dal diritto interno degli Stati membri.

Tuttavia «*contract law has not been harmonized throughout Europe and this can create discrepancies as to the level of protection afforded to such databases among the various Member States*».

Tale conclusione risulta particolarmente pericolosa per le **banche dati *single source***, i cui costitutori, non godendo di alcuna tutela giuridica ai sensi della **Direttiva 96/9/CE**, potrebbero comunque monopolizzare le informazioni contenute.

L'automatizzazione dei processi di acquisizione e immagazzinamento implica che il costitutore di tali banche dati **non** possa accedere alla tutela giuridica di diritto d'autore, prevista dagli **artt. 3 ss.**

della Direttiva 96/9/CE, giacché la scelta e la disposizione degli elementi del *database* non possono essere considerati una creazione dell'ingegno del costitutore.

N.B. In definitiva, l'unica tutela cui si può ricorrere in tali casi può essere quella del diritto sui generis ai sensi degli artt. 7 ss. della Direttiva 96/9/CE.

Per queste ragioni, i soggetti che controllano i *dataset* non godono della tutela accordata dalla Direttiva 96/9/CE.

5.12.b.3) La tutela brevettuale

La tutela brevettuale fa riferimento a tre categorie di invenzioni industriali:

1) le invenzioni di procedimento,
2) le invenzioni di prodotto,
3) le invenzioni d'uso.

In taluni casi, i ***Big data*** trattando dati potrebbero ricondursi alla categoria delle "**invenzioni di procedimento**", ma difficilmente la protezione brevettuale può offrire una tutela rilevante per i "soggetti controllori" dei dati.

È probabile che le tecnologie dell'Internet delle Cose diventino oggetto di **protezione esclusiva** in quanto riconducibili alle **cc.dd. *Computer- Implemented Inventions* (CII),** che sono invenzioni «*which involve the use of a computer, computer network or other programmable apparatus, where one or more features are realised wholly or partly by means of a computer program*».

Più complessa appare la configurazione delle attività di analisi e organizzazione condotte dalle imprese come **invenzioni di procedimento.**

Le maglie di taluni requisiti di proteggibilità delle invenzioni, cioè **la novità** (art. 54 EPC - *European Patent Convention*) e **l'attività inventiva** (art. 56 EPC), **appaiono troppo strette per conferire tutela giuridica a tali pratiche**.

European Patent Convention articolo 54 - Novità

(1) Un'invenzione sarà considerata nuova se non fa parte dello stato dell'arte.

(2) ***Lo stato della tecnica*** *deve comprendere tutto ciò che è stato messo a disposizione del pubblico mediante una descrizione scritta o orale, mediante l'uso o in altro modo prima della data di deposito della domanda di brevetto europeo.*

(3) Inoltre, ***il contenuto delle domande di brevetto europee*** *depositate, le cui date di deposito sono precedenti alla data di cui al paragrafo 2 e che sono state pubblicate a partire da tale data, sono considerate come comprese nello stato dell'arte.*

(4) I paragrafi 2 e 3 non escludono la brevettabilità di alcuna sostanza o composizione, compresa lo stato dell'arte, per l'uso in un metodo di cui all'articolo 53, lettera c), a condizione che il suo uso per tale metodo non sia compreso nella all'avanguardia.

(5) I paragrafi 2 e 3 non escludono inoltre la brevettabilità di alcuna sostanza o composizione di cui al paragrafo 4 per qualsiasi uso specifico in un metodo di cui all'articolo 53, lettera c), a condizione che tale uso non sia compreso nello stato dell'arte.

European Patent Convention articolo 56 - Passo inventivo

Un'invenzione deve essere considerata come implicante una fase inventiva se, tenuto conto dello stato della tecnica, non è ovvio per una persona esperta nella tecnica. Se lo stato dell'arte include anche documenti ai sensi dell'articolo 54, paragrafo 3, questi documenti non devono essere presi in considerazione nel decidere se c'è stata una fase inventiva.

Tranne che nel caso delle tecnologie dell'Internet delle Cose, la tutela brevettuale non si estende agli scenari di sfruttamento economico dei *Big Data*.

5.12.b.4) Il segreto commerciale: la Direttiva (UE) 2016/943 – TUTELA RESIDUALE

Taluni autori hanno fatto notare che la protezione giuridica del segreto commerciale **(*trade secret*)** è complementare e residuale a quella fornita dagli altri diritti di proprietà intellettuale:

- da una parte, la tutela del segreto coinvolge non tanto un'opera o un'invenzione in quanto tali, bensì il processo creativo mediante il quale si perviene al prodotto finale, a patto che la fase di creazione sia tenuta segreta;

- dall'altra, il segreto commerciale si estende ai casi in cui non si può invocare la protezione di alcun'altra privativa intellettuale.

Se la tutela dei *trade secrets* fosse troppo forte, essa costituirebbe in capo al titolare del diritto un monopolio di fatto «potenzialmente perpetuo», che distorcerebbe la concorrenza del mercato e impedirebbe il raggiungimento da parte degli agenti economici dell'allocazione ottimale delle risorse.

Al fine di ridurre tali rischi, nella maggior parte degli ordinamenti giuridici il detentore del segreto commerciale non è titolare di un vero e proprio diritto esclusivo, ma è **tutelato mediante regole di responsabilità (*liability rules*) riguardanti l'acquisizione, l'utilizzo e la divulgazione illeciti delle informazioni segrete.**

La tutela giuridica del segreto commerciale dà origine a un **potere di fatto sulle informazioni segrete**, equiparabile al concetto civilistico di **possesso**.

Per queste ragioni, **il segreto commerciale** si è guadagnato l'appellativo di "Cenerentola" dei diritti di proprietà intellettuale si potrebbe dire che costituisce una "**tutela residuale**".

La protezione giuridica del segreto commerciale ha fatto la sua comparsa nel **diritto europeo** nel 2016, con l'entrata in vigore della **Direttiva (UE) 2016/943**,

1) In alcuni Paesi dell'Unione (Austria, Bulgaria, Repubblica Ceca, Germania, Danimarca, Estonia, Grecia, Spagna, Finlandia, Ungheria, Lettonia, Lituania, Polonia, Romania, Slovenia e Slovacchia) la disciplina del segreto commerciale rientra espressamente nelle regole riguardanti la concorrenza sleale, secondo il paradigma incardinato **nell'art. 39 dell'Accordo TRIPs** (*The Agreement on Trade Related Aspects of Intellectual Property Rights* - in italiano, Accordo sugli aspetti commerciali dei diritti di proprietà intellettuale), spesso noto come accordo TRIPs, è un trattato internazionale promosso dall'Organizzazione mondiale del commercio, meglio conosciuta come OMC, al fine di fissare lo standard per la tutela della proprietà intellettuale. L'Accordo è stato ufficializzato dal GATT – ora WTO - alla fine dell'incontro avvenuto a Marrakech nel 1994, al termine del negoziato Uruguay Round.)

a tali norme, poi, si accostano quelle generali in materia di responsabilità extracontrattuale da **informazioni segrete**.

Art. 39 TRIPs

*1. Nell'assicurare un'efficace **protezione contro la concorrenza sleale** ai sensi dell'art. 10-bis della Convenzione di Parigi (1967), i Membri assicurano la **protezione delle informazioni segrete** conformemente al paragrafo 2 e quella dei dati forniti alle autorità pubbliche o agli organismi pubblici conformemente al paragrafo 3.*

*2. Le persone fisiche e giuridiche hanno la facoltà di **vietare che**, salvo proprio consenso, le informazioni sottoposte al loro legittimo controllo siano rivelate a terzi oppure acquisite o utilizzate da parte di terzi in un modo contrario a leali pratiche commerciali nella misura in cui tali informazioni:*

> *a) siano segrete **nel senso che** non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione;*
>
> *b) abbiano valore commerciale in quanto segrete; e*
>
> *c) siano state sottoposte, da parte della persona al cui legittimo controllo sono soggette, a misure adeguate nel caso in questione intesa a mantenerle segrete.*

3 I Membri, qualora subordinino l'autorizzazione della commercializzazione di prodotti chimici farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche alla presentazione di dati relativi a prove o di altri dati segreti, la cui elaborazione comporti un considerevole impegno, assicurano la tutela di tali dati da sleali usi commerciali. Essi inoltre proteggono detti dati dalla divulgazione, salvo nei casi in cui risulti necessaria per proteggere il pubblico o a meno che non vengano prese misure atte a garantire la protezione dei dati contro sleali usi commerciali.

2) In un gruppo più ristretto di Stati membri, non vi è una **disciplina specifica concernente il segreto commerciale**: la tutela si fonda sui principi della responsabilità aquiliana/extracontrattuale (Belgio, Francia, Lussemburgo, Paesi Bassi) o sull'elaborazione giurisprudenziale in materia di *breach of confidence* (Irlanda).

3) In Svezia, **Italia** e Portogallo, il legislatore ha scelto di conferire una protezione giuridica più forte al segreto commerciale, prevedendo norme specifiche nei codici di proprietà intellettuale nazionali o in atti normativi ad hoc.

La mancanza di una tutela giuridica unitaria a livello europeo ha due effetti negativi sulle attività economiche europee:

- da un lato, gli incentivi alla conduzione di attività di innovazione a livello transfrontaliero sono scarsi, poiché il rischio di acquisizione e divulgazione illecite dei segreti commerciali aumentano negli Stati membri in cui il livello di tutela giuridica è basso;

- dall'altro, una protezione giuridica inadeguata del segreto commerciale riduce la competitività delle imprese, dal momento che «*businesses will lose competitive advantages if their trade secrets are misappropriated*».

Stando al testo della **Direttiva (UE) 2016/943**, la **nozione di segreto commerciale**, **che ricalca l'art. 39 dell'accordo TRIPs**, comprende le informazioni che rispondono cumulativamente ai seguenti requisiti:

«*a) **sono segrete** nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione;*

b) hanno valore commerciale in quanto segrete;

c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete».

Numerosi punti della normativa europea rendono il segreto commerciale uno **strumento giuridico inadeguato** rispetto alle attività di sfruttamento dei *Big Data*.

Il legislatore europeo, infatti, non aveva in mente tali scenari economici al momento della stesura delle disposizioni.

In primo luogo, a differenza della tutela giuridica delle banche dati, **la protezione si estende sia ai singoli dati,** sia, come si desume dal **n. 1 dell'art. 2 della Direttiva (UE) 2016/943**, all'insieme dei dati in quanto tale.

Art. 2 - Convenzioni in materia di proprietà intellettuale

1. In relazione alle parti II, III e IV del presente Accordo, i Membri si conformano agli articoli da 1 a 12 e all'art. 19 della Convenzione di Parigi (1967).

2. Nessuna disposizione delle parti da I a IV del presente Accordo pregiudica gli eventuali obblighi reciproci incombenti ai Membri in forza della Convenzione di Parigi, della Convenzione di Berna, della Convenzione di Roma e del Trattato sulla proprietà intellettuale in materia di semiconduttori.

Il segreto commerciale tutela l'informazione:

- semantica e
- sintattica.

Per accedere alla tutela, i singoli dati o i *datasets* **non** devono necessariamente rispondere a requisiti di originalità, ma **è sufficiente che riguardino attività commerciali e, quindi, siano raccolti e archiviati come parte di dette attività**.

Tuttavia, appare difficile conciliare i singoli dati con il presupposto del valore commerciale stabilito dalla **Direttiva (UE) 2016/943**: secondo il dettato normativo, «*la definizione di segreto commerciale esclude le informazioni trascurabili*».

A) Nella catena del valore dei *Big Data* il singolo dato non detiene, di per sé, un valore commerciale; al contrario, a questo requisito rispondono più verosimilmente le correlazioni fra i dati di un *dataset* e, di conseguenza, gli insiemi di dati e le informazioni di valore ottenute mediante la sottoposizione del *dataset* stesso ai processi automatizzati di analisi.

B) Secondo un'altra lettura della norma, negli scenari di sfruttamento economico dei *Big Data*, nessun dato può essere considerato trascurabile, e, di conseguenza, «*there may no longer be any trivial information that would fall outside the scope of protection*».

In secondo luogo, taluni punti della disciplina europea del segreto commerciale paiono assai difficilmente conciliabili con gli scenari di raccolta dei dati nell'Internet delle Cose.

A ben vedere, **il requisito di segretezza** stabilito dal **par. I dell'art. 2 (lett. a)** non può essere facilmente applicato al contesto di produzione dei dati mediante i sensori di cui sono dotati gli oggetti *Smart* (quali *wearables*, automobili, tostapane, termostati), giacché, «*while the secrecy could be confirmed for data that is produced by the machines inside a factory, data collected by*

Smart cars on freely accessible roads could be collected by the cars of many manufacturers and, hence, will not fulfil this requirement».

Inoltre, **la Direttiva (UE) 943/2016** non spiega quali siano le "**misure ragionevoli**" che il detentore del segreto deve porre in essere per soddisfare il requisito in questione.

5.13) Gli accordi di esclusiva fra le intese restrittive della concorrenza e l'abuso di posizione dominante

Negli scenari economici caratterizzati dall'utilizzo delle tecnologie dei *Big Data* e dell'Internet delle cose, si possono individuare accordi mediante i quali **i soggetti interessati pongono limiti all'accesso ai *datasets*.**

Come si è detto, tali accordi di esclusiva possono essere analizzati

- sia alla luce delle intese restrittive della concorrenza,
- sia dell'abuso di posizione dominante.

Com'è noto, la figura **dell'abuso di posizione dominante** richiede l'accertamento di **due condizioni**:

1. in primis, occorre verificare l'esistenza di una posizione dominante (art. 102 TFUE);
2. in secondo luogo, è necessario dimostrare l'abuso, cioè il comportamento dell'agente economico monopolista che pregiudica la posizione dei concorrenti.

In un caso risalente, **il concetto di posizione dominante** è stato **definito** dalla **CGCE** come «*situazione di potenza economica grazie alla quale l'impresa che la detiene è in grado di ostacolare la persistenza di una concorrenza effettiva sul mercato di cui trattasi ed ha la possibilità di tenere comportamenti alquanto indipendenti nei confronti dei suoi concorrenti, dei suoi clienti e, in ultima analisi, dei consumatori*».

Riguardo alle intese anticoncorrenziali, sussistono notevoli dubbi su come possano essere considerati

- il pregiudizio sensibile (alla luce del principio de minimis stabilito dalla Commissione) e
- il mercato rilevante ai fini dell'applicazione della norma.

Vi sono almeno due scenari riconducibili alla materia de qua, e, in particolare, al **modello di business basato sui cc.dd. *Product-Service Systems* (PSS)**, cioè set di prodotti e servizi che soddisfano congiuntamente i bisogni dell'utente.

Com'è noto, grazie all'integrazione di *software* e sensori, gli oggetti dell'**Internet delle Cose** dispongono di ampie funzionalità.

I sensori del dispositivo *Smart* raccolgono dati, che sono successivamente archiviati e analizzati e, sulla base dei risultati dell'analisi, l'apparecchiatura modifica la sua funzionalità automaticamente mediante gli attuatori attivati da remoto; inoltre, i dati raccolti da una parte sono utili al funzionamento della macchina, dall'altra sono riutilizzabili per altri scopi.

Si possono immaginare **diversi scenari**.

Si pensi, **per esempio**:

1) alle **clausole contrattuali di esclusività** inserite nei contratti di cessione dei dati;
2) alle **restrizioni contrattuali** che proibiscono il c.d. *reverse engineering* da parte dell'utilizzatore del software in un oggetto dell'Internet delle Cose;

   Il Reverse engineering: consiste nella ricostruzione di un prodotto già esistente, in questo caso di un software. Il prodotto viene "smontato" per comprenderne l'architettura, la struttura e il funzionamento. Lo scopo del reverse engineering in ambito software è quello di riprodurre il codice di un programma esistente. In questo modo è possibile ottimizzare il software correggendone gli errori di funzionamento, analizzare i programmi della concorrenza o sviluppare nuovi prodotti.

3) alle **restrizioni inserite negli accordi contrattuali** fra un soggetto controllore e un terzo concernenti il riuso dei *datasets*;

4) alla **restrizione della portabilità** dei dati di un soggetto economico allorché decide di interrompere il rapporto con l'impresa che fornisce tali risorse e passare a un altro *provider*.

In queste ipotesi, nel caso in cui il **compratore e il venditore** stipulano un contratto, si configura la fattispecie dell'intesa anticoncorrenziale (verticale) se ai concorrenti è precluso l'accesso ai mercati della riparazione dell'oggetto *Smart*, ovvero se le clausole contrattuali impediscono al compratore di condividere i dati prodotti dall'apparecchiatura in questione.

Tuttavia, a ben vedere, negli accordi presi in esame non rileva tanto il contenuto dell'accordo, quanto la «*de facto position of the supplier, who may well be the only business in a position to provide the service (for "products as a service") and to distill information form the data gathered from the Thing*».

La fattispecie di abuso di posizione dominante rileva allorché si integrino le situazioni sopra descritte non in presenza di strumenti contrattuali, **ma di misure tecniche e di controllo tecnologico de facto** che, escludendo di fatto uno o più concorrenti dal mercato interessato, hanno effetti anticoncorrenziali.

Tuttavia, come già fatto presente supra, le problematiche relative alla definizione del mercato rilevante ostano all'applicazione delle norme a tutela della concorrenza, e, **in definitiva, rendono il diritto antitrust un campo non particolarmente adeguato a risolvere le questioni inerenti all'accesso ai *Big Data* allo stato delle cose.**

ALCUNI CASI RECENTI:

1) ***GOOGLE*** acquisisce una montagna di dati grazie ai *cookie* inseriti insieme a *banner*, *pop-up* o altre forme di messaggi pubblicitari visibili durante la consultazione di un sito web, ma anche grazie a tutta una serie di strumenti che vanno dal sistema operativo mobile *Android*, al *browser Crome*, a *Google Maps*, a *Waze*, a *Gmail*, *Drive*, *Docs*, *Youtube*.

L'autorità *Antitrust* Italiana, ma ugualmente si sta facendo in USA, il 12 ottobre 2020 ha avviato un procedimento contro *Google* per far luce se *Google* facendo leva sui dati ottenuti attraverso i suoi servizi sia in grado di permettere alla propria *Google Marketing Platform – Demand Side Platform*

– ed al proprio *Google Ad Manager – Supply Side Platform* – di avere prestazioni in tema di capacità di targhettizzazione e di identificazione degli utenti che visualizzano inserzioni non raggiungibili da altri operatori.

Quindi l'ipotesi di abuso di posizione dominante, ex art. 102 TFUE, è stata formulata, poiché *Google,* non mettendo a disposizione i dati fra cui quelli richiesti da I.A.B. - *Interactive Advertising Bureau* - non lascerebbe spazio pubblicitario ad altri sul mercato.

Motiva così *l'Antitrust*: "L'assenza di concorrenza nell'intermediazione delle società specializzate in digital advertising potrebbe ridurre le risorse destinate ai produttori di siti web ed agli editori impoverendo così la qualità dei contenuti diretti ai clienti finali. Inoltre l'assenza di un'effettiva competizione basata sui meriti potrebbe scoraggiare l'innovazione tecnologica per lo sviluppo di tecnologie e tecniche pubblicitarie meno invasive per i consumatori".

Google ha rilasciato, tramite un suo portavoce, affermando che: "I cambiamenti oggetti dell'indagine sono in parte misure per proteggere la *privacy* delle persone e rispondere ai requisiti del GDPR."

Da questa affermazione si ricava che il GDPR vieterebbe la diffusione dei dati richiesti da I.A.B., che però ha già fatto sapere che condivide l'indagine dell'Autorità *Antitrust*

Google infatti, sfruttando la propria posizione dominante ha attuato pratiche concorrenziali nel merito discriminando la concorrenza e chi non aveva acquistato spazi pubblicitari, essendo perciò inseriti nel database interno (c.d. indice dei prodotti): un algoritmo di aggiustamento metteva in risalto, anche nella grafica, questi ultimi, così da rendere di fatto invisibili tutti gli altri concorrenti, sfruttando altri criteri anziché quelli della pertinenza come fatto da altri motori di ricerca generalisti o specializzati in questo settore.

Il 10 novembre 2021 il Tribunale UE nel decidere il ricorso T-162/17 (EU:T:2021:763) ha in gran parte confermato la multa da €.2,42 mld. inflitta dalla Decisione della Commissione UE C(2017)/4444 a *Google* (ed *Alphabet*) per l'intesa anticoncorrenziale con cui ha favorito i propri servizi a danno dei *competitors*.

2) Simile accusa, in data 10 novembre 2020, è stata mossa dalla Commissaria UE alla Concorrenza, Margrethe Vestager, contro ***Amazon*** in quanto la società avrebbe usato a proprio beneficio i dati di fornitori terzi e garantito una via preferenziale ai suoi servizi.

… VEDREMO GLI SVILUPPI di questa procedura contro *Amazon* ed in particolare se ci sarà una pronuncia giudiziaria allineata a quanto è stato deciso per *Google*….

5.14) Il diritto dei consumatori a tutela delle imprese: la Direttiva 93/13/CEE

Clausole vessatorie ex artt. 33 ss del codice del consumo

Nei casi in cui sia stipulato un contratto di fornitura di dati non personali (*data trading*), il soggetto economico dotato di maggiore potere contrattuale può esercitare un'influenza notevole nella conduzione delle trattative, **imponendo clausole lesive dei diritti dell'altro contraente.**

Le norme inserite nella **Direttiva 93/13/CEE**, che rispondono alla ratio di tutela dei consumatori, possono essere rilevanti per redistribuire il potere contrattuale fra le due parti negli scenari di sfruttamento dei Big Data, cioè, in particolare, riguardo ai contratti di fornitura di dati (non personali) acquisiti dagli oggetti dell'Internet delle Cose.

In particolare, ai sensi del **l'art. 3 della Direttiva 93/13/CEE**

Articolo 3

*1. **Una clausola contrattuale, che non è stata oggetto di negoziato individuale, si considera abusiva se, malgrado il requisito della buona fede, determina, a danno del consumatore, un significativo squilibrio dei diritti e degli obblighi delle parti derivanti dal contratto.***

*2. Si considera che **una clausola non sia stata oggetto di negoziato individuale quando è stata redatta preventivamente in particolare nell'ambito di un contratto di adesione e il consumatore non ha di conseguenza potuto esercitare alcuna influenza sul suo contenuto.***

Il fatto che taluni elementi di una clausola o che una clausola isolata siano stati oggetto di negoziato individuale non esclude l'applicazione del presente articolo alla parte restante di un contratto, qualora una valutazione globale porti alla conclusione che si tratta comunque di un contratto di adesione.

Qualora il professionista affermi che una clausola standardizzata è stata oggetto di negoziato individuale, gli incombe l'onere della prova.

3. L'allegato contiene un elenco indicativo e non esauriente di clausole che possono essere dichiarate abusive.

ALLEGATO

CLAUSOLE DI CUI ALL'ARTICOLO 3, PARAGRAFO 3

1. Clausole che hanno per oggetto o per effetto di:

a) escludere o limitare la responsabilità giuridica del professionista in caso di morte o lesione personale del consumatore, risultante da un atto o da un'omissione di tale professionista;

b) escludere o limitare impropriamente i diritti legali del consumatore nei confronti del professionista o di un'altra parte in caso di totale o parziale inadempimento o di adempimento difettoso da parte del professionista di un qualsiasi obbligo contrattuale, compresa la possibilità di compensare un debito nei confronti del professionista con un credito esigibile dallo stesso;

c) prevedere un impegno definitivo del consumatore mentre l'esecuzione delle prestazioni del professionista è subordinata ad una condizione il cui adempimento dipende unicamente dalla sua volontà;

d) permettere al professionista di trattenere somme versate dal consumatore qualora quest'ultimo rinunci a concludere o a eseguire il contratto, senza prevedere il diritto per il consumatore di ottenere dal professionista un indennizzo per un importo equivalente qualora sia questi che recede dal contratto;

e) imporre al consumatore che non adempie ai propri obblighi un indennizzo per un importo sproporzionatamente elevato;

f) autorizzare il professionista a rescindere a sua discrezione il contratto qualora la stessa facoltà non sia riconosciuta al consumatore, nonché permettere al professionista di trattenere le somme versate quale corrispettivo per le sue prestazioni non ancora fornite, qualora sia il professionista che rescinde il contratto;

g) autorizzare il professionista a porre fine senza un ragionevole preavviso ad un contratto di durata indeterminata, tranne in caso di gravi motivi;

h) prorogare automaticamente un contratto di durata determinata in assenza di manifestazione' contraria del consumatore qualora sia stata fissata una data eccessivamente lontana dalla scadenza del contratto quale data limite per esprimere la volontà del consumatore di non prorogare il contratto;

i) constatare in modo irrefragabile l'adesione del consumatore a clausole di cui egli non ha avuto di fatto possibilità di prendere conoscenza prima della conclusione del contratto;

j) autorizzare il professionista a modificare unilateralmente le condizioni del contratto senza valido

motivo specificato nel contratto stesso;

k) autorizzare il professionista a modificare unilateralmente, senza valido motivo, alcune caratteristiche del prodotto o del servizio da fornire;

1) stabilire che il prezzo dei beni sia determinato al momento della consegna, oppure permettere al venditore di beni o al fornitore di servizi di aumentare il prezzo senza che, in entrambi i casi, il consumatore abbia il diritto corrispondente di recedere dal contratto se il prezzo finale è troppo elevato rispetto al prezzo concordato al momento della conclusione del contratto;

m) permettere al professionista di stabilire se il bene venduto o il servizio prestato è conforme a quanto stipulato nel contratto o conferirgli il diritto esclusivo di interpretare una clausola qualsiasi del contratto;

n) limitare l'obbligo del professionista di rispettare gli impegni assunti dai suoi mandatari o assoggettare i suoi impegni al rispetto di una particolare formalità;

o) obbligare il consumatore ad adempiere ai propri obblighi anche in caso di eventuale mancato adempimento degli obblighi incombenti al professionista;

p) prevedere la possibilità per il professionista di cedere a terzi il contratto senza l'accordo del consumatore, qualora ne possano risultare inficiate le garanzie per il consumatore stesso;

q) sopprimere o limitare l'esercizio di azioni legali o vie di ricorso del consumatore, in particolare obbligando il consumatore a rivolgersi esclusivamente a una giurisdizione di arbitrato non disciplinata da disposizioni giuridiche, limitando indebitamente i mezzi di prova a disposizione del consumatore o imponendogli un onere della prova che, ai sensi della legislazione applicabile, incomberebbe a un'altra parte del contratto.

2. Portata delle lettere g), j) e 1) a) la lettera g) non si oppone a clausole con cui il fornitore di servizi finanziari si riserva il diritto di porre fino unilateralmente, e senza preavviso, qualora vi sia un valido motivo, a un contratto di durata indeterminata, a condizione che sia fatto obbligo al professionista di informare immediatamente l'altra o le altre parti contraenti;

L'applicazione della normativa ai contesti sopracitati desta talune problematiche di non facile risoluzione:

- da una parte, **non** sono previste linee guida nella valutazione delle clausole in materia di raccolta e utilizzo dei dati;
- dall'altra, il campo di applicazione della **Direttiva 93/13/CEE** è **limitato** ai soli rapporti fra le **imprese e i consumatori** (B2C).

Occorre notare che alcuni Stati membri dell'Unione hanno esteso la normativa anche alle relazioni fra più imprese (B2B): a ben vedere, i quattro scenari prospettati nel paragrafo precedente potrebbero essere risolti facendo ricorso a tali norme (per esempio mediante la previsione della **nullità della clausola o del contratto**).

N.B. Tuttavia, l'assenza di armonizzazione implica una sostanziale incertezza del diritto, e postula la necessità di un'estensione da parte del legislatore sopra descritta anche ai contesti B2B in ogni Stato membro.

5.15) Il diritto di portabilità dei dati non personali

Il diritto di portabilità dei dati ha a che fare con la facoltà del titolare di disporne e trasferirli.

Il Regolamento (UE) 2016/679 prevede che l'interessato abbia il diritto di portabilità dei dati personali, cioè di «*ricevere in un formato strutturato, di uso comune e leggibile da dispositivo*» o di «*trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti*».

Come si è detto la portabilità risponde a una fondamentale esigenza di tutela del consumatore, giacché consente di abbattere i costi di transizione (*switching costs*) e di diminuire gli effetti di *lockin*:

i consumatori possono passare da un servizio *online* offerto da un'impresa ad uno simile fornito da un'altra **anche se ciò non è espressamente previsto dalle condizioni contrattuali.**

Il diritto europeo non prescrive particolari obblighi che impongono un livello minimo di portabilità dei dati non personali.

«*This is partly because the requirements for implementing data portability can be technically demanding and costly, as different providers of the same services may store data differently*».

Secondo la Commissione, ci sono ottime ragioni per estendere il diritto di portabilità anche ai dati non personali e alle relazioni contrattuali fra più imprese (*business to business*, B2B).

In modo analogo a quanto accade per i consumatori, **un'impresa** che si avvale di un servizio offerto da un altro agente economico incontra notevoli costi di transizione al momento del cambiamento dell'operatore, se non è prevista la possibilità di trasferire i dati.

Per esempio, «*a lock-in problem can […] arise with regard to industrial data where suppliers want to take data with them concerning the quality and longevity of their parts after the termination of the supply contract with the manufacturer of the final product*».

Nella prassi, le compagnie inseriscono **clausole contrattuali** che regolano (e spesso negano) la possibilità di trasferire i dati non personali a terzi, col rischio che gli attori privati più grandi impongano condizioni sfavorevoli alle imprese minori (PMI).

Un diritto di portabilità dei dati non personali garantirebbe l'accesso al patrimonio informativo a un numero più elevato di soggetti, rafforzando la concorrenza sul mercato, e, nel contempo, non avrebbe gli effetti negativi di un diritto di esclusiva.

La Commissione si è impegnata a promuovere un dibattito fra i diversi *stakeholders* sulla possibilità di estendere il diritto di portabilità ai dati non personali nei contratti riguardanti alcuni servizi online, tenendo conto degli effetti che una tale allocazione avrebbe sul mercato.

GUIDA PRATICA DIGITALIZZAZIONE PER L'ESTERO.
TECH LAW: BLOCKCHAIN, SMART CONTRACT, TOKEN, BIG DATA E CRYPTOVALUTE.

Il panorama normativo sia italiano che internazionale su queste tematiche, che vengono definite di Tech Law, è ancora agli albori. L'obiettivo di questa Guida è quello di ripercorrere gli sviluppi di queste aree e, dove possibile, offrire soluzioni.

La mole di dati – Biga Data - e la relativa capacità di calcolo, che permette l'elaborazione degli stessi, sono entrambi crescenti ad un ritmo esponenziale; questo ha portato alla redazione di normative il più complete possibili per la gestione dei casi, e delle relative problematiche a cui questi strumenti possono portare.

La volontà di garantire l'adempimento del contratto limitando gli insoluti e la fase contenziosa ha stimolato la creazione di smart legal contract ed il loro veicolo costituito dalla Blockchain.

La smaterializzazione dei diritti e la ricerca di nuovi strumenti finanziari di produzione e veicolazione della ricchezza hanno prodotto le cryptovalute ed i token.

Lo studio in merito alle tematiche sopracitate si svolgerà analizzando, anche attraverso casi reali, le problematiche e le relative normative di riferimento per arginare e gestire nel miglior modo possibile la sempre più complessa materia digitale.

Per facilitare la comprensione del quadro d'insieme di tutti questi nuovi istituti giuridici e del collegamento con il mondo informatico la guida si compone di molteplici esempi concreti e dati normativi di riferimento imprescindibili per orientare l'operatore che si vuole avvicinare a questo "nuovo mondo".

Per ogni specifica esigenza aziendale, vista la complessità della materia e la continua evoluzione normativa, Unioncamere Lombardia raccomanda di utilizzare in aggiunta a questa pubblicazione il proprio servizio di assistenza consulenziale o, in alternativa, di acquisire comunque altro parere qualificato.

Nessuna responsabilità derivante da un utilizzo improprio dei contenuti della presente pubblicazione, da eventuali modifiche intervenute nella normativa o da possibili imprecisioni potrà essere imputata a Regione Lombardia ed Unioncamere Lombardia o agli estensori della guida stessa.

CAMERA DI COMMERCIO BERGAMO
Camera di Commercio Cremona
Camera di Commercio Pavia
CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA BRESCIA
Camera di Commercio Mantova
Camera di Commercio Sondrio
CAMERA DI COMMERCIO COMO-LECCO insieme per lo sviluppo
CAMERA DI COMMERCIO MILANO MONZABRIANZA LODI
CAMERA DI COMMERCIO VARESE Futuro Impresa Territorio