

DIPARTIMENTO DI IMPRESA E MANAGEMENT

Cattedra di Diritto Pubblico dell'Economia

IL DIRITTO DELL'INNOVAZIONE TECNOLOGICA

RELATORE

Valerio Lemma

CANDIDATA

Alice Greselin

Matr. 215971

ANNO ACCADEMICO 2018-2019

Sommario

INTRODUZIONE	4
CAPITOLO I	5
CENNI SULL'INFLUENZA SOCIO - GIURIDICA DELL'INNOVAZIONE TECNOLOGICA	5
1. <i>Il diritto e la scienza.</i>	5
1. <i>L'IA e il diritto.</i>	8
2. <i>Le tecnologie intelligenti e l'industria 4.0.</i>	13
CAPITOLO II	18
LA REGOLAZIONE DELL'INNOVAZIONE TECNOLOGICA	18
1. <i>L'IA e il diritto: l'autonomous vehicle.</i>	18
1. <i>L'attività contrattuale: gli "smart contracts"</i>	23
2. <i>La blockchain.</i>	26
CAPITOLO III	32
L'INNOVAZIONE TECNOLOGICA NELLA MATERIA BANCARIA E FINANZIARIA	32
1. <i>Fintech.</i>	32
CONCLUSIONE	43
BIBLIOGRAFIA	44

INTRODUZIONE

Il presente elaborato tratta del rapporto tra la tecnologia e il diritto e, nello specifico, dell'influenza che la prima esercita sui rapporti commerciali e la conseguente regolazione di quest'ultima da parte del secondo.

Le problematiche giuridiche che verranno poste non sono nuove, né è possibile pretendere che un giorno svaniscano, in quanto vanno di pari passo con il progresso tecnologico, il quale è necessario al fine dello sviluppo della società.

Nel primo capitolo ci si è posti l'obiettivo di inquadrare alcune nozioni fondamentali inerenti al rapporto tra diritto e scienza, così da fornire gli strumenti necessari al fine di affrontare problematiche maggiormente tecniche. Si sono inoltre introdotte le questioni giuridiche le quali si riferiscono all'intelligenza artificiale e alla c.d. industria 4.0, prodromiche agli argomenti trattati nei capitoli successivi.

Nel secondo capitolo si analizzeranno tre tematiche nate dall'applicazione della tecnologia ai rapporti commerciali e sociali, ovvero i sistemi di guida automatizzati, il contratto del nuovo millennio e la c.d. *blockchain*.

Nel terzo capitolo infine si è affrontato il fenomeno, più specificatamente commerciale - finanziario, *Fintech*, ovvero dell'applicazione della tecnologia alla finanza.

CAPITOLO I

CENNI SULL'INFLUENZA SOCIO - GIURIDICA DELL'INNOVAZIONE TECNOLOGICA

1. Il diritto e la scienza.

Ai fini della presente disamina, ovvero allo scopo di descrivere il rapporto tra il diritto e la scienza e dell'influenza che lo sviluppo di quest'ultima ha sul primo, è necessario preliminarmente delimitare l'ambito della locuzione "scienza".

Per alcuni, almeno fino al recente passato, l'espressione "scienza", nell'ambito del rapporto con il diritto, equivaleva a quella di "scienze della vita", il che determinava il settore del "diritto e scienze della vita"¹. Recentemente tuttavia, sebbene non si sia negato il primato delle scienze biologiche nello sviluppo sociale e scientifico, si è rilevato il fatto che non vi sia una netta prevalenza di una tipologia di scienza rispetto a un'altra, e che anzi vi sia la tendenza a far convergere tipologie di scienza di differente origine². Si pensi anche al fatto che lo sviluppo scientifico fa riemergere interesse verso materie o settori che si ritenevano privi di rilievo, quale a esempio gli studi delle emozioni, il che conseguentemente influisce sullo spazio che agli stessi può essere riservato nel contesto giuridico, la qual cosa a sua volta mina, secondo i più, la razionalità del diritto³. Focalizzare l'oggetto della presente analisi al "diritto delle scienze della vita" sarebbe limitante anche per le tradizionali scienze mediche e biologiche⁴, le quali nel corso del loro sviluppo hanno travalicato i loro stessi confini per interagire con altre discipline in maniera tutt'altro che rigidamente preordinata. È necessario pertanto intendere il termine "scienza" considerando l'incertezza dei confini del c.d. biodiritto⁵, in forza della convergenza tecnologica alla quale prima si è accennato.

Paradigmatico è il caso delle neuroscienze, settore il quale tende a riprodurre le questioni giuridiche, a suo tempo, già sollevate in tema di biologia e nello specifico di genetica⁶. Sebbene, in effetti, i problemi e i dubbi giuridici inerenti al tema delle neuroscienze non siano così diversi a livello

¹ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, Padova, Cedam, 2016, p. 2.

² Si pensi alla c.d. *synthetic biology* che affronta lo sviluppo della genetica attraverso lo sviluppo di calcolo dei computer e di altre tecnologie informatiche e meccaniche.

³ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 2 – 3.

⁴ Si veda SANTOSUOSSO, *Corpo e libertà. Una storia tra diritto e scienza*, Milano, Raffaello Cortina editore, 2001.

⁵ In tema CASONATO, *Introduzione al biodiritto*, Torino, Giappichelli, 2009.

⁶ Si veda in tema di neuroscienza SANTOSUOSSO (a cura di), *Le neuroscienze e il diritto*, Ibis, Como – Pavia, 2009.

qualitativo da quelli emersi nel corso del XIX secolo⁷, è di fatto aumentata la rilevanza della loro trattazione in virtù dello sviluppo delle nuove tecnologie e dell'«ampliamento tecnologico del compasso umano»⁸. La neuroscienza odierna si avvale, ai fini di ricostruire i nessi eziologici del comportamento umano, principalmente di due strumentazioni le quali godono del più ampio e pressoché unanime consenso in ambito scientifico, si tratta della misurazione del flusso sanguigno interno all'area celebrale e dell'analisi dell'attività tecnica sempre riferito alla medesima area⁹. Le tecniche che si avvalgono di questi strumento sono la *neuroimaging*, lo studio dell'amigdala e delle regioni prefrontali, lo studio dell'ippocampo e le tecniche di *lie – detection*¹⁰. Attraverso la *neuroimaging* vengono ricostruite in triplice dimensione la struttura e la funzione del cervello, le quali vengono riprodotte in “neuroimmagini” tramite i raggi X e le tecniche tomografiche¹¹. Le tecniche attualmente in uso sono la Tomografia Computerizzata (TC), la Risonanza Magnetica (RM), la Tomografia a Emissione di Fotone singolo (SPECT) e la Tomografia a Emissione di Positroni (PET)¹². In tale ambito è stata sviluppata anche la functional Magnetic Resonance Imaging (fMRI), attraverso la quale è possibile individuare nei soggetti esaminati le aree cerebrali attivate durante le operazioni cognitive. Sono oggetto di studio, inoltre, le regioni del cervello alle quali è connessa la produzione delle emozioni, come l'amigdala e le zone prefrontali, la cui analisi, assieme alle tecniche di *brain imaging*, potrebbe allargare il campo d'indagine delle neuroscienze. Così anche può determinarsi anche con l'approfondimento dello studio sull'ippocampo, zona celebrale dedicata alla conservazione dei dati mnemonici, la cui utilità, in ambito a esempio processuale penale, può portare alla conoscenza di elementi spesso altrimenti preclusi ad altre modalità di ricerca¹³. Gli studi da ultimo descritti hanno condotto alcuni studiosi a considerare l'utilizzo delle neuro – tecniche per determinare le c.d. *lie – detection*, ovvero l'individuazione di reazioni fisiologiche che, in quanto

⁷ LEVI, *Discorso che potrebbe servire ad uso di programma*, in *Riv. sperimentale di freniatria e di Medicina legale*, n. 1, 1875.

⁸ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 248.

⁹ Si veda BOTTINI, SEDDA, *Neuroscienze Cognitive e Diritto*, in SANTOSUOSSO, GARAGNA, BOTTALICO, REDI, *Scienze Biomediche e Diritto. Un dialogo tra discipline, culture e lingue*, Como – Pavia, Ibis, 2010.

¹⁰ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 254.

¹¹ In tema KHOSHBIN L. S., KHOSHBIN S., *Imaging the mind, Minding the image: an historical introduction to brain imaging and the law*, in *AJLM*, vol. 33, 2007, p. 171 – 192.

¹² Per esempio, con la PET un isotopo radioattivo viene mescolato a una molecola semplice per formare il c.d. *radiotracer* il quale, agendo come una molecola originale ed essendo però radioattivo, una volta iniettato nel sangue del cervello del soggetto, indicherà tramite una traccia elaborata da un computer esterno, una serie di elementi i quali valutati all'esterno potranno essere collegati a particolari azioni, reazioni e stimoli. Si veda SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 255.

¹³ Si veda SCILLIGO, *Stato dell'io e correlati neuronal*, in *Psicologia, psicoterapia e salute*, vol. 9, n. 2, 2003.

indicative di stati mentali veri o falsi, possono verificare quando il soggetto non dica la verità, ipotizzandosi così una prima forma di *mind – reading*¹⁴. A partire dagli anni Ottanta lo studio per definire le *lie detection* è stato condotto attraverso l'ElettroEncefaloGramma (EEG), il quale individuando la presenza di tracce di memoria autobiografica in forza di determinati stimoli, è idoneo a individuare il vero e il falso per via indiretta. Tale tecnica è nota come *fingerprinting* e nel rivelare avvenimenti passati si basa sull'analisi di onde cerebrali, le *p300*, con elettrodi i quali analizzano i picchi di attività cerebrale del soggetto il quale viene messo in contatto con un oggetto, un'immagine e in generale un'esperienza che possa essere capace di rivelare le "impronte cerebrali"¹⁵. Tale risultato è stato perseguito anche attraverso l'impiego della fMRI, tuttavia le tecniche descritte per individuare le c.d. *lie – detection* sembrano ancora troppo pervase da criticità che non consente alla comunità scientifica di essere pressoché unanime sul loro utilizzo¹⁶.

Il diritto odierno, nell'interazione con l'evoluzione scientifica e tecnologica, deve regolare anche il rapporto che detiene con l'etica. È il caso, a esempio, della neuroetica¹⁷, definito quale «studio delle questioni etiche, giuridiche e sociali che sorgono quando le scoperte scientifiche sul cervello vengono portate nella pratica medica, nelle interpretazioni giuridiche e nella politica sanitaria e sociale. Queste scoperte stanno avvenendo nel campo della genetica, del *brain imaging* e nella diagnosi e predizione delle malattie. La neuroetica ha il compito di esaminare come i medici, i giudici e gli avvocati, gli assicuratori e i politici, così come il pubblico si occupano di questi temi»¹⁸. Si rischia di riproporre quindi il problema che già si è presentato in tema di biodiritto, ove con quest'ultimo sembrava volesse effettuarsi più una ricognizione delle norme che si occupavano delle questioni giuridiche inerenti alla vita, al corpo e alla medicina, piuttosto che introdurre un nuovo tema di indagine¹⁹.

¹⁴ Sul poligrafo si veda GANIS, KEENAN, The cognitive neuroscience of deception, in *Social neuroscience*, 4, 2009, p. 465 – 472; HONTS, KIRCHER, Mental and physical countermeasures reduce the accuracy of polygraph tests, *Journal of applied psychology*, 79, 1994, p. 252 – 259.

¹⁵ Lo studio è stato condotto per primo da FARWELL, SMITH, Using brain MERMER testing to detect concealed knowledge despite efforts to conceal, in *Journal of forensic science*, 46, 1.

¹⁶ Sebbene gli studi di Farwell abbiano condotto a una infallibilità dei risultati prossima al 100%. SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 258.

¹⁷ Termine coniato per la Conferenza Neuroethics: Mapping the Field, San Francisco, 13 – 14 giugno 2002.

¹⁸ MARCUS, Neuroethics. Mapping the field. Conference proceedings, Dana press, NY, 2002.

¹⁹ Si veda SANTOSUOSSO, *Bioetica e diritto*, in BARNI, SANTOSUOSSO (a cura di), *Medicina e diritto. Prospettive e responsabilità della professione medica oggi*, Milano Giuffrè, 1995, in particolare p. 21 – 29.

1. L'IA e il diritto.

Lo sviluppo delle nuove tecnologie ha suscitato un acceso dibattito, non solo a livello giuridico, il quale ha fatto emergere critiche allarmistiche in riferimento al timore che la tecnologia possa esercitare un crescente controllo sull'uomo. Una delle questioni socio-giuridiche maggiormente rilevanti sembra essere il bilanciamento tra gli interessi che l'applicazione tecnologica da una parte tutela e dall'altra "danneggia". Se infatti l'espropriazione della capacità professionale dei lavoratori può essere un ragionevole effetto dell'utilizzo della tecnologia in luogo della mano d'opera ai fini della tutela della salute degli operai, così come la riduzione della *privacy* in ambito bancario può perseguire fini di lealtà sociale, e se è difficile individuare cosa vi sia di negativo in un *software* il quale, contenendo tutte le informazioni legislative e giurisprudenziali, effettui un calcolo previsionale in merito a un'azione giudiziaria, nello stesso tempo non potendo prevedere tutti gli effetti dell'applicazione tecnologica all'ordinamento sociale è comprensibile che residuino timori come quello di cui si è accennato.

La questione della convergenza delle nuove tecnologie²⁰, quali nanotecnologia, biotecnologia, tecnologie dell'informazione e scienze cognitive pone la domanda su quale possa essere il ruolo del diritto nella c.d. età dell'oro²¹. Il progredire delle nuove tecnologie, tuttavia, non sembra ridurre in termini generali la necessità di regolazione giuridica la quale, anzi, sembra essere maggiormente richiesta da parte dell'opinione pubblica a fronte del progresso tecnologico²². Il problema, pertanto, non sembra essere quello di intendere se il diritto avrà un ruolo in futuro, quanto quello di identificare quale diritto sarà idoneo a regolare le fattispecie nell'epoca tecnologica.

Nell'ordinamento giuridico, inoltre, non esiste una definizione di "nuove tecnologie", sebbene la giurisprudenza europea se ne sia occupata²³ e la Carta dei Diritti Fondamentali dell'Unione Europea regoli varie materie in tema, in particolare l'art. 8 della CDFUE il quale disciplina la protezione dei dati

²⁰ V. *supra* §1.

²¹ Si veda in tema ROCO, BAINBRIDGE, Overview, in ROCO, BAINBRIDGE, *Converging technologies for improving human performance nanotechnology, biotechnology, information technology and cognitive science*, Arlington, Virginia, 2002; NAAM, *More than human*, Broadway books, 2005; BROCKMAN, *The new humanist: science at the edge*, Barnes & Noble, 2003.

²² GASKELL et al, *Europeans and biotechnology in 2010. Winds of change? A report to the european commission's directorate – general for research*, oct. 2010, in *ec.europa.eu*.

²³ Si veda RUGGIU, *Diritti e temporalità. I diritti umani nell'era delle tecnologie emergenti*, Bologna, Il Mulino, 2012.

di carattere personale. In termini generali ci si potrebbe riferire alle nuove tecnologie in determinati campi specifici oppure a un ambiente tecnologico nuovo²⁴.

È parte delle “nuove tecnologie” quell’ambito della scienza che fa riferimento all’Intelligenza Artificiale, il quale ambito di studio ha avuto un’importante momento di sviluppo durante la metà del XX secolo²⁵, ove l’idea di costruire un computer capace di simulare il cervello umano ha persuaso gli scienziati a perseguire progetti di *strong* IA, i quali tuttavia sono stato abbandonati nel corso degli anni Ottanta per l’impossibilità di conseguire l’oggetto sociale a causa di importanti limiti concettuali²⁶. Gli studiosi passarono quindi allo studio della *light* IA la quale, abbandonando l’idea della ricostruzione analogica del cervello umano, adotta un approccio sostanzialista, perseguendo perciò l’obiettivo di riprodurre alcune funzioni del cervello umano, piantando così le radici della robotica moderna. In quest’ultima, questione emergente è la costruzione di robot i quali imparano dalle proprie esperienze, il che pone l’essere umano di fronte una macchina della quale non è sempre possibile prevedere le reazioni. In tal senso infatti attualmente si parla più in generali di agenti autonomi, nei quali vengono ricompresi i droni, i *software* e, appunto, i *robot*²⁷.

L’autonomia dei *robot* può classificarsi su diversi livelli. Questa può innanzitutto caratterizzare la capacità cognitiva dell’automa il quale sarà in grado di modificare le proprie conoscenze di base attraverso la manipolazione logica delle conoscenze disponibili, di calcolare e selezionare i comportamenti attuabili, e di modificare le conoscenze di base attraverso l’interazione con l’ambiente. Vi sono poi i c.d. *robot* sociali i quali sono in grado di riconoscere l’interlocutore e di impegnarsi in interazioni sociali, percependo il mondo esterno tramite la propria esperienza e imparando dagli altri. La tipologia di *robot* da ultimo citata rientra nella categoria degli automi evolutivi, i quali sono in grado di sviluppare le proprie abilità autonomamente in interazione con l’ambiente fisico e sociale circostante, subordinatamente alla funzione progettata dallo sperimentatore²⁸. Un’analisi accurata pertanto consente di distinguere tre dimensioni di autonomia, ovvero l’indipendenza, le capacità cognitive e l’architettura cognitiva²⁹. La questione diventa inoltre

²⁴ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 305.

²⁵ TURING, *Computing machinery and intelligence*, in *Mind*, New series, n. 236, 1950.

²⁶ FLORIDI, *Philosophy and computing. An introduction*, Routledge, London and New York, 1999, p. 132 ss.

²⁷ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 323.

²⁸ La classificazione è operata da SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 329 - 330.

²⁹ Si veda SARTOR, OMICINI, *The autonomy of technological systems and responsibilities for their use*, in BHUTA, BECK, GEISS, KRESS, LIU, *Autonomous weapons systems: law, ethics, policy*, Cambridge University Press, 2016.

più complessa se si considera che all'interno dell'architettura cognitiva è possibile distinguere l'adattabilità, la teleologia e l'autonomia multilivello, e che tali dimensioni sono ortogonali³⁰. Evidentemente quanto esposto ha effetti notevoli sul regime della responsabilità giuridica per l'azione dei sistemi informatici, e ciò in considerazione anche del fatto che i sistemi automatici sono inseriti a loro volta in sistemi sociotecnici nei quali vi è la combinazione integrata di componenti umane, tecnologiche e organizzative, e per le quali la questione circa il tipo o il livello di autonomia si pone in riferimento a ogni componente.

Per quanto riguarda quello che può essere definito come il livello di autonomia più basso³¹, le azioni poste in essere dall'automa corrispondono al comportamento preimpostato dal progettatore, qualificabili più come mere reazioni predeterminate agli stimoli proveniente dall'esterno. In caso di danni arrecati da tali beni tecnologici al consumatore sarà applicabile lo schema legale della responsabilità del produttore predisposto dalle Direttive n. 1985/374/EC e n. 1999/34/EC, recepite dal D.lgs. n. 206/2005, basate sul principio che il produttore è responsabile dei danni causati dai difetti del bene da questi prodotto, previsto all'art. 114 cod. cons.³². In quest'ultimo qualora il soggetto danneggiato non riesca a provare la responsabilità del produttore, o se questi ne riesca a provare la mancanza, saranno applicabili ove ne ricorrano i presupposti gli artt. 2050³³ – 2051³⁴ c.c.³⁵. Esistono *robot* i quali svolgono attività pericolose di routine come in ambito aerospaziale, industriale, si pensi a esempio alla verniciatura professionale, e medico³⁶. Proprio in riferimento a quest'ultimo ambito è opportuno evidenziare come la giurisprudenza abbia avuto l'opportunità di indagare diverse questioni, ove si è innanzitutto affermato che l'attività medico – chirurgica non può essere considerata pericolosa, escludendosi pertanto l'applicazione dell'art. 2050 c.c.³⁷. Analogamente, qualora l'operazione si esegua mediante *robot*, il chirurgo non potrà essere considerato quale custode

³⁰ *Ibidem*.

³¹ In tema BOSCARATO, Who is responsible for robot's actions? An initial examination of italian law within a european perspective, Atti del Convegno "TILTING perspective 2011 – Technologies on the stand: legal and ethical questions in neuroscience and robotics", Tilburg University, april 2011.

³² Si veda SANTOSUOSSO, BOSCARATO, CAROLEO, *Robot e diritto: una prima ricognizione*, in NGCC, 2012, p. 494 ss.

³³ «Responsabilità per l'esercizio di attività pericolose», «Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno».

³⁴ «Danno cagionato da cosa in custodia», «Ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che provi il caso fortuito».

³⁵ In tema COMPORTI, *Le responsabilità presunte – Artt. 2044 – 2048*, in *Il codice civile – commentario*, SCHLESINGER (fondato da), BUSNELLI (diretto da), Giuffrè, Milano, 2009.

³⁶ Vedi VERUGGIO, EURON roboethics roadmap, january 2007, in www.roboethics.org, p. 33.

³⁷ Così tra le prime Cass., Sez. III, sent. 28 settembre 1968, n. 3011, in www.italgiure.it.

del supporto tecnologico, tantomeno potrà sostenersi che il robot abbia causato il danno autonomamente³⁸.

Al livello successivo di autonomia si possono identificare i *robot* i quali hanno la facoltà di locomozione. In questo caso l'automa agisce sempre secondo gli *standard* preimpostati da chi l'ha progettato e non può porre in essere comportamenti imprevedibili, tuttavia l'attribuzione del potere di movimento richiede l'applicazione di cautele maggiori rispetto alla categoria vista in precedenza. In tal caso, quanto alla disciplina applicabile, sembra più confacente l'art. 2052 c.c.³⁹, in considerazione anche del fatto che la giurisprudenza ha, spesso, applicato l'art. 2051 c.c. a cose immobili, o mobili ma ancorate al suolo. Tale distinzione tuttavia ha limitati effetti giuridici. L'art. 2052 c.c. ha ancora più rilevanza se si pensa che nella categoria in esame rientrano tutti quei *robot* i quali sono dotati di capacità di adattamento all'ambiente esterno la quale si basa sulle esperienze maturate e che è necessaria ad assicurare la propria sopravvivenza. La capacità adattativa è quindi una componente dell'intelligenza artificiale⁴⁰.

La categoria di *robot* che presenta il massimo grado di autonomia è quella che determina anche effetti giuridici maggiormente complessi. Si pensi al *robot iCub* sviluppato dal Centro IIT di Genova⁴¹ il quale, costruito sulla base dell'anatomia umana, è capace di apprendere e muoversi autonomamente in forza dei 53 gradi di libertà dei quali è dotato⁴². Lo scopo dei ricercatori e progettatori è infatti quello di creare un automa il quale sia in grado di imparare dai propri errori e di trarre un insegnamento dalle proprie esperienze attraverso la simulazione di procedimenti mentali eseguiti in forza di algoritmi processati dal *software* del *robot*. L'ulteriore scopo che si cela dietro l'obiettivo di creare un automa con capacità cognitive è quello di costruire uno strumento utile a uno studio bidirezionale, dall'uomo verso la macchina e dalla macchina verso l'uomo, del sistema cognitivo in generale. Ed è proprio in questo campo che si ha un esempio della convergenza delle scienze della quale si è fatto cenno⁴³, in quanto è necessario che, nella costruzione di un *robot* della categoria della

³⁸ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 335.

³⁹ «Danno cagionato da animali», « Il proprietario di un animale o chi se ne serve per il tempo in cui lo ha in uso, è responsabile dei danni cagionati dall'animale, sia che fosse sotto la sua custodia, sia che fosse smarrito o fuggito, salvo che provi il caso fortuito».

⁴⁰ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 338.

⁴¹ Un'esposizione delle caratteristiche dello stesso in www.robotcub.org.

⁴² SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 338.

⁴³ *Supra* §1 e §2.

quale si tratta, vi sia l'apporto di esperti in robotica, bioingegneria e neuroscienza⁴⁴. Le azioni poste in essere dal *robot* le quali sono diretta conseguenza della sua capacità di apprendere dalle proprie esperienze, la quale capacità è a sua volta determinata dalle reti neurali artificiali e dagli algoritmi implementati nel *software* del *robot*, non vengono predeterminate dal programmatore il quale elabora esclusivamente l'algoritmo utile all'apprendimento. Le scelte operate dal *robot* durante la sua attività non saranno pertanto prevedibili, se non in maniera indiretta in quanto in ogni caso riconducibili al tipo di programmazione impostata per l'apprendimento⁴⁵. In questi casi è lecito chiedersi chi sia il responsabile dei danni arrecati dal robot il quale detenga un tale grado di autonomia, soprattutto nei casi in cui l'automa abbia la possibilità di imparare dal possessore⁴⁶. I progettatori hanno enucleato un algoritmo da implementare nel *software* degli automi dei quali si tratta che contempla una serie di problemi etici innanzi ai quali l'automa potrebbe venire a trovarsi, prevedendo contestualmente le relative soluzioni. Quest'ultime si classificano in base al principio della beneficenza, non maleficenza ed equità e, fornendo al *robot* una regola etica di condotta generale, sulla base della stessa l'automa sarà in grado di valutare situazioni nuove e costruire una reazione assiologicamente coerente alla regola citata⁴⁷. Al ricorrere delle circostanze esposte sembra applicabile l'art. 2048 c.c.⁴⁸ nel caso di danni arrecati dal *robot*, il cui II comma prevede che per i danni cagionati dal fatto illecito di allievi e apprendisti sono responsabili gli insegnanti se, al momento della commissione del fatto che ha cagionato l'evento, ricorreva la loro vigilanza. La norma non stabilisce una responsabilità di tipo oggettivo, bensì una presunzione di responsabilità per *culpa in vigilando* e per *culpa in educando*, la quale presunzione riguarda, per l'appunto, la responsabilità, e non la colpa, il che denota un vantaggio per il danneggiato in quanto il precettore potrà provare l'assenza della sua responsabilità per il danno solo in quanto dimostri che non avrebbe potuto in nessun caso evitarne il verificarsi. Si ritiene pertanto che nel caso di sistemi robotici dotati di algoritmi utili all'apprendimento sia responsabilità del produttore inserire all'interno della macchina un "codice etico", così come è

⁴⁴ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 339.

⁴⁵ *Ibidem*.

⁴⁶ Un esempio di tale tipo di *robot* è *Nao*, le cui caratteristiche sono rinvenibili in www.aldebaran-robotics.com.

⁴⁷ Tale tipo di automa è impiegato in ambito assistenziale ospedaliero, si veda ANDERSON M., ANDERSON S. L., *Robot be good: a call for ethical autonomous machines*, in *Scientific american*, oc. 2010.

⁴⁸ «Responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte», «Il padre e la madre, o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi. La stessa disposizione si applica all'affiliante. I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza. Le persone indicate dai commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto».

responsabilità dell'utilizzatore dettare principi etici e di condotta generalmente ritenuti conformi all'ordinamento, in quanto altrimenti si determinerebbe un'omessa vigilanza⁴⁹.

Quanto esposto porta alla considerazione che, almeno in forma embrionale, sembra paventarsi sullo sfondo dell'ordinamento giuridico moderno il riconoscimento della soggettività giuridica ai *robot*.

2. *Le tecnologie intelligenti e l'industria 4.0.*

L'avvento delle nuove tecnologie ha avuto un rilevante impatto sul mondo del lavoro⁵⁰. Grazie al progresso tecnologico, difatti, il mercato inerente alla produzione e allo scambio di beni e servizi è divenuto globale, in forza della maggiore facilità nell'importazione e nell'esportazione di merci, capitali e informazioni, nonché in virtù della possibilità di ridistribuire a livello territoriale attività che in passato non era possibile svolgere se non in quell'unico luogo dove era originata, essendo ora possibile dirigere e coordinare quella stessa attività da remoto⁵¹. La trasformazione in senso tecnologico del mercato del lavoro è stata determinata in particolar modo dalla costruzione dei *robot* industriali intelligenti, dal *cloud computing* e in generale dai nuovi dispositivi digitali. In tal senso si parla della nascita dell'industria 4.0 con il verificarsi della quarta rivoluzione industriale, la quale è caratterizzata dall'utilizzo di sistemi produttivi e logistici intelligenti, il che determina un effetto trasversale nel mondo del lavoro in riferimento, a esempio, alla delocalizzazione dell'attività posta in essere dal lavoratore che ridefinisce i confini spaziali del lavoro, al continuo aggiornamento delle competenze che il lavoratore deve perseguire contestualmente allo svilupparsi del mondo tecnologico, nonché all'inevitabile sostituzione del lavoratore – persona fisica con il lavoratore – *robot*⁵². Ciò impone l'analisi della disciplina del lavoro e della tutela del lavoratore alla luce del ruolo assunto dalla tecnologia nel mercato lavorativo.

Il termine "industria 4.0" è entrato a far parte del lessico socio – economico a partire dal secondo decennio degli anni Duemila quando diversi Paesi, come la Germania e gli Stati Uniti, hanno deciso di

⁴⁹ Così SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 341.

⁵⁰ In tema BOTTALICO, Workplace technological innovation: what role for the law?, in SANTOSUOSSO, GOODENOUGH, TOMASI, *The challenge of innovation in law. The impact of technology and science in legal studies and practise*, Pavia University press, 2015.

⁵¹ Si veda HUWS, *Labor in the global digital economy: the cybertariat comes*, Monthly review press, NY, 2014.

⁵² SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 342.

investire in un nuovo modello produttivo, promuovendo l'informazione circa le possibilità che la digitalizzazione offre all'industria⁵³. Strettamente connesso all'industria 4.0 è il c.d. *Internet of things*⁵⁴, ovvero la circostanza che tutte le novità tecnologiche in ambito robotico e digitale sono connesse a *internet*, essendo in tal modo in grado di scambiare reciprocamente informazioni in tempo reale per svariate finalità. Nella categoria delle tecnologie le quali rientrano nell'IoT vi sono i *robot* industriale, i quali sono dispositivi meccanici utilizzati per il supporto nell'attività produttiva. Tali si distinguono per il grado di libertà, come già visto peraltro trattando in generale di IA⁵⁵, per il tipo di applicazione nel processo di fabbricazione, l'architettura e la marca⁵⁶. Se, inoltre, in passato le macchine utilizzate in ambito industriale erano identificabili quali sistemi isolati con "limitate" capacità di calcolo, di memoria e di elaborazione di dati, attualmente il mercato industriale fa utilizzo di *robot* dotati di nuove capacità di scambio di informazioni e di esecuzione di dati attraverso la rete, il c.d. *cloud robotics*. Tale sistema, detto anche *cloud computing*, è l'innovazione maggiormente rilevante degli ultimi anni in quanto il suo utilizzo ha consentito, in modalità remoto tramite l'accesso a *internet*, l'archiviazione, l'elaborazione e l'uso di una mole di dati non contemplabile nel recente passato⁵⁷. Funzione particolarmente rilevante è la capacità predittiva che l'intero sistema contempla grazie all'elaborazione dei c.d. Big data⁵⁸, in virtù della quale è possibile trarre informazioni in riferimento al comportamento degli individui o di gruppi di persone e circa le decisioni di questi, nonché effettuare precise valutazioni del rischio riguardo gli aspetti maggiormente pericolosi e problematici in ambito lavorativo⁵⁹. Il *cloud* pertanto consente di conoscere dati di produzione o problematiche inerenti all'attività produttiva in tempo reale anche per i soggetti i quali siano delocalizzati e che possono intervenire di conseguenza, il tutto connotato a priori da un procedimento

⁵³ Si veda a titolo esemplificativo President's Council of advisor on science and technology, Report to the President on ensuring american leadership in advanced manufacturing, in www.whitehouse.gov, 2011.

⁵⁴ KOUROUPETROGLOU, Enhancing the human experience through assistive technologies and E – accessibility, IGI global, 2014.

⁵⁵ *Supra* §2.

⁵⁶ PANDILOV, DUKOVSKY, Comparison of the characteristics between serial and parallel robots, Acta tehnica corviniensis, Bulletin of engineering, 1, in part. p. 143 – 160.

⁵⁷ V. *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni. Sfruttare il potenziale del cloud computing in Europa*, Bruxelles, COM(2012), in *eur – lex.europa.eu*. Cfr. anche FERRARI, ZANLEONE, *Cloud computing. Aspettative, problemi, progetti e risultati di aziende passate al modello as a service*, Franci Angeli, Milano, 2011. CARR, *The big switch: rewiring the world, from Edison to Google*, NY – London, WW Norton, 2009.

⁵⁸ Cenni sul tema LOHR, The age of Big data, in NYT, 11 feb. 2012.

⁵⁹ HOLTGREVE, New technologies: the future and the present of work in information and communication technology, in *New technology, work and employment*, 2014.

“*smart*”, ovvero basato sulla predittività delle azioni e degli accadimenti futuri in base ai dati raccolti, il che definisce una nuova tipologia di *enhancement* tecnologico inteso quale potenziamento dell’individuo in virtù dell’utilizzo della tecnologia portatile e diffusa⁶⁰.

Il progresso tecnologico e il diritto vivono nell’attuale momento storico un processo di mutuo riconoscimento, il che consente di abbracciare l’innovazione senza però rinunciare a curare profili di tutela del soggetto. In tal senso si è difatti già accennato all’erosione della concezione tradizionale del “luogo e dell’orario di lavoro” cui porta l’applicazione tecnologica al mondo del lavoro. Con la *portable technology*, infatti, la localizzazione del luogo di lavoro diventa diffusa, non riducendosi più all’ufficio o alla sede societaria stabilita in un determinato territorio, potendo in taluni casi il datore di lavoro pretendere che il soggetto da lui dipendente si renda produttivo anche quando è in viaggio⁶¹. La definizione di nuove mansioni lavorative, le quali non sono più limitate al solo utilizzo del macchinario ma richiedono che il soggetto monitori e gestisca il *robot* il quale dovrà espletare le azioni produttive, determinano nuove aspettative circa la diligenza del dipendente, il quale non potrà non contemplare la componente digitale⁶². In tema, difatti, la Corte di cassazione ha affermato che il prestatore di lavoro debba applicare una diligenza parametrata alle mansioni, alla qualifica e comunque alle reali posizioni assunte dallo stesso nella concreta organizzazione del lavoro⁶³, emergendo in tal modo inoltre l’equiparazione della diligenza che il lavoratore deve applicare nell’espletamento della sua attività con l’interesse e l’esigenza organizzativa che l’impresa persegue, i quali due ultimi elementi fungono da ulteriori parametri di determinazione del livello di diligenza richiesto nella fattispecie concreta⁶⁴. Quanto esposto corrobora la considerazione la quale evidenzia che, essendo necessaria la cooperazione con i *robot* e in generale con le tecnologie autonome digitali nell’industria 4.0, vi è una crescente necessità di formazione del personale dipendente il che conduce a una maggiore flessibilità dello stesso⁶⁵.

⁶⁰ SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., p. 346.

⁶¹ *Ibidem*.

⁶² In tema l’art. 2104 c.c. rubricato «Diligenza del prestatore di lavoro» stabilisce che «Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall’interesse dell’impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l’esecuzione e per la disciplina del lavoro impartite dall’imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende».

⁶³ Cass. civ., sez. lav., sent. 27 settembre 2000, n. 12769, con commento di NADALET, *Sull’obbligo di diligenza e i c.d. compiti accessori: verso un’estensione della sfera di imputabilità*, in *Riv. it. dir. lav.*, 3, 2001, p. 446.

⁶⁴ VISCOMI, *Diligenza e prestazioni di lavoro*, Torino, Giappichelli, 1997, p. 151 ss.

⁶⁵ In tema è rilevante l’art. 2103 c.c. rubricato «Prestazione del lavoro», il quale a seguito della riforma del d.lgs. 15 giugno 2015 n. 81 prevede che «Il lavoratore deve essere adibito alle mansioni per le quali è stato assunto o a quelle corrispondenti all’inquadramento superiore che abbia successivamente acquisito ovvero a mansioni riconducibili allo stesso livello di

In tema di controllo a distanza dei lavoratori l'art. 4 l. n. 300/1970 rubricato «Impianti audiovisivi» stabilisce che «Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196»⁶⁶. Le informazioni raccolte dai computer aziendali, dai robot industriali e dalle

inquadramento delle ultime effettivamente svolte. In caso di modifica degli assetti organizzativi aziendali che incidono sulla posizione del lavoratore, lo stesso può essere assegnato a mansioni appartenenti al livello di inquadramento inferiore purché rientranti nella medesima categoria legale. Il mutamento di mansioni è accompagnato, ove necessario, dall'assolvimento dell'obbligo formativo, il cui mancato adempimento non determina comunque la nullità dell'atto di assegnazione delle nuove mansioni. Ulteriori ipotesi di assegnazione di mansioni appartenenti al livello di inquadramento inferiore, purché rientranti nella medesima categoria legale, possono essere previste dai contratti collettivi. Nelle ipotesi di cui al secondo e quarto comma, il lavoratore ha diritto alla conservazione del livello di inquadramento e del trattamento retributivo in godimento, fatta eccezione per gli elementi retributivi collegati a particolari modalità di svolgimento della precedente prestazione lavorativa. Nelle sedi di cui all'articolo 2113, ultimo comma, o avanti alle commissioni di certificazione, possono essere stipulati accordi individuali di modifica delle mansioni, del livello di inquadramento e della relativa retribuzione, nell'interesse del lavoratore alla conservazione dell'occupazione, all'acquisizione di una diversa professionalità o al miglioramento delle condizioni di vita. Il lavoratore può farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato o da un avvocato o da un consulente del lavoro. Nel caso di assegnazione a mansioni superiori il lavoratore ha diritto al trattamento corrispondente all'attività svolta e l'assegnazione diviene definitiva, salva diversa volontà del lavoratore, ove la medesima non abbia avuto luogo per ragioni sostitutive di altro lavoratore in servizio, dopo il periodo fissato dai contratti collettivi, anche aziendali, stipulati da associazioni sindacali comparativamente più rappresentative sul piano nazionale o, in mancanza, dopo sei mesi continuativi. Il lavoratore non può essere trasferito da un'unità produttiva ad un'altra se non per comprovate ragioni tecniche, organizzative e produttive. Salvo che ricorrano le condizioni di cui al secondo e quarto comma e fermo quanto disposto al sesto comma, ogni patto contrario è nullo».

⁶⁶ Diversamente dalla precedente disciplina la quale stabiliva la necessità della sussistenza di un accordo tra il datore di lavoro e i Sindacati o, in alternativa, si una specifica autorizzazione da parte delle Direzioni territoriali del lavoro competenti, ora

strumentazioni elettronico – digitali in generale, non necessiteranno pertanto di specifiche procedure per essere utilizzate ai fini disciplinari o di gestione del rapporto di lavoro, sempreché venga data al lavoratore adeguata informazione circa le modalità di utilizzo degli strumenti e di effettuazione dei controlli secondo la normativa disciplinante la privacy⁶⁷.

Come affermato in precedenza, la *smart technology* conduce a un nuovo modo di approcciarsi alle materie già regolate dal legislatore, come nel caso da ultimo citato ove, a fronte del progresso tecnologico, piuttosto che impedire *tout court* la raccolta di dati sul lavoratore e sull'attività da questi svolta, si è deciso di regolare la raccolta e l'uso delle predette informazioni, escludendosi in ogni caso violazioni della dignità e della privacy del lavoratore⁶⁸.

non necessaria nel caso in cui le informazioni vengano raccolte dagli strumenti utilizzati per rendere la prestazione lavorativa o che registrano gli accessi e le presenze.

⁶⁷ Si veda BARRACO, SITZIA, *La tutela della privacy nei rapporti di lavoro*, Milano, Wolters Kluwer, 2012.

⁶⁸ V. Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, in www.garanteprivacy.it.

CAPITOLO II

LA REGOLAZIONE DELL'INNOVAZIONE TECNOLOGICA

1. *L'IA e il diritto: l'autonomous vehicle.*

Rappresenta un dato di fatto, sebbene agli albori, la commercializzazione delle automobili con vari livelli di autonomia, il che sancisce l'inizio di una circolazione stradale mista con le automobili a conduzione manuale. Ciò, come già in parte rilevato⁶⁹, pone degli interrogativi in materia di responsabilità innanzitutto in riferimento al produttore, sia in termini di *product liability* che di responsabilità per attività pericolosa, ma anche nei confronti del proprietario e dell'utilizzatore, soprattutto se si considera la circostanza che, verosimilmente nel prossimo futuro, le automobili saranno *driverless*, ovvero completamente autonome e prive di comandi di guida⁷⁰.

Trattando il tema è necessario distinguere fra la disciplina legale della responsabilità per danni da conduzione, proprietà, fabbricazione o distribuzione dei mezzi di trasporto a guida automatizzata e quella, prevalentemente amministrativa, che regola i requisiti tecnici esigibili, quali le caratteristiche minime per la omologazione⁷¹. Preliminarmente è necessario evidenziare che le regole proprie della responsabilità civile non posso essere troppo diverse, nella loro conformazione, a seconda che il danno sia provocato da un veicolo automatizzato o a conduzione umana, il che evidenzia il carattere prematuro delle esigenze tecno-etiche le quali vorrebbero norme *ad hoc* in materia di responsabilità per il danno prodotto da un automa, e inoltre eventuali norme le quali richiedessero all'I.A. generali capacità più elevate di analisi e percezione delle circostanze rispetto all'uomo ostacolerebbero, in termini di analisi economica del diritto, l'industrializzazione e la fruizione di nuove tecnologie⁷².

⁶⁹ V. *supra* cap. I.

⁷⁰ BURNS, SHULGAN, *Autonomy - The quest to build the driverless car - and how it will reshape our world*, Ecco Press, New York, 2018.

⁷¹ In tema RUFFOLO, *Self-driving car, auto driverless e responsabilità*, in RUFFOLO (a cura di), *Intelligenza Artificiale e responsabilità*, Milano, 2017.

⁷² RUFFOLO, MUREDEN, *"Intelligenza artificiale" e diritto, autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense*, in *Giur. It.*, 7, 1704, 2019. Gli AA. evidenziano come «Rischia di svilupparsi, così, una cultura dell'innovazione che si rivela suo malgrado luddista, e che genera pre-giudizi tecnologicamente illogici, eppure ingiustificatamente penetrati nel comune sentire. Irragionevole appare, così, il senso di timore verso la guida automatizzata, diffusosi, dopo i primi entusiasmi, sull'eco delle notizie dei relativamente rari incidenti mortali imputabili alla circolazione sperimentale di auto *selfdriving*, e talora anche *driverless*. Eppure, la incidenza statistica di tali sinistri è già oggi comparativamente molto bassa, a parità di chilometri percorsi, rispetto a quella da ordinaria circolazione».

La prospettiva la quale denota una diminuzione degli incidenti causati dall'uomo, in virtù dell'utilizzo di veicoli autonomi, spinge alla considerazione che la responsabilità per i danni prodotti da un *autonomous vehicles* possa essere addebitata ai produttori, determinandosi quindi lo spostamento dell'intero baricentro della ripartizione della responsabilità tra produttore – utilizzatore/proprietario il che rappresenterebbe, anche in tal caso, una possibile causa di ostacolo al progresso tecnologico. È possibile affermare, tuttavia, che fino a quando non si tratti di veicoli completamente autonomi, benché dotati di un notevole grado di autonomia, il conducente è il responsabile per i danni cagionati dalla vettura in quanto *human in command*, al quale è richiesto di restare vigile e di prendere quando necessario il comando del mezzo di trasporto, così non potendosi qualificare come mero supervisore bensì quale effettivo conducente ai sensi del decreto 28 febbraio 2018 concernente «Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni *Smart Roads* e di guida connessa e automatica».

Quanto da ultimo affermato, a maggior ragione, sancisce la permanenza della responsabilità del produttore, in considerazione anche del fatto che «L'analisi costi-benefici, e le esigenze di ottimizzare massimo produttivo e massimo sociale, convergono dunque verso la opportunità di lasciare immutato l'attuale regime, di matrice comunitaria, di responsabilità oggettiva del produttore di veicoli, quando le nuove tecnologie tendono a far scemare le responsabilità dell'utente. Senza dimenticare che traslare su quest'ultimo taluni rischi da prodotto tecnologicamente evoluto significherebbe disincentivarne l'acquisto. E, sempre in termini di analisi economica del diritto, non pare razionale, a fronte di prodotto più sicuro e quindi socialmente più desiderabile, alleggerire le responsabilità del fabbricante per non disincentivarne l'attività produttiva, pagando però il prezzo di rendere meno incline l'acquirente verso quel segmento di mercato e quella tipologia di prodotto. Il rimedio sarebbe peggiore del male»⁷³.

In materia di *product liability* il rapporto tra responsabilità da prodotto e rispetto degli *standard* imposti dalla legge è di rilevanza centrale, rilevando se è quando il rispetto di tali standard sia una condizione sufficiente a ritenere il prodotto non difettoso o se invece debba essere considerato un elemento necessario ma non sufficiente⁷⁴. Il prodotto non conforme dev'essere ritenuto

⁷³ RUFFOLO, MUREDEN, ult. op. cit., p. 69.

⁷⁴ In tema AMIDEI, *Intelligenza artificiale e responsabilità da prodotto: gli sviluppi del diritto del diritto dell'Unione Europea*, in *Giur. It.*

automaticamente difettoso ma non può simmetricamente sostenersi che il prodotto conforme sia, per ciò solo, sicuro e non difettoso⁷⁵.

Ciò è in linea con la tesi la quale sostiene la cumulabilità fra la tutela da *product liability* e quella prevista dall'art. 2050 c.c.⁷⁶, in quanto la sicurezza garantita dall'applicazione di standard non esclude la pericolosità di una determinata attività produttiva e, quindi, del conseguente prodotto, così come non è possibile pertanto escludere la pericolosità di un prodotto omologato. In tema peculiare problema che concerne tutti i prodotti dotati di I.A., e in particolare i veicoli, il quale può produrre degli effetti sulla disciplina della responsabilità è la fattispecie di *hackeraggio*⁷⁷. L'*hacker* attraverso operazione informatiche è in grado di sabotare, alterare o comunque deviare il funzionamento del veicolo dotato di guida intelligente, potendo letteralmente dirottare l'autovettura. Così benché un veicolo sia conforme agli standard di produzione imposti dalla legge, ciò non escluderebbe che possa essere *hackerato*. In tal caso sarebbe incongruo escludere l'applicabilità dell'art. 2050 c.c. vista la permeabilità del sistema informatico la quale ha reso possibile l'illegittima attività dell'hacker, ancorché tale permeabilità non fosse nota al momento della commercializzazione del prodotto tecnologico⁷⁸.

Il dibattito tra la necessità di un sistema normativo *ad hoc* per alcune fattispecie riferibili all'I.A. e la sufficienza in materia di quello vigente sembra, attualmente, muoversi verso il secondo orientamento, il quale presenta una proposta normativa con molteplici positività in quanto «[...] risulterebbe coordinata con le discipline delle responsabilità da proprietà o conduzione del veicolo. Le quali, sulla base dell'art. 2054 c.c., si estendono anche ai “danni derivanti da vizi di costruzione o da difetto di manutenzione del veicolo”.

Difficile, dunque, sollevare il fabbricante da forme di *strict liability* (per i difetti del prodotto) omologhe, ancorché non identiche, a quelle comunque gravanti sull'incolpevole proprietario o

⁷⁵ RUFFOLO, MUREDEN, “*Intelligenza artificiale*” e diritto, *cit.*, non potendosi affermare «[...] il contrario invocando le esigenze di ottimale allocazione dei rischi (a spese, così, dei soggetti lesi), o di uniformità degli standard di sicurezza, i quali sono normativamente imposti solo come requisiti minimi per permettere la commercializzazione di taluni prodotti (si pensi alla omologazione delle automobili, o, in settore del tutto diverso, alle certificazioni del Banco di Prova che condizionano la lecita commercializzazione o possesso delle armi detenibili da privati). Essi dovrebbero essere il più uniformi possibile (ed in buona parte sono già, di fatto, sostanzialmente “globalizzati”). Ma non è questa la via per rendere omogenea la disciplina del danno da prodotto. E neppure quella per assicurare la migliore allocazione dei rischi, ed ancor meno una tutela minima conveniente per i soggetti lesi: il risultato sarebbe un inaccettabile abbassamento dell’asticella della tutela».

⁷⁶ V. *supra* cap. I.

⁷⁷ Vedi GAMBINO, *Diritti fondamentali e cybersecurity*, in POLLICINO, FROSINI, APA (a cura di), *Diritti e libertà in internet*, Milano, 2017.

⁷⁸ RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giur. It.*

conducente (per “vizi di costruzione”). E va altresì posta attenzione alla circostanza che i “vizi di costruzione” ex art. 2054 c.c. potrebbero non coincidere con i difetti del prodotto di cui alla norma consumeristica, e dunque potrebbero anche non beneficiare di quella sorta di scriminante che, per il produttore, è relativa al “rischio da sviluppo”; sarebbe coordinata, altresì, con la ipotizzabile responsabilità del conducente (anche) ex art. 2050 c.c., in relazione a taluni picchi di pericolosità specifica del *self-driving* car (ad esempio, per la guida di veicoli sperimentali o, in talune circostanze, per l’interazione del veicolo con specifiche categorie di pedoni particolarmente a rischio), ancorché quest’ultimo si riveli in generale più sicuro rispetto ai mezzi a guida umana; consentirebbe di attribuire una concorrente responsabilità ex art. 2050 c.c. in capo al fabbricante, così escludendo che il “rischio da sviluppo”, quando tanto incidente da caratterizzare la pericolosità del produrre, resti in capo al solo “proprietario” o “conducente”.

Consideriamo, a tal proposito, che, secondo l’art. 117 Cod. cons. “un prodotto non può essere considerato difettoso per il solo fatto che un prodotto più perfezionato sia stato in qualunque tempo messo in commercio”. Ne consegue che un’auto *self-driving* ritenuta “sicura” al momento della sua messa in circolazione, e solo pochi mesi o semestri dopo reputata non più tale grazie al veloce progresso tecnologico, potrà comunque continuare a circolare per anni, senza essere considerata “difettosa” ai sensi della disciplina della responsabilità da prodotto. Ne risulterebbero, così, responsabilizzati il proprietario ed il conducente (sempre ex art. 2054 c.c., e talora forse anche per attività pericolosa), ma resterebbe esente da responsabilità il fabbricante, in virtù dell’esimente del “rischio da sviluppo”.

La cumulabilità, in capo al fabbricante, della responsabilità da prodotto con quella da attività pericolosa eviterebbe una siffatta abnorme situazione; consentirebbe, in relazione anche a quanto precede, di giungere ad una lettura “evolutiva” dell’art. 2054 c.c., quale specificazione particolare della responsabilità “per fatto della cosa” ex art. 2051 c.c. (che sarebbe altrimenti applicabile anche alla “cosa automobile”) ed altresì a quella da cosa “animata”, quale l’animale, ex art. 2052 c.c. E si rifletta sulla circostanza che tale norma codicistica è fondata sul criterio del “*cuius commoda eius incommoda*”, il quale renderebbe eticamente ingiustificata ed ingiustificabile una limitazione di responsabilità da rischio da sviluppo a favore del proprietario o del conducente del veicolo. Senza contare che mancherebbe comunque ogni appiglio normativo per giustificarla.

Tanto è confermato anche da una lettura sistematica delle discipline in questione⁷⁹: tale limitazione di responsabilità risulta espressamente prevista dalla norma presente nel Codice di consumo in materia di responsabilità da prodotto, ma risulta assente, invece, in quelle del codice civile. L'art. 2054 c.c., così, responsabilizza (ed è cosa eticamente apprezzabile) colui che continua a detenere o usare veicoli nel frattempo divenuti relativamente pericolosi perché superati dalle sopravvenute tecnologie caratterizzanti i prodotti successivamente messi in circolazione; detterebbe responsabilità selettive ed idonee ad incentivare una produzione ottimale in un settore, quale quello in esame, caratterizzato da elevata pericolosità nel produrre in quanto esposto a rapide evoluzioni tecnologiche: si è detto che le auto *self-driving* sono molto sicure in generale, ma sono anche suscettibili di presentare specifici "talloni d'Achille", con picchi settoriali di pericolosità.

Una forma di responsabilizzazione specificamente e conseguentemente modulata, come qui si prospetta, oltre a corrispondere alla lettera come allo spirito della legge, costituirebbe un valido incentivo ad elidere quella pericolosità specifica, inducendo il fabbricante a destinare risorse alle "misure idonee" ad eliminarla, e dunque ad affrontare i correlati oneri preventivi, per sottrarsi ai costi risarcitori successivi che, in assenza di quelle misure, l'art. 2050 c.c. altrimenti imporrebbe; eviterebbe, in ultima istanza, storture interpretative del sistema.

La generale esigenza di allocare i costi risarcitori là dove possono costituire incentivo a produzioni più virtuose, da un canto non può sempre essere soddisfatta a spese delle vittime e, dall'altro, non deve generare incongruenze sistemiche. Quali quelle che deriverebbero dal voler assicurare, per via normativa o interpretativa, parziali immunità ad una produzione capace di rendere le strade molto più sicure, ma a pena di un sensibile incremento di pericolosità settoriali⁸⁰. Alcuni correttivi alle soluzioni avanzate dalla dottrina e da ultimo citate potrebbe rinvenirsi nella previsione da parte del legislatore di appositi obblighi e doveri assicurativi da evento, e nella predisposizione di fondi dedicati a risarcire o indennizzare danni causati da veicoli a guida automatizzata, fondi che dovrebbero essere finanziati soprattutto dal prelievo fiscale nei confronti degli operatori di settore, i quali vedrebbero così ridurre alcuni potenziali costi da responsabilità senza però trasferire tale riduzione sui soggetti danneggiati o in generale sulla collettività.

⁷⁹ *Ibidem*.

⁸⁰ RUFFOLO, MUREDEN, "Intelligenza artificiale" e diritto, cit., p. 75 – 76. V. anche RUFFOLO, *Intelligenza Artificiale*, cit.

1. L'attività contrattuale: gli "smart contracts".

La nomenclatura "*smart contract*", coniata da N.J. Szabo⁸¹, indica dei protocolli transattivi computerizzati i quali eseguono i termini di un contratto⁸². Dalla *vending machine* si è passati a protocolli di sicurezza rispettosi di determinati termini contrattuali, capaci di eseguire la prestazione promessa o di verificare il corretto adempimento della controprestazione, prefigurando l'inizio di un percorso di assorbimento della logica contrattuale nella tecnologia⁸³.

La definizione specifica di *smart contract* è una questione pregiudiziale non di facile soluzione⁸⁴, in quanto troppo spesso viene affrontata tramite gli strumenti delle *technicalities*⁸⁵, sulle strutture delle stesse e sul loro nesso con il fenomeno degli *smart contracts*⁸⁶.

Un primo approccio, particolarmente estensivo, qualifica lo *smart contract* come l'accordo soggetto a esecuzione automatizzata, ove rientrano tutte le transazioni ad alta frequenza⁸⁷ e le interazioni collusive le quali fissano i prezzi in vista dell'obiettivo di massimizzazione del profitto⁸⁸, entrambi in assenza di consapevolezza della compartecipazione di persone fisiche⁸⁹. Tale definizione da ultimo

⁸¹ Si veda SZABO, Smart contracts, in www.virtualschool.edu, 1994; ID., Smart contracts: Building blocks for digital markets, in www.fon.hum.uva.nl, 1996; ID., Formalizing and securing relationships on public networks. In first Monday 2, in ojphi.org, 1997.

⁸² Si v. in particolare SZABO, Smart contracts: Building blocks for digital markets, cit.

⁸³ Cfr. RASKIN, The law and legality of smart contracts, 1 Geo. L. Tech. Rev., 305, 2017.

⁸⁴ CLACK, BAKSHI, BRAINE, Smart contract templates: foundations, design landscape and research directions, Cornell University computing research repository, in arxiv.org.

⁸⁵ Si veda KOLVART, POOLA, RULL, Smart contracts, in KERIKMAE, RULL (eds), The future of law and eTechnologies, Springer, 2016, 133.

⁸⁶ MIK, Smart contracts: terminology, technical limitations and real world complexity, 9 law, innovation & technology, 269, 2017.

⁸⁷ DI CIOMMO, Gli smart contract e lo smarrimento del giurista nel mondo che cambia. Il caso dell'High frequency trading (HFT) finanziario, in FIMMANÒ, FALCONE (a cura di), Fintech, Universitas mercatorum, Napoli.

⁸⁸ Cfr. SCHREPEL, Collusion by Blockchain and smart contract, in www.ssrn.com, 2019.

⁸⁹ HARRINGTON, Developing competition law for collusion by autonomous artificial agents, in Competition law and economics.

riportata, tuttavia, sembra far sfumare i contorni della categoria *de qua*, contemplando da un lato archetipi industriali di modesto interesse quali, a esempio, le *vending machine*, e dall'altro procedure computerizzate sprovviste tuttavia di un disegno progettuale fondamentale per un regolamento di autonomia privata⁹⁰. Proprio in considerazione di ciò si è delineata una diversa definizione di *smart contract*, la quale lo identifica con una sequenza di codice computerizzato inserita in una blockchain suscettibile di essere attivata dalle operazioni economiche le quali si svolgono all'interno della stessa e di elaborare le informazioni del database digitale decentralizzato sulla quale si basa la sua struttura⁹¹. Così è possibile definire lo *smart contract* come «l'insieme di clausole, espressione di un accordo di due o più parti, programmate in codice alfanumerico [...] [il quale codice] viene conservato sulla blockchain»⁹², definizione la quale è stata sostanzialmente riprodotta nell'art. 8 – *ter*, l. 12 febbraio 2019, n. 12 il quale prevede che «Si definisce “*smart contract*” un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse», il che rende possibile che tutti i contratti possano essere resi *smart* attraverso il collocamento degli stessi nei blocchi»⁹³. Parte degli studiosi ha inoltre affermato che «Il libro mastro digitale condiviso rappresenti la nuova frontiera dell'innovazione digitale, destinata a ridefinire gran parte degli assetti fin qui conosciuti, sarà lecito presupporre che proprio lì vada cercata quella che qualcuno ha voluto definire la “*contract law 2.0*”»⁹⁴.

È da evidenziare che in forza dell'incertezza sull'evoluzione del fenomeno muta considerevolmente anche la prognosi della disciplina giuridica da enucleare in tema. Se alcuni sostengono che il processo di informatizzazione e automazione dei contratti abbia caratteristiche e potenzialità rilevanti in grado di prevedere le variabili ad alto tasso di responsività⁹⁵, altri contrappongono riserve basate sullo scetticismo nei confronti della capacità delle tecnologie applicate ai contratti di ricomprendere le molteplici fattispecie proprie della contrattualistica tradizionale⁹⁶. La medesima divergenza di opinioni

⁹⁰ PARDOLESI, DAVOLA, «Smart contract»: *lusinghe ed equivoci dell'innovazione purchessia*, in CAPRIGLIONE (a cura di), *Liber amicorum Guido Alpa*, Milano, Cedam, 2019, p. 302.

⁹¹ *Ibidem*.

⁹² PAROLA, MERATI, GAVOTTI, *Blockchain e smart contract: questioni giuridiche aperte*, in *Contratti*, 2018, 681 ss.

⁹³ GANS, *The fine print in smart contracts*, in www.nber.org, 2019.

⁹⁴ SAVELYEV, *Contract law 2.0: “smart” contract as the beginning of the end of classic contract law*, in *Information & communication technology law*, 116, 2017.

⁹⁵ BUTERIN, *A next generation smart contract and decentralized application platform*, in *White paper*, GitHub.

⁹⁶ DRUCK, “Smart contract” are neither smart nor contract, 37/10, in *Banking financial services*

è riscontrabile nell'individuazione delle criticità di maggior rilievo le quali possono riscontrarsi nell'evoluzione dello *smart contract*. In tema si sono ipotizzati i problemi di *governance* in materia di *smart contract*, sia in riferimento al controllo esercitabile da parte dell'autorità pubblica che all'impatto esercitato sulle tradizionali strutture di esercizio del potere della stessa⁹⁷.

La letteratura in materia si concentra sugli effetti della tecnologia nella regolazione dei rapporti tra privati, in considerazione dei rischi e delle opportunità emergenti soprattutto in riferimento al problema identitario, ovvero se gli *smart contract* possano qualificarsi alla stregua di veri e propri regolamenti di autonomia privata, o se piuttosto con tale locuzione si indichi semplicemente un codice contrattualistico preesistente il quale, invece di operare con le tradizionali tecnologie, interagisce con la *blockchain*⁹⁸. La questione è dirimente, e lo spartiacque è rappresentato dalla riconducibilità dello *smart contract* nell'area dei contratti in senso proprio⁹⁹, o della qualificazione degli stessi quali protocolli tecnologici di trasferimento¹⁰⁰, ove in quest'ultimo caso non si avrebbero rilievi giuridici immediati¹⁰¹.

Tale ultima considerazione contrasta con l'opinione secondo la quale gli *smart contract* rappresenterebbero uno strumento in grado di ridefinire gli assetti dello scambio nel mondo digitale, pertanto non considerandoli uno strumento in grado di limitare la discrezionalità dei privati¹⁰², negandone inoltre la differenziazione "biologica" rispetto alla contrattualistica tradizionale¹⁰³ e escludendo che tale categoria nominalistica possa giustificare l'introduzione di una disciplina del consumatore maggiormente garantisca, in quanto il consumatore dotato di nuove risorse di contrattazione online può eliminare le asimmetrie informative le quali caratterizzano la materia¹⁰⁴. Sembra tuttavia ovvio¹⁰⁵ interrogarsi sulla compatibilità degli *smart contract* quale realtà di fatto con la disciplina di diritto positivo prevista in materia di contratti, soprattutto in riferimento alla normativa

⁹⁷ Vedi WRIGHT, DE FILIPPI, Decentralized blockchain technology and the rise of lex cryptographia, in ssrn.com; REIJERS, O'BROLCHAIN, HAYNES, Governance in blockchain technologies & social contract theories, Ledger, 2016.

⁹⁸ GREENSPAN, Beware of the impossible smart contract, in www.the-blockchain.com, 2016.

⁹⁹ ALLEN, WIDDISON, Can computer make contracts?, Harv. J. Law and technology, 25, 1996.

¹⁰⁰ STARK, Making sense of blockchain smart contracts, in www.coindesk.com.

¹⁰¹ PARDOLESI, DAVOLA, «Smart contract», cit.

¹⁰² SWANSON, Great chain of numbers: a guide to smart contracts, smart property and trustless asset management, 2014, 14.

¹⁰³ HOLDEN, MALANI, Can blockchain solve the holdup problem in contracts?, University of Chicago Coase – Sandor institute for law & economics research, p. n. 846, 2017, in ssrn.com.

¹⁰⁴ FAIRFIELD, Smart contracts, bitcoin bots, and consumer protection, Washington and lee law review online, 2, 2014, in www.scholarlycommons.law.wlu.edu.

¹⁰⁵ PARDOLESI, DAVOLA, «Smart contract», cit., p. 307.

in tema di interpretazione del contratto¹⁰⁶, dell'effettività del consenso espresso dalle parti nel caso di prestazione c.d. dinamiche¹⁰⁷, dell'allocazione della responsabilità nel caso di malfunzionamento del contratto¹⁰⁸, e dei casi di riconducibilità di tale ultima fattispecie nei casi di inadempimento o caso fortuito¹⁰⁹.

Sembra pertanto che se tali codici variamente automatizzati non vengono qualificati come contratti, individuandoli esclusivamente come mere neo – fattispecie concrete del diritto moderno sussumibili alla disciplina vigente, si perda l'*ubi consistam* della categoria stessa¹¹⁰.

2. La blockchain.

Internet e lo sviluppo della tecnologia rende possibile comunicare a distanza con chiunque, ovunque si trovi nel mondo, per scopi personali e commerciali, il che determina una massiccia circolazione di dati sul web. Tali dati vengono normalmente utilizzati dalle aziende che li acquistano per scopi di profilazione, creando pubblicità personalizzate o mirate a orientare la scelta del consumatore¹¹¹. Il mercato dei dati sul web è in costante crescita raggiungendo, in ottica previsionale, gli 84 miliardi di euro/dollari entro il 2020¹¹².

La tecnologia della *blockchain*¹¹³ si sviluppa nell'ambito di un processo il quale trae le proprie origini negli Anni 90' ove si è iniziato lo studio delle reti c.d. *peer – to – peer* e della crittografia. La *blockchain*, inizialmente, si è sviluppata nell'ambito delle c.d. criptovalute, prima tra tutte il *Bitcoin* di

¹⁰⁶ Cfr. CASEY, NIBLETT, Self – driving laws, University of Toronto law journal, 2016, 429.

¹⁰⁷ Si veda CHIERICI, *Gli smart contract: profili giuridici con una struttura informatica*, 2018, in www.salvisjuribus.it.

¹⁰⁸ V. in tema KOLBER, Not – so – smart blockchain contracts and artificial responsibility, in Stan. Tech. L. rev., 2018, 198.

¹⁰⁹ CAGGIANO, *Il contratto nel mondo digitale*, in *Nuova giur. civ.* 2018, 1152.

¹¹⁰ Così PARDOLESI, DAVOLA, «Smart contract», cit., p. 308, il quale rimanda a LIPSHAW, The persistence of “Dumb” contracts, in www.ssrn.com, 2018.

¹¹¹ DEFILIPPI, The interplay between decentralization and privacy: the case of blockchain technologies, CERSA-CNRS-Université Paris II, Berkman Center for Internet & Society at Harvard, 2016, 2 ss.

¹¹² BARLOW, A Declaration of the Independence of Cyberspace, in www.eff.org/it/cyberspaceindependence, 1996.

¹¹³ GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'Informazione e dell'Informatica*, 2019, 6, 989; F. DI CIOMMO, *Smart contract e (non-) diritto. Il caso dei mercati finanziari*, in *Nuovo diritto civile*, 2019, 1, 257 ss.; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 2018, 2, 441; IDELBERGER, Connected contracts reloaded - smart contracts as contractual networks, in S. GRUNDMANN (a cura di), *European Contract Law in the Digital Age*, Intersentia, 2018, 205 ss.; MIK, Smart contracts: terminology, technical limitations and real world complexity, in *Law, Innovation and Technology*, 2017, vol. 9, n. 2, 269; SAVELYEV, Contract Law 2.0: “Smart” contracts as the beginning of the end of classic contract law, in Higher School of Economics Research Paper n. WP BRP 71/LAW/2016.

Nakamoto, il quale ha rappresentato la prima valuta virtuale pensata per effettuare pagamenti online da un soggetto direttamente verso un altro, senza la necessità di dover usufruire del servizio di un intermediario finanziario o di una banca, ovviando a tutte le criticità che l'operato di quest'ultimi implicano, sebbene vengano meno anche le tutele e le garanzie che gli stessi sono in grado di fornire¹¹⁴. La *blockchain*, sulla quale opera il sistema dei *bitcoin* e delle criptovalute, elude il problema del c.d. double spending money, ovvero la doppia spendita dello stesso importo di denaro senza la necessità di ulteriori garanzie di terzi¹¹⁵. Il fenomeno, iniziato nel gennaio del 2009, ha infatti avuto un successo esponenziale, potendosi attualmente contare più di 1600 *alternative coins* all'interno della *blockchain*¹¹⁶.

La *blockchain* può essere il luogo informativo dove è possibile registrare non solo criptovalute ma qualsiasi tipo di dato, come informazioni personali e accordi contrattuali¹¹⁷, derivando che le *decentralised applications* della *blockchain* possono essere almeno pari nel numero al tipo di informazioni circolanti nel mondo ogni giorno¹¹⁸. In tal senso il Parlamento europeo ha affermato che la *blockchain* «[...] può costituire uno strumento che rafforza l'autonomia dei cittadini dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati [...] »¹¹⁹.

La *blockchain* è un *database* distributivo, il quale contiene caratteristiche di tecnologie preesistenti quali i sistemi distributivi e la crittografia asimmetrica. Il sistema distributivo si pone quale alternativa al modello *client – server* nel quale le informazioni transitano dal *server* diramandosi in forza dei *downloads* dei *clients*, ove i dati vengono posizionati in una serie di computer, i “nodi”, in una posizione di parità¹²⁰.

Il termine “*blockchain*” è stato coniato sulla base della modalità di funzionamento del sistema stesso, il quale prevede che le transazioni vengano cronologicamente organizzate, tramite dei *server* di marcatura temporale, i *timestamps*, mediante una divisione in blocchi identificati tramite una stringa

¹¹⁴ Si veda PAGLIERY, *Bitcoin and the future of money*, Triumph books, Chicago, 2014.

¹¹⁵ CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè, 2015, p. 35 – 36.

¹¹⁶ Il dato è fornito da CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova Giur. Civ.*, 2017, I, 107 ss.

¹¹⁷ SWAN, *Blockchain, Blueprint for a New Economy*, O'Reilly, 2015, 23.

¹¹⁸ BOUCHER, *How blockchain technology could change our lives*, European Parliamentary Research Service, 2017, 6 ss.

¹¹⁹ V. GAMBINO, BOMPRESZI, *Blockchain e protezione dei dati personali*, in *Diritto dell'Informazione e dell'Informatica* (II), fasc.3, 2019, p. 619.

¹²⁰ *Ibidem*.

alfanumerica, l'*hash*, il quale include sempre l'*hash* del blocco precedente, fino a formare una concatenazione di blocchi, la *blockchain* per l'appunto¹²¹. La struttura della *blockchain* da ultimo descritta rende piuttosto difficile ogni tentativo di frode, in quanto la modifica di un solo *hash* inciderebbe sull'intera catena, modificando anche gli *hash* collegati, palesandosi una manipolazione in forza del contrasto con gli altri "nodi" all'interno del *network*¹²².

In tal senso si è parlato dell'immutabilità unilaterale della *blockchain*¹²³. Quanto alla crittografia asimmetrica questa rileva al fine dell'inserimento dei dati all'interno della *blockchain*, i quali dati possono essere decriptati solo dal chi detiene la relativa chiave di lettura, il che è funzionale al mantenimento della trasparenza all'interno della *blockchain*, la quale può funzionare mantenendo un certo grado di riservatezza. «La crittografia asimmetrica si basa su un sistema a doppia chiave pubblico/privata. La chiave pubblica coincide con l'account dell'utente, ed è conosciuta da tutti; ad essa è abbinata una chiave privata, che rimane segreta. In questo modo, i messaggi destinati ad un particolare soggetto vengono criptati con la sua chiave pubblica, affinché possa accedervi con la propria chiave privata, che non necessita di essere condivisa»¹²⁴.

L'immutabilità della *blockchain* alla quale si è fatto riferimento, unitamente all'utilizzo della crittografia, fa sì che molti denotino la sicurezza della stessa, ove l'aggiunta di un nuovo "blocco" avviene da parte di "nodi" a ciò predeterminati, i c.d. *validation nodes*, sulla base delle regole prestabilite dal protocollo informatico e condivise dal *network*. «La modalità più conosciuta prende il nome di "*Proof of Work*" (*PoW*), e consiste in una competizione tra nodi (*miners*); il primo tra questi che risulti capace di risolvere un complesso problema matematico, trovando un *hash* che sia composto da un numero predeterminato di zeri nella parte iniziale, è legittimato ad inserire un nuovo blocco e a ricevere una ricompensa per il lavoro svolto.

¹²¹ BELLINI, *Blockchain & Bitcoin*, Milano, 2018.

¹²² Si veda COMELLINI, VASAPOLLO, *Blockchain, criptovalute, I.C.O. e smart contract*, Maggioli, 2019; PERUGINI, *Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni*, Key editore, 2018; NICOTRA, SARZANA, DiSANT'IPPOLITO, *Diritto della blockchain, intelligenza artificiale e IoT*, Ipsoa, 2018. BASHIR, *Mastering blockchain*, Packt, 2018.

¹²³ AA. VV., *Smart contracts as a specific application of blockchain technology*, Smart contract Working Group, Dutch Blockchain Coalition, in www.ducthblockchain.coalition.org.

¹²⁴ GAMBINO, BOMPRESZI, *Blockchain e protezione dei dati personali*, cit.; v. anche FINOCCHIARO, *Firme elettroniche e firma digitale*, in DELFINI, FINOCCHIARO, *Diritto dell'informatica*, UTET, 2014, 309; ID. *Tecniche di imputazione della volontà negoziale: le firme elettroniche e la firma digitale*, in CLARIZIA (a cura di), *I contratti informatici*, in RESCIGNO, GABRIELLI (diretto da), *Trattato dei contratti*, UTET, 2007, 201; GAMBINO, voce *Informatica giuridica e diritto dell'informatica*, in *Diritto online*, Treccani, 2013; ID., voce *Firma elettronica*, in *Enc. giur. Treccani*, Roma, 2004.

Alla *PoW* se ne aggiungono molte altre, come *Proof of Stake*, *Proof of Capacity*, *Proof of Activity*, etc.

La scelta dipende in gran parte dalla tipologia di *blockchain* utilizzata: nelle *blockchain* pubbliche e *permissionless*, ad esempio, la *PoW* è la più appropriata, poiché la sfida tra nodi e la previsione di remunerazioni per il lavoro svolto incentiva i partecipanti a mettere a disposizione la potenza computazionale dei propri dispositivi informatici per far funzionare il sistema, cosa che altrimenti risulterebbe difficile in assenza di un gestore»¹²⁵.

Sebbene la *blockchain* non abbia, tutt'ora, dei precisi *standard* predefiniti ai fini della sua implementazione, è possibile operare una sommaria ma principale distinzione in tema, ovvero tra *blockchain* di tipo *permissionless* o *blockchain permissioned*. Le principali differenze risiedono nell'identificabilità dei soggetti i quali ne fanno uso, la modalità di selezione dei "nodi" e la grandezza del *network*, le particolarità relative al meccanismo del consenso condiviso e la trasparenza del contenuto dei blocchi¹²⁶.

«Nelle *blockchain permissionless* (come ad esempio Bitcoin), ciascuno può entrare a far parte del *network*, ed ogni computer può fungere da nodo; pertanto, il *network* può crescere a dismisura, e conseguentemente il meccanismo del consenso rende questo tipo di *blockchain* immutabili, essendo praticamente impossibile (perché richiederebbe un'enorme potenza computazionale e l'accordo tra il 50% più uno dei nodi) qualsiasi forma di modifica. Infine, ogni utente può visualizzare l'intera *blockchain*, per cui il grado di trasparenza è massimo. Le *blockchain permissioned* sono caratterizzate da una maggiore centralizzazione, perché un'entità centrale ha l'autorità di determinare chi può accedervi, dietro preidentificazione.

Il fatto che le identità che si celano dietro i nodi siano conosciute e che gli accessi siano controllati diminuisce il livello di immutabilità, posto che in astratto il raggiungimento della maggioranza necessaria per apportare cambiamenti è più semplice. Anche la trasparenza può essere diminuita, potendo escludere determinati nodi dalla visione integrale della *blockchain*»¹²⁷. Un'ulteriore importante differenza tra la *blockchain* pubblica e quella privata riguarda la gestione dell'infrastruttura informatica. La *blockchain* pubblica, difatti, non è gestita da nessun soggetto, creandosi in tal caso man mano che i soggetti si aggiungono al *network*.

¹²⁵ GAMBINO, BOMPRESZI, *Blockchain e protezione dei dati personali*, cit.; v. anche COMELLINI, VASAPOLLO, *Blockchain, criptovalute*, cit., p. 98 ss.

¹²⁶ MAXWELL, SALMON, *A guide to blockchain and data protection*, Hogan Lovells, 2017, in www.hoganlovells.com.

¹²⁷ GAMBINO, BOMPRESZI, *Blockchain e protezione dei dati personali*, cit.

La *blockchain* privata, invece, è istituita e gestita da una singola organizzazione o persona, le quali rappresentano « [...] poco più di un sistema centralizzato tradizionale [...] »¹²⁸ il quale può beneficiare delle caratteristiche di sicurezza nei confronti dell'esterno proprie della *blockchain*. Di norma, inoltre, le *blockchain* pubbliche sono anche *permissionless*, ma possono anche essere *permissioned* nel caso in cui venga richiesta una preidentificazione in ingresso¹²⁹.

Le caratteristiche descritte dovranno innanzitutto conciliarsi con i principi fissati nel GDPR, direttamente applicabile in tutti gli Stati membri, e con le norme contenute nel codice della *privacy*, recentemente adeguato al citato Regolamento, con il d.lgs. 10 agosto 2018, n. 101¹³⁰. La normativa citata stabilisce che il trattamento dei dati personali deve essere lecito, equo e trasparente, limitato allo scopo specifico per il quale sono stati originariamente raccolti, contemplando tra gli stessi solo i dati assolutamente necessari allo scopo specifico, applicando la c.d. minimizzazione dei dati). I dati devono inoltre essere accurati e aggiornati, non conservati più a lungo del necessario e devono essere elaborati in modo sicuro, secondo i principi di integrità e riservatezza¹³¹.

Parte degli studiosi ha affermato che « [...] alcuni dei principi stabiliti dal Regolamento trovano sicura tutela nella *blockchain*, se si considera che tale tecnologia, è decentralizzata e distribuita e questo rende molto più difficile un attacco di *cybercrime*; le informazioni sulle transazioni, quali l'identità dei soggetti e gli altri dati personali, sono, come detto, pseudonimizzate, ancorché pubbliche e, quindi, noti agli altri nodi; la crittografia utilizzata, in linea di principio, garantisce un metodo

¹²⁸ BUTERIN, On Public and Private Blockchains, Ethereum Blog, 2015, in <https://blog.ethereum.org/>.

¹²⁹ BASHIR, Mastering blockchain, cit.

¹³⁰ NICOTRA, Blockchain e GDPR: le norme da conoscere per tutti i problemi, 24 luglio 2018, in <https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/>.

¹³¹ Cfr. art. 5 GDPR, «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»)). Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»)).

piuttosto sicuro per archiviare e gestire le informazioni»¹³², tuttavia «altri principi fissati nella normativa europea che difficilmente potranno essere rispettati, come quello che sancisce il diritto alla cancellazione dei dati personali (c.d. diritto all'oblio) o anche alla loro rettifica, stante il carattere immodificabile della *blockchain*.

A parte l'utilizzo di tecniche per anonimizzare i dati trattati nella *blockchain*, come nel caso di utilizzo di una coppia di chiavi per ciascuna transazione da parte del medesimo soggetto, ad oggi la tecnologia in esame non consente l'esercizio di un tale diritto»¹³³. Rilevante è inoltre la questione sull'individuazione dei soggetti nei confronti dei quali gli utenti devono rivolgersi per chiedere il rispetto dei principi fissati a tutela dei loro dati, il che evidenzia l'importanza del tema della *governance* della *blockchain*, il quale è influenzato dalla distinzione della tipologia pubblica o privata del sistema cui si fa riferimento¹³⁴.

¹³² GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'Informazione e dell'Informatica* (II), fasc.6, 2018, p. 989.

¹³³ *Ibidem*, il quale si riferisce a NICOTRA, SARZANA, DiSANT'IPPOLITO, *Diritto della blockchain*, cit., p. 89.

¹³⁴ V. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, cit., il quale afferma che « [...] affrontando il problema dell'individuazione dei soggetti destinatari della legislazione privacy, non vi è dubbio che nelle blockchain del tipo consorzio o private, data la loro caratteristica strutturale, porterebbe senz'altro ad individuare nel soggetto/i validatore/i del consenso il titolare del trattamento o il responsabile del trattamento, nei casi in cui questi gestisce il dato per conto del titolare. Diversa, invece, è la conclusione se si guarda la blockchain pubblica, caratterizzata da un contesto fortemente decentralizzato, nella quale sembra al quanto arduo identificare uno più soggetti che abbiamo un controllo sui dati registrati nel ledger. [...] Volendo trarre una prima conclusione, nelle fattispecie “pure” di blockchain, data la loro architettura completamente aperta, occorre guardare più che altro all'utente/nodo che immette i dati nella blockchain e il suo ruolo rispetto ai dati che gestisce. Detto nodo potrà, infatti, assumere la qualifica di titolare se determina le finalità e i mezzi del trattamento di dati personali, o di responsabile se tratta, invece, i dati personali solo per conto del titolare del trattamento. A tale scopo occorre considerare che l'art. 2 del regolamento esclude la sua applicazione nel caso di trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Inoltre, stante il carattere immodificabile del contenuto dei blocchi della blockchain, problemi di compatibilità con il Regolamento sorgono in ordine al diritto alla cancellazione di quei dati che siano stati immessi nel sistema e dove nessuno ha né il potere né il diritto di manipolare o cancellare in tutto in parte. L'utente, dunque, che si trovasse a operare in un tale sistema, nell'ottica di un principio di autoreponsabilità, dovrebbe aver valutato i rischi che tale tecnologia comporta e accettato le limitazioni ad alcuni diritti che, nel caso in esame, la regolamentazione sulla protezione dei dati gli attribuisce, in ragione della tecnica in uso in un dato momento storico».

CAPITOLO III

L'INNOVAZIONE TECNOLOGICA NELLA MATERIA BANCARIA E FINANZIARIA

1. *Fintech.*

La crescente e preponderante innovazione tecnologica connessa allo sviluppo di *internet*, avviatasi durante il secolo scorso, ha sollevato all'attenzione dell'interprete giuridico questioni connesse alla *cybernetica* e all'informazione mediatica. Le riflessioni in tal senso dapprima si mossero nel descrivere le caratteristiche del mondo virtuale e in particolare le modalità organizzative dello stesso¹³⁵, e successivamente si soffermarono in ambito finanziario, con riferimento alla globalizzazione dei mercati, all'automatizzazione delle risorse umane operanti nelle banche, alla negoziazione dei contratti a distanza, alle questioni inerenti alla proprietà intellettuale e, in generale, alla riorganizzazione dell'intera materia la quale si mostrò fin da subito ontologicamente sensibile al fenomeno *cybernetico*¹³⁶. Ciò in quanto non può intendersi *internet* esclusivamente quale serie coordinata di fenomeni tecnologici, identificando una nuova formula della comunicazione per la quale è necessario procedere a una codificazione della *cyber law*¹³⁷, respingendo le concezioni che ne descrivono solo una parte o un aspetto¹³⁸. La *cyber law*, infatti, nella sua dimensione privatistica intrattiene rapporti concettuali con diversi ambiti del settore del mercato, inteso sia quale spazio ideale autonomo qualificato dall'assoluta libertà di azione sia come spazio ideale nel quale devono essere dettate regole giuridiche strutturali destinate a limitare tale libertà, come a esempio l'autodisciplina, la deontologia, la convenzionalità¹³⁹.

L'attuale configurazione dei processi connessi all'innovazione tecnologica, soprattutto in riferimento all'ambito finanziario, denota un radicale cambiamento rispetto al passato delle forme operative

¹³⁵ Si veda ALPA, *Il contratto in generale, I, Fonti, teorie, metodi*, in CICU, MESSINEO, MENGONI, SCHLESINGER (a cura di), *Tratt. Dir. civ. comm.*, Milano, 2014, p. 219 ss.

¹³⁶ In tema ALPA, *Il contratto del terzo millennio: intervento conclusivo*, in *Nuova giur. civ. comm.*, 2018, n. 7 – 8, 1158.

¹³⁷ PELLEGRINI, *Il diritto cybernetico nei riflessi sulla materia bancaria e finanziaria*, in CAPRIGLIONE, *Liber amicorum*, cit., p. 352.

¹³⁸ ALPA, *Cyber law. Problemi giuridici connessi allo sviluppo di internet*, in *Nuova giurisprudenza civile commentata*, 1998, 6, II, p. 385 ss.

¹³⁹ ALPA, *Le stagioni del contratto*, Bologna, 2012.

recate dal *Fintech*¹⁴⁰. La rivoluzione tecnologica inerente ai prodotti e agli strumenti finanziari ha innovato l'operatività del mercato configurando nuove piattaforme negoziali virtuali, e nuove modalità di relazione tra soggetti le quali «[...] pongono in tensione i confini tra intermediari emittenti e mercati sino a renderli evanescenti»¹⁴¹.

Il processo evolutivo tecnologico ha infatti delineato forme operative nuove e distinte dai canoni tradizionali creando relazioni intersoggettive a distanza, «dalla *Techfin* si è dunque passati alla *Fintech*, cioè allo sfruttamento nel modo più profittevole e sicuro delle nuove tecnologie articolato in un nuovo mondo che implica il ruolo, le competenze e il controllo comportamentale di nuovi soggetti, tendenzialmente intermediari, la realizzazione di nuovi mercati di beni e servizi, nuovi rapporti con i destinatari dei beni e dei servizi, i consumatori-*retailers*, la creazione di nuove autorità di controllo o l'estensione dei poteri delle autorità esistenti a livello nazionale, europeo o internazionale, e quindi nuovi studi in cui le applicazioni tecniche sono rielaborate nella prospettiva scientifica, quella giuridica in *primis*, con tutto l'apparato conseguente: un nuovo vocabolario, nuovi concetti, nuove discipline»¹⁴². Ciò pertanto conduce al ridimensionamento delle funzioni delle autorità di controllo di settore e al progressivo allontanamento dell'*agere* finanziario al di fuori dei tradizionali luoghi fisici di negoziazione il che, nel segno della riduzione dei costi di transazione dell'intermediazione in genere, favorisce la promozione di piattaforme informatiche per le negoziazioni alternative all'interno dei mercati finanziari, le quali valorizzano il controllo diffuso delle transazioni e la totale disintermediazione delle operazioni finanziarie, affidate spesso a sistemi algoritmici di scambio automatico¹⁴³, tutti fattori di efficienza e democraticità¹⁴⁴.

Se non è dubbio il fatto che il mercato digitale aumenta la produttività e il consumo, per altro verso deve evidenziarsi la necessità che lo stesso venga regolato da una disciplina idonea a supportare l'espansione informatica, in considerazione del fatto che l'applicazione di modelli digitali all'interno del mercato, fondano lo stesso sulla libera circolazione dei capitali e sulla possibilità di effettuare investimenti senza frontiere, e determinando una spersonalizzazione dei rapporti negoziali, ha indotto

¹⁴⁰ Con il termine “*Fintech*” si fa riferimento, sebbene il consenso non sia unanime, alla “nuova industria finanziaria che applica la tecnologia per migliorare le attività finanziarie”, si veda in tal senso SCHUEFFEL, Taming the Beast: A Scientific Definition of Fintech, in *Journal of Innovation Management*, vol. 4, n° 4, 9 marzo 2017, pp. 32–54.

¹⁴¹ TROIANO, *Fintech tra innovazione e regolamentazione*, Relazione al Convegno “*Fintech*: prime esperienze e prospettive di regolamentazione”, Università La Sapienza, Roma, 4 dicembre 2017, p. 7.

¹⁴² ALPA, *Fintech: un laboratorio per i giuristi*, in *Contratto e Impr.*, 2019, 2, 377.

¹⁴³ PAECH, The governance of blockchain financial networks, in *Modern law review*, 2017, 1073 – 1110.

¹⁴⁴ LEE, CHEN, LOW, *Inclusive Fintech: blockchain, cryptocurrency and ICO*, Word scientific, 2018.

l'enucleazione dei c.d. scambi senza accordo¹⁴⁵. Ne consegue la necessità di rivisitare l'ambito degli organismi di controllo, con l'individuazione di regole per gli istituti bancari che consentano agli stessi di effettuare penetranti verifiche sulle attività portate a conoscenza degli amministratori degli stessi¹⁴⁶.

Attualmente si registrano perplessità¹⁴⁷ nei riguardi del regime di *soft law*, di stampo UE¹⁴⁸, volto alla realizzazione di un quadro normativo inerente alle transazioni in rete degli agenti di mercato.

Una figura intermedia tra le nuove piattaforme virtuali e i tradizionali perimetri regolamentari è rappresentata dai cc.dd. *sandbox*¹⁴⁹, i quali palesano i problemi relativi alla validità esterna di tali esperimenti e all'incertezza dei sistemi normativi a termine¹⁵⁰.

Fintech è stato definito un laboratorio per il giurista¹⁵¹ sia per lo sviluppo dell'apparato normativo che ne è conseguito a opera delle istituzioni europee e del legislatore nazionale, sia più specificatamente per le innovazioni nel diritto civile. Per quanto riguarda il primo degli aspetti citati, quanto al diritto europeo è opportuno citare, tra i diversi documenti normativi, il «Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo»¹⁵² ove la Commissione ha affermato che «le tecnologie finanziarie rappresentano il punto di incontro dei servizi finanziari e del mercato unico digitale. Il settore finanziario è il principale utilizzatore delle tecnologie digitali e un importante motore della trasformazione digitale dell'economia e della società. Vi sono importanti sinergie tra la strategia della Commissione per il mercato unico digitale, la strategia dell'UE per la

¹⁴⁵ IRTI, *Scambi senza accordo*, in *Riv. trim. di dir. e proc. civ.*, 52, 1998, 347 ss.

¹⁴⁶ Cfr. ENRIQUES, *Financial supervision and regtech: four roles and four challenges*, in *Revue trimestrielle de droit financier*, 53, 2017.

¹⁴⁷ PELLEGRINI, *Il diritto cybernetico nei riflessi sulla materia bancaria e finanziaria*, cit., p. 356.

¹⁴⁸ Vedi Comunicazione Commissione, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, Bruxelles, 8 marzo 2018, COM(2018), 109 final.

¹⁴⁹ BROMBERG, GODWIN, RAMSAY, *Fintech, sandboxes: achieving a balance between regulation and innovation*, in *Journal of banking and finance law and practice*, 2017, 4, 314 – 336. V. anche ALPA, *Fintech: un laboratorio per i giuristi*, cit., il quale riporta la seguente definizione di *sandbox* «In ambito informatico, una nuova applicazione o una modifica ad una applicazione esistente viene prima sviluppata nell'ambiente di sviluppo (*development environment*), poi testata in un ambiente apposito (*test environment*), infine verificato il corretto funzionamento in un ambiente di qualità (*quality environment*), in cui siano presenti dati copiati recentemente da un ambiente di produzione (*live environment* o *production environment*), per poi essere trasferita definitivamente nell'ambiente di produzione. I dati copiati dalla produzione all'ambiente di qualità, se del caso sono trattati al fine di non esporli per esteso in un ambiente che solitamente non ha le adeguate caratteristiche di sicurezza. Il termine *sandbox* identifica normalmente un ambiente estraneo, diverso da quelli elencati, in cui possono essere fatte sperimentazioni che potrebbero non portare neppure ad aprire una fase di sviluppo, e il cui scopo è quello di investigare sugli effetti di eventuali modifiche o sviluppi che sono ancora nella fase di “studio della fattibilità” o di “analisi costibenefici”».

¹⁵⁰ V. Report *Fintech: regulatory sandboxes and innovation hubs*. JC 2018/74, ESMA, EBA, EIOPA, gennaio 2019, in www.esma.europa.eu.

¹⁵¹ ALPA, *Fintech: un laboratorio per i giuristi*, cit.

¹⁵² Comunicazione della Commissione, 2018, in eur-lex.europa.eu.

cibersicurezza, il regolamento eIDAS e le iniziative per i servizi finanziari come il piano d'azione per i servizi finanziari ai consumatori e la revisione intermedia dell'Unione dei mercati dei capitali (UMC)». Vi è inoltre la Risoluzione del Parlamento europeo del 17 maggio 2017 sulla tecnologia finanziaria¹⁵³, la nuova disciplina recata dalla direttiva sui pagamenti elettronici (PSD2) integrata dal Regolamento delegato n. 2018/389, in collegamento con MIFID2, e la riforma del regolamento *ePrivacy*¹⁵⁴.

Quanto alle innovazioni proprie del diritto civile la Risoluzione del Parlamento europea citata invita la Commissione ad applicare alcuni principi generali al fine della realizzazione di un mercato unico digitale, quali "stessi servizi e stessi rischi", secondo il quale si dovrebbero applicare le stesse norme indipendentemente dal tipo di entità giuridica interessata o dalla sua ubicazione nell'Unione; la neutralità tecnologica; un approccio basato sui rischi, tenendo conto della proporzionalità delle azioni legislative e di vigilanza rispetto ai rischi e della rilevanza dei rischi¹⁵⁵. Il Parlamento ha inoltre invitato la Commissione a implementare le regole sulla concorrenza, a promuovere l'ingresso nel mercato di *start up*, a limitare il potere dei c.d. *Big Data*, a favorire lo sviluppo tecnologico nel settore finanziario e, per quanto riguarda i consumatori, ha segnalato « [...] la necessità di sviluppare una maggiore consapevolezza tra i consumatori riguardo al valore dei loro dati personali; osserva che i consumatori possono stipulare contratti per la condivisione dei contenuti digitali in cambio del pagamento di una commissione; sottolinea che ciò può tradursi in vantaggi economici ma può anche essere usato in modo discriminatorio; invita la Commissione a valutare la possibilità di approntare una strategia europea sulla condivisione dei dati allo scopo di dare ai consumatori il controllo dei loro dati; ritiene che un approccio chiaro e incentrato sui consumatori migliorerà la fiducia nei servizi basati sul cloud e stimolerà i nuovi servizi innovativi offerti dai diversi soggetti della catena del valore finanziario, ad esempio utilizzando le interfacce per programmi applicativi (API) o facilitando l'accesso diretto ai dati per i servizi di pagamento elettronici; invita la Commissione a valutare le potenzialità future dei sistemi di gestione delle informazioni personali quali strumenti tecnici con cui i consumatori gestiscono i loro dati personali»¹⁵⁶. Quanto alla *blockchain*, sempre il Parlamento con la Risoluzione citata, ha evidenziato « [...] le potenzialità delle applicazioni *blockchain* per il denaro contante e il

¹⁵³ In www.europarl.europa.eu.

¹⁵⁴ La disciplina nella sua organicità fa « [...] a norme tecniche, quindi ad una normativa di secondo grado che viene intesa come integrativa delle norme primarie, nonché a linee guida, che invece sono orientative, e hanno la funzione di valutare gli standard di comportamenti degli operatori», v. ALPA, *Fintech: un laboratorio per i giuristi*, cit.

¹⁵⁵ *Ibidem*.

¹⁵⁶ Ris. 2016/2243 INI, cit.

trasferimento di titoli, nonché per la facilitazione di “contratti intelligenti”, in quanto offrono un’ampia gamma di possibilità per entrambi i contraenti di un contratto finanziario, in particolare per quanto concerne le disposizioni sul finanziamento al commercio e sui prestiti alle imprese, inoltre hanno la possibilità di semplificare complesse relazioni contrattuali in ambito commerciale e finanziario tra imprese (B2B) e tra imprese e consumatori (B2C); sottolinea che le piattaforme *blockchain* sono inoltre adatte per la semplificazione di complesse transazioni B2B e B2C; e ovviamente invita la Commissione a promuovere la cultura delle tecnologie digitali anche per migliorare la posizione dei consumatori»¹⁵⁷. A quest’ultimi, come già accennato, è dedicato un “Piano d’azione” nel quale vengono analizzati i principali aspetti delle operazioni che i consumatori intraprendono con gli istituti bancari e finanziari e con i terzi, investendo pertanto in questioni di trasparenza e di commissioni delle operazioni transfrontaliere, i costi e i tassi di conversione della valuta, il trasferimento dei dati e dei conti bancari per agevolare il cambiamento dei fornitori dei servizi, il miglioramento dell’assicurazione degli autoveicoli, con i relativi principi di trasparenza, e si prendono in considerazione le direttive in materia di credito al consumo e di vendita a distanza di servizi finanziari, che dovrebbero essere aggiornate alla luce delle nuove tecnologie, insieme con l’agevolazione del credito transfrontaliero¹⁵⁸.

I principi ai quali l’intera disciplina descritta sono volti a promuovere l’accesso ai servizi finanziari per i consumatori e le imprese, ridurre i costi operativi e aumentare l’efficienza del settore, rendere più competitivo il mercato unico riducendo gli ostacoli all’accesso e bilanciare una maggiore condivisione e trasparenza in materia di dati con le esigenze di tutela della vita privata.

Prendendo quale paradigma la riforma europea in tema di *privacy*, fondante l’attuale GDPR, è opportuno evidenziare le finalità essenziali della stessa esposte nella Relazione introduttiva la quale afferma che «Il rispetto delle comunicazioni è un diritto fondamentale sancito dalla Carta. Il contenuto delle comunicazioni elettroniche può rivelare informazioni altamente sensibili relative agli utenti finali coinvolti nella comunicazione. Analogamente, i metadati derivati dalle comunicazioni elettroniche possono anch’essi rivelare informazioni estremamente sensibili e personali, come espressamente riconosciuto dalla CGUE. La maggioranza degli Stati membri riconosce inoltre l’esigenza di tutelare le comunicazioni come diritto costituzionale distinto. Anche se è possibile che gli

¹⁵⁷ *Ibidem*.

¹⁵⁸ Comunicazione della Commissione, cit.

Stati membri adottino politiche volte a garantire che tale diritto non sia violato, questo risultato non sarebbe uniforme in assenza di norme dell'Unione e si creerebbero restrizioni ai flussi transfrontalieri di dati personali e non personali connessi all'uso di servizi di comunicazione elettronica. Infine, per mantenere la coerenza con il regolamento generale sulla protezione dei dati, è necessario riesaminare la direttiva sulla vita privata elettronica e adottare misure atte ad allineare i due strumenti. [...]

Requisiti per un corretto funzionamento del mercato unico digitale sono eque condizioni per gli operatori di mercato che forniscono servizi sostituibili e un'identica tutela degli utenti finali a livello dell'Unione».

In particolare «Il capo II contiene le disposizioni principali volte a garantire la riservatezza delle comunicazioni elettroniche (articolo 5) e i fini limitati consentiti e le condizioni di trattamento dei dati di tali comunicazioni (articoli 6 e 7). Esso disciplina altresì la protezione delle apparecchiature terminali, i) garantendo l'integrità delle informazioni ivi conservate e ii) proteggendo le informazioni provenienti dall'attrezzatura terminale, in quanto possono consentire l'identificazione dell'utente finale (articolo 8). L'articolo 9 disciplina in modo particolareggiato il consenso degli utenti finali, un elemento lecito del presente regolamento, facente riferimento esplicito alla sua definizione e alle condizioni derivate dal regolamento generale sulla protezione dei dati, mentre l'articolo 10 impone un obbligo ai fornitori di programmi di comunicazione elettronica di aiutare gli utenti finali a definire in modo efficace le impostazioni relative alla vita privata. L'articolo 11 disciplina in modo particolareggiato le finalità e le condizioni in cui gli Stati membri possono restringere le predette disposizioni. Il capo III disciplina i diritti degli utenti finali a controllare l'invio e la ricezione di comunicazioni elettroniche per tutelare la propria vita privata: i) il diritto degli utenti finali di impedire la presentazione dell'identificazione della linea chiamante per garantire l'anonimato (articolo 12) e le relative limitazioni (articolo 13); e ii) l'obbligo imposto ai fornitori di comunicazione interpersonale basate sul numero pubblicamente disponibile di prevedere la possibilità di limitare il ricevimento di chiamate indesiderate (articolo 14). Questo capo disciplina altresì la condizioni alle quali gli utenti finali possono essere inclusi negli elenchi pubblici (articolo 15) e le condizioni alle quali si possono effettuare comunicazioni indesiderate a fini di commercializzazione diretta (articolo 17). Esso è altresì connesso ai rischi per la sicurezza contempla un obbligo per i fornitori di servizi di comunicazione elettronica di avvertire gli utenti finali in caso di rischio particolare suscettibile di compromettere la sicurezza della rete e dei servizi. Gli obblighi di sicurezza contenuti nel regolamento generale sulla

protezione dei dati e nel codice europeo delle comunicazioni elettroniche saranno applicabili ai fornitori di servizi di comunicazione elettronica».

Le implicazioni derivanti dal progresso tecnologico sui canali di distribuzione del credito, interessando la totalità dei settori sociali ed economici in maniera orizzontale interagisce con la struttura dei mercati, sulle strategie imprenditoriali e sui programmi e sulle modalità di investimento, il che determina un mutamento della logica concorrenziale e un diverso equilibrio dei fattori della domanda e delle relazioni economiche. Il cambiamento è intervenuto anche in riferimento alle tecniche meccanicistiche delle negoziazioni contrattuali¹⁵⁹ e, invero, tale processo nella diversificazione del tipo e della varietà dei prodotti disponibili, rappresentando un parametro di riferimento per l'individuazione delle forme assunte dal capitalismo nell'era della globalizzazione¹⁶⁰.

La questione della governabilità delle innovazioni *Fintech*, quali a esempio digitalizzazione, automazione, intelligenza artificiale, ha evidenziato problematiche relative alla corretta valutazione degli strumenti creditizi nelle operazioni commerciali su piattaforme digitali, le quali problematiche si moltiplicano in relazione a settori diversi quali, a esempio, la *privacy*, il mobile banking e la criminalità informatica¹⁶¹. L'utilizzo sempre maggiore di canali di distribuzione a distanza ha inoltre contribuito ad aumentare le incertezze in riferimento ai rischi di mercato a causa della mancanza di autorità di vigilanza *ad hoc* e, la possibilità di valutare nel merito il credito attraverso algoritmi, con modalità diverse rispetto alla previgente personalizzazione dei rapporti finanziari, se da un lato favorisce la circolazione di beni e risorse all'interno del mercato, dall'altro lato richiede un'approfondita conoscenza di sofisticate applicazioni informatiche¹⁶².

La disponibilità inoltre di *cluster*, di dati qualitativamente differenti da quelli tradizionalmente utilizzati per la valutazione del merito di credito, permette agli operatori del mercato di far riferimento a informazioni le quali sfuggono al dato normativo¹⁶³. Se da una parte, infatti, la possibilità di utilizzare algoritmi predittivi del rischio di *default* dei debitori, in grado di generare una

¹⁵⁹ V. *supra* Cap. II.

¹⁶⁰ CAPRIGLIONE, *Relazione al Seminario* "Globalizzazione intelligente. Riflessioni e spunti tratti dall'opera di Dani Rodrik", Università Luiss, Roma, 14 febbraio 2019.

¹⁶¹ KARAKAS, STAMEGNA, *Defining a EU – framework for financial technology (fintech): economic perspectives and regulatory challenges*, in *Law and economics yearly review*, 2018, p. 106 ss.

¹⁶² GESLEVICH PACKIN, LEV – ARETZ, *On social credit and the right to be unnetworked*, in *Columbia business law review*, 2016, 2, p. 401 ss.

¹⁶³ Si veda JAGTIANI, LEMIEUX, *Fintech lending: financial inclusion, Risk pricing, and alternative information*, in *FBR of Philadelphia working paper*, 2017, n. 17 – 17.

discriminazione del credito garantito e delle relative condizioni, e la possibilità di far riferimento a dati i quali possano garantire l'accesso al credito ai soggetti considerati "trasparenti", rappresentano innovazioni che incidono sul mercato, ampliandolo, dall'altro lato l'emersione di strategie alternative introduce nuovi rischi, i quali si riferiscono sia alla tutela dei dati utilizzati, sia in generale all'effetto discriminatorio, che ai vincoli di trasparenza e alla violazione della proprietà intellettuale e industriale¹⁶⁴.

È possibile affermare pertanto che a una riduzione delle distanze dovuta alla rivoluzione tecnologica e all'abbattimento dei costi di intermediazione corrispondono rischi non trascurabili e i limiti delle istituzioni internazionali¹⁶⁵, i quali ultimi aspetti citati evidenziano le criticità riferibili alla regolazione delle piattaforme informatiche, alla delocalizzazione delle negoziazioni e all'espansione del mercato globalizzato¹⁶⁶ governato dalle multinazionali.

Nel contesto descritto viene pertanto proposta la ricerca di nuove scelte interpretative della realtà socioeconomica e del sistema disciplinate lo stesso, volte all'individuazione di modalità organizzative efficienti fondate sulla razionalità e sulla correttezza. Si necessita pertanto di un criterio d'azione che gli Stati possano proiettare nel contesto internazionale il quale sia improntato alla trasparenza e al rispetto delle controparti, con professionalità degli intermediari deontologicamente predeterminata¹⁶⁷ e un sistema di controllo dei processi operativi e di calcolo automatizzati¹⁶⁸.

Da quanto finora emerso è possibile affermare che la costituzione del mercato globalizzato si basa sulle caratteristiche della cybernetica, nonché del diritto cybernetico, ove gli operatori affidano alle macchine l'attività di intermediazione¹⁶⁹. La globalizzazione inoltre agisce sia da catalizzatore e da impulso all'innovazione finanziaria, che da nuovo paradigma per gli scambi che avvengono nel mercato, il quale fonda un modello organizzativo digitale che dilata gli equilibri tra tutela del singolo e salvaguardia dei valori della collettività. In tal senso si assiste, in virtù dell'affermazione di un sistema

¹⁶⁴ PASQUALE, *The black – box society. The secret algorithms that control money and information*, Harvard University press, 2015.

¹⁶⁵ GETTER, *Consumer and credit reporting, Scoring, and related policy issues*, Congressional research service, 2017.

¹⁶⁶ V. *supra* cap. I.

¹⁶⁷ Si veda ALPA, *La trasparenza dei contratti bancari*, Bari, 2003; PELLEGRINI, *Etica e regole di condotta degli intermediari finanziari*, in SABBATELLI (a cura di), *Banche ed etica*, Padova, 2013.

¹⁶⁸ HURLEY, ADEBAYO, *Credit scoring in the era of big data*, Yale journal of law & technology, 2017.

¹⁶⁹ ALPA, *Relazione introduttiva al Convengo "Cyberlaw. Problemi giuridici connessi allo sviluppo di Internet"*, Roma, 9 luglio 2018.

integrato di telecomunicazione il quale si basa su tecniche informatiche, allo sviluppo di nuove forme di commercio nel cyberspazio¹⁷⁰.

Il mercato globale così delineato, se da un lato pertanto accresce la produzione e il consumo, con maggiore mobilità del risparmio, dall'altro accentua la condizione di dipendenza dei Paesi economicamente più deboli nei confronti dei Paesi più forti dal punto di vista economico, con la conseguenza che le opportunità di crescita derivanti dall'informatizzazione dei flussi commerciali vengono compensate da effetti negativi¹⁷¹. Tra quest'ultimi emerge il rischio dell'instabilità finanziaria, aggravata dalla circostanza che l'operatività su piattaforme virtuali amplifica tale effetto il quale può propagarsi potenzialmente a dismisura. Da qui la fondamentale esigenza di governare la rivoluzione tecnologica con la possibilità così di salvaguardare le economie deboli e, più in generale, di avviare una fase di sviluppo dei sistemi internazionali volti al conseguimento di obiettivi sociali attraverso una equa ripartizione delle risorse del pianeta¹⁷².

Il processo di sviluppo tecnologico, inoltre, non dovrà causare parimenti un incontrollato liberismo che lascia l'investitore privo di tutela¹⁷³. L'aspetto centrale in tal senso è la ricerca di un punto razionale di equilibrio tra innovazione finanziaria, sviluppo tecnologico e creazione di un quadro unitario di regole in quanto, soprattutto in mancanza di un approccio normativo adeguato, le tecnologie esasperano le asimmetrie informative e di potere le quali costituiscono la ratio della disciplina a tutela dell'investitore, specialmente in considerazione delle peculiarità nelle trattative *b2c*¹⁷⁴.

La mancanza di omogenei moduli applicativi produce una compressione del regime di tutela previsto dei *global regulators*, originariamente ben più estesa soprattutto in riferimento alle asimmetrie informative proprie delle negoziazioni aventi a oggetto strumenti finanziari virtuali. Ciò determina inoltre incertezza circa le modalità d'intervento adottate dalle *authorities* di vigilanza, le cui *policy* stentano a omogeneizzarsi a schemi operativi standardizzati. Di talché la necessità di individuare forme disciplinari volte alla formazione di schemi di supervisione integrati, attraverso nuovi spazi

¹⁷⁰ RIFKIN, *L'era dell'accesso*, Milano, 2000.

¹⁷¹ CAPRIGLIONE, *Mercato regole democrazia*, Milano, 2013, p. 19.

¹⁷² ONIDA, *La globalizzazione aumenta o riduce disuguaglianze e povertà?*, in *Il mulino*, 1, 2002.

¹⁷³ In tema CAPRIGLIONE, *Etica della finanza mercato globalizzazione*, Bari, 2004.

¹⁷⁴ In tema DAVOLA, *Bias cognitivi e contrattazione standardizzata: quasi tutele per i consumatori?*, in *Contratto e impresa*, 2, 2017.

operativi i quali, ispirati alla reciproca fiducia e riconoscimento, diano attuazione al processo di integrazione regolamentare¹⁷⁵.

Potrebbe essere auspicabile, secondo alcuni¹⁷⁶, l'opportunità di una possibile coesione delle funzioni di supervisione in virtù di un dialogo permanente tra autorità nazionali ed europee in riferimento alle modalità di gestione degli scambi in rete, così da ovviare ai problemi derivanti dall'assenza di strategie comuni di supervisione.

I processi tecnologici i quali caratterizzano le modalità organizzative del mercato finanziario e la regolazione dei regimi di gestione delle piattaforme online hanno determinato un ridimensionamento del ruolo degli intermediari bancari e dei tradizionali canali di distribuzione del credito. Le attuali misure di controllo e d'intervento sulle procedure *hi – tech* sembrano non ancora sufficientemente avanzate per rispondere all'esigenza di contrastare eventuali shock sistemici e di contenimento dei rischi delle manovre speculative¹⁷⁷.

Nel ridimensionamento del *framework*, pertanto, non è possibile prescindere da strategie comuni sulle modalità e sui termini del cambiamento, dovendo a tal fine eseguirsi la distinzione tra l'azione disciplinare volta a colmare i *gap* di regolazione esistente da quella inerente a migliorarne, nel tempo, la portata innovativa¹⁷⁸. Sebbene non sia possibile, nel programmare gli sviluppi descritti, prevedere la reale efficacia del processo di riforma, appare tuttavia opportuno che si proceda in ogni caso all'integrazione tra Stati al fine di stabilire le linee programmatiche comuni volte a disciplinare l'*agere* nel mercato.

La logica legislativa, nazionale ed europea, non dovrebbe contrapporsi ai principali attori nel mercato dei servizi finanziari, quanto piuttosto dovrebbe essere volta al promovimento di un processo normativo interattivo e cooperativo, il che determinerebbe una maggiore certezza dei rapporti giuridici svincolando lo stesso legislatore dalla posizione di *information taker* che determina un ostacolo alla *governance* del processo tecnologico¹⁷⁹.

L'attesa della definizione di un quadro disciplinare definito evidenzia la mancanza di una predeterminazione delle competenze spettanti alle autorità di supervisione e di controllo poste al

¹⁷⁵ ASSO, *Globalizzazione reale e globalizzazione finanziaria: aspetti teorici e problemi di regolamentazione*, in *Ragion pratica*, 18, 2002.

¹⁷⁶ PELLEGRINI, *Il diritto cybernetico nei riflessi sulla materia bancaria e finanziaria*, cit., p. 362.

¹⁷⁷ PELLEGRINI, *Il diritto cybernetico nei riflessi sulla materia bancaria e finanziaria*, cit., p. 362 – 363.

¹⁷⁸ *Ibidem*.

¹⁷⁹ ALPA, *Fintech*, cit.

vertice dell'ordinamento finanziario europeo e la necessità di uno stabile assetto organizzativo del regime di prevenzione dei c.d. *cybercrime*. Ciò in un'ottica ove sfumano i confini dei concetti di luogo, sovranità e sovranismo¹⁸⁰, il che determina una modifica delle relazioni intersoggettive le quali s'instaurano nelle strutture cibernetiche le quali, enucleando nuovi schemi negoziali virtuali, mutano specificatamente i rapporti commerciali.

¹⁸⁰ Così CAPRIGLIONE, *Non luoghi. Sovranità, sovranismi. Alcune considerazioni*, in *Riv. trim. dir. ec.*, 4, 2018, 393 ss.

CONCLUSIONE

Le questioni affrontate, probabilmente, lasciano più interrogativi di quante risposte forniscano tuttavia, è stato quantomeno possibile porre in evidenza i punti nevralgici dai quali impostare le possibili soluzioni.

Sono emerse tematiche generali dalle quali non è possibile prescindere come la globalizzazione del diritto e il transgovernalismo¹⁸¹, il che pone la questione ulteriore della disaggregazione dei sistemi giuridici¹⁸².

Sembra sia necessario, alla luce delle considerazioni svolte, enucleare una nuova struttura concettuale capace di comprendere e dar conto dei principali aspetti dell'attuale esperienza giuridica transnazionale. Il diritto del futuro sarà contestualizzato in un ambiente globale altamente evoluto a livello tecnologico, e la condizione di incertezza che ne segue è un'opportunità di scambio e di dialogo con la scienza e le nuove tecnologie.

Il "diritto del futuro" è pertanto plausibile che si presenti come digitalizzato, molecolare, non gerarchico, multilingue e poliarchico¹⁸³.

Se pertanto gli effetti positivi del rapporto tra tecnologia, diritto e mercato sembrano innanzitutto prodursi in generale nei rapporti sociali e commerciali, l'effetto negativo sembra quello della frammentazione e dispersione del diritto applicabile.

A tal proposito il fattore di coerenza e comunicabilità dello stesso, che è necessario ricercare, è identificabile nell'interoperabilità delle discipline giuridiche vigenti, il che può rappresentare la modalità maggiormente idonea a sviluppare il diritto di pari passo con lo sviluppo della tecnologia.

¹⁸¹ Si v. per tutti TEITEL, *Comparative constitutional law in a Global age*, in 117 Harv. L. Rev., 2004, 2570.

¹⁸² SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit. p. 363 ss.

¹⁸³ Così SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit. p. 375 ss.

BIBLIOGRAFIA

- AA. VV., Smart contracts as a specific application of blockchain technology, Smart contract Working Group, Dutch Blockchain Coalition, in www.dutchblockchain.coalition.org.
- ALLEN, WIDDISON, Can computer make contracts?, Harv. J. Law and technology, 25, 1996.
- ALPA, Cyber law. Problemi giuridici connessi allo sviluppo di internet, in Nuova giurisprudenza civile commentata, 1998, 6, II.
- ALPA, Fintech: un laboratorio per i giuristi, in Contratto e Impr., 2019, 2.
- ALPA, Il contratto del terzo millennio: intervento conclusivo, in Nuova giur. civ. comm., 2018, n. 7 – 8.
- ALPA, Il contratto in generale, I, Fonti, teorie, metodi, in CICU, MESSINEO, MENGONI, SCHLESINGER (a cura di), Tratt. Dir. civ. comm., , Milano, 2014.
- ALPA, La trasparenza dei contratti bancari, Bari, 2003; PELLEGRINI, Etica e regole di condotta degli intermediari finanziari, in SABBATELLI (a cura di), Banche ed etica, Padova, 2013.
- ALPA, Le stagioni del contratto, Bologna, 2012.
- ALPA, Relazione introduttiva al Convegno “Cyberlaw. Problemi giuridici connessi allo sviluppo di Internet”, Roma, 9 luglio 2018.
- AMIDEI, Intelligenza artificiale e responsabilità da prodotto: gli sviluppi del diritto del diritto dell’Unione Europea, in Giur. It.
- ANDERSON M., ANDERSON S. L., Robot be good: a call for ethical autonomous machines, in Scientific american, oc. 2010.
- ASSO, Globalizzazione reale e globalizzazione finanziaria: aspetti teorici e problemi di regolamentazione, in Ragion pratica, 18, 2002.
- BARLOW, A Declaration of the Independence of Cyberspace, in www.eff.org/it/cyberspaceindependence, 1996.
- BARRACO, SITZIA, La tutela della privacy nei rapporti di lavoro, Milano, Wolters Kluwer, 2012.
- BELLINI, Blockchain & Bitcoin, Milano, 2018.
- BOSCARATO, Who is responsible for robot’s actions? An initial examination of italian law within a european perspective, Atti del Convegno “TILTING perspective 2011 – Technologies on the stand: legal and ethical questions in neuroscience and robotics”, Tilburg University, april 2011.

BOTTALICO, Workplace technological innovation: what role for the law?, in SANTOSUOSSO, GOODENOUGH, TOMASI, The challenge of innovation in law. The impact of technology and science in legal studies and practise, Pavia University press, 2015.

BOTTINI, SEDDA, Neuroscienze Cognitive e Diritto, in SANTOSUOSSO, GARAGNA, BOTTALICO, REDI, Scienze Biomediche e Diritto. Un dialogo tra discipline, culture e lingue, Como – Pavia, Ibis, 2010.

BOUCHER, How blockchain technology could change our lives, European Parliamentary Research Service, 2017.

BROCKMAN, The new humanist: science at the edge, Barnes & Noble, 2003.

BROMBERG, GODWIN, RAMSAY, Fintech, sandboxes: achieving a balance between regulation and innovation, in Journal of banking and finance law and practice, 2017.

BUTERIN, A next generation smart contract and decentralized application platform, in White paper, GitHub.

BUTERIN, On Public and Private Blockchains, Ethereum Blog, 2015, in <https://blog.ethereum.org/>.

CAGGIANO, Il contratto nel mondo digitale, in Nuova giur. civ. 2018. CAPACCIOLI, Criptovalute e bitcoin: un'analisi giuridica, Giuffrè, 2015.

CAPRIGLIONE, Etica della finanza mercato globalizzazione, Bari, 2004.

CAPRIGLIONE, Mercato regole democrazia, Milano, 2013.

CAPRIGLIONE, Non luoghi. Sovranità, sovranismi. Alcune considerazioni, in Riv. trim. dir. ec., 4, 2018.

CAPRIGLIONE, Relazione al Seminario “Globalizzazione intelligente. Riflessioni e spunti tratti dall’opera di Dani Rodrik”, Università Luiss, Roma, 14 febbraio 2019.

CASEY, NIBLETT, Self – driving laws, University of Toronto law journal, 2016.

CASONATO, Introduzione al biodiritto, Torino, Giappichelli, 2009.

Cass. civ., sez. lav., sent. 27 settembre 2000, n. 12769, con commento di NADALET, Sull’obbligo di diligenza e i c.d. compiti accessori: verso un’estensione della sfera di imputabilità, in Riv. it. dir. lav., 3, 2001.

CHIERICI, Gli smart contract: profili giuridici con una struttura informatica, 2018, in www.salvisjuribus.it.

CLACK, BAKSHI, BRAINE, Smart contract templates: foundations, design landscape and research directions, Cornell University computing research repository, in arxiv.org.

COMELLINI, VASAPOLLO, Blockchain, criptovalute, I.C.O. e smart contract, Maggioli, 2019.

COMPORTI, Le responsabilità presunte – Artt. 2044 – 2048, in Il codice civile – commentario, SCHLESINGER (fondato da), BUSNELLI (diretto da), Giuffrè, Milano, 2009.

Comunicazione Commissione, Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo, Bruxelles, 8 marzo 2018, COM(2018).

DAVOLA, Bias cognitivi e contrattazione standardizzata: quasi tutele per i consumatori?, in Contratto e impresa, 2, 2017.

DEFILIPPI, The interplay between decentralization and privacy: the case of blockchain technologies, CERSA-CNRS-Université Paris II, Berkman Center for Internet & Society at Harvard, 2016.

DI CIOMMO, Gli smart contract e lo smarrimento del giurista nel mondo che cambia. Il caso dell'High frequency trading (HFT) finanziario, in FIMMANÒ, FALCONE (a cura di), Fintech, Universitas mercatorum, Napoli.

DI CIOMMO, Smart contract e (non-) diritto. Il caso dei mercati finanziari, in Nuovo diritto civile, 2019, 1.

DRUCK, "Smart contract" are neither smart nor contract, 37/10, in Banking financial services.

ENRIQUES, Financial supervision and regtech: four roles and four challenges, in Revue trimestrielle de droit financier, 53, 2017.

FAIRFIELD, Smart contracts, bitcoin bots, and consumer protection, Washington and Lee Law Review Online, 2, 2014, in www.scholarlycommons.law.wlu.edu.

FARWELL, SMITH, Using brain MERMER testing to detect concealed knowledge despite efforts to conceal, in Journal of forensic science, 46, 1.

FERRARI, ZANLEONE, Cloud computing. Aspettative, problemi, progetti e risultati di aziende passate al modello as a service, Franci Angeli, Milano, 2011. CARR, The big switch: rewiring the world, from Edison to Google, NY – London, WW Norton, 2009.

FINOCCHIARO, Diritto dell'informatica, UTET, 2014.

FINOCCHIARO, Il contratto nell'era dell'intelligenza artificiale, in Rivista Trimestrale di Diritto e Procedura Civile, 2018, 2.

FINOCCHIARO, Tecniche di imputazione della volontà negoziale: le firme elettroniche e la firma digitale, in CLARIZIA (a cura di), I contratti informatici, in RESCIGNO, GABRIELLI (diretto da), Trattato dei contratti, UTET, 2007. GAMBINO, voce Informatica giuridica e diritto dell'informatica, in Diritto online, Treccani, 2013.

FLORIDI, Philosophy and computing. An introduction, Routledge, London and New York, 1999.

GAMBINO, BOMPRESZI, Blockchain e protezione dei dati personali, in Diritto dell'Informazione e dell'Informatica (II), fasc.3, 2019, p. 619.

GAMBINO, Diritti fondamentali e cybersecurity, in POLLICINO, FROSINI, APA (a cura di), Diritti e libertà in internet, Milano, 2017.

GAMBINO, voce Firma elettronica, in Enc. giur. Treccani, Roma, 2004.

GANIS, KEENAN, The cognitive neuroscience of deception, in Social neuroscience, 4, 2009.

GANS, The fine print in smart contracts, in www.nber.org, 2019.

GASKELL et al, Europeans and biotechnology in 2010. Winds of change? A report to the european commission's directorate – general for research, oct. 2010, in ec.europa.eu.

GESLEVICH PACKIN, LEV – ARETZ, On social credit and the right to be unnetworked, in Columbia business law review, 2016, 2.

GETTER, Consumer and credit reporting, Scoring, and related policy issues, Congressional research service, 2017.

GIULIANO, La blockchain e gli smart contracts nell'innovazione del diritto del terzo millenio, in Diritto dell'Informazione e dell'Informatica (II), fasc.6, 2018.

GIULIANO, La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio, in Diritto dell'Informazione e dell'Informatica, 2019, 6.

GREENSPAN, Beware of the impossible smart contract, in www.the-blockchain.com, 2016.

HARRINGTON, Developing competition law for collusion by autonomous artificial agents, in Competition law and economics.

HOLDEN, MALANI, Can blockchain solve the holdup problem in contracts?, University of Chicago Coase – Sandor institute for law & economics research, 2017, in ssrn.com.

HOLTGREVE, New technologies: the future and the present of work in information and communication technology, in New technology, work and employment, 2014.

HONTS, KIRCHER, Mental and physical countermeasures reduce the accuracy of polygraph tests, Journal of applied psychology, 79, 1994.

HURLEY, ADEBAYO, Credit scoring in the era of big data, Yale journal of law & technology, 2017.

HUWS, Labor in the global digital economy: the cybertariat comes, Monthly review press, NY, 2014.

IDELBERGER, Connected contracts reloaded - smart contracts as contractual networks, in S. GRUNDMANN (a cura di), *European Contract Law in the Digital Age*, Intersentia, 2018.

IRTI, Scambi senza accordo, in *Riv. trim. di dir. e proc. civ.*, 52, 1998.

JAGTIANI, LEMIEUX, Fintech lending: financial inclusion, Risk pricing, and alternative information, in FBR of Philadelphia working paper, 2017, 17.

KARAKAS, STAMEGNA, Defining a EU – framework for financial technology (fintech): economic perspectives and regulatory challenges, in *Law and economics yearly review*, 2018.

KHOSHBIN L. S., KHOSHBIN S., Imaging the mind, Minding the image: an historical introduction to brain imaging and the law, in *AJLM*, vol. 33, 2007.

KOLBER, Not – so – smart blockchain contracts and artificial responsibility, in *Stan. Tech. L. rev.*, 2018, 198.

KOLVART, POOLA, RULL, Smart contracts, in KERIKMAE, RULL (eds), *The future of law and eTechnologies*, Springer, 2016.

KOUROUPETROGLOU, Enhancing the human experience through assistive technologies and E – accessibility, IGI global, 2014.

LEE, CHEN, LOW, *Inclusive Fintech: blockchain, cryptocurrency and ICO*, Word scientific, 2018.

LEVI, Discorso che potrebbe servire ad uso di programma, in *Riv. sperimentale di freniatria e di Medicina legale*, n. 1.

LIPSHAW, The persistence of “Dumb” contracts, in *www.ssrn.com*, 2018.

LOHR, The age of Big data, in *NYT*, 11 feb. 2012.

MARCUS, *Neuroethics. Mapping the field. Conference preceedings*, Dana press, NY, 2002.

MAXWELL, SALMON, A guide to blockchain and data protection, Hogan Lovells, 2017, in *www.hoganlovells.com*.

MIK, Smart contracts: terminology, technical limitations and real world complexity, in *Law, Innovation and Technology*, 2017, vol. 9, n. 2.

MIK, Smart contracts: terminology, technical limitations and real world complexity, 9 *law, innovation & technology*, 269, 2017.

NAAM, *More than human*, Broadway books, 2005.

NICOTRA, Blockchain e GDPR: le norme da conoscere per tutti i problemi, 24 luglio 2018, in <https://www.agendadigitale.eu/sicurezza/blockchain-e-gdpr-le-norme-da-conoscere-per-tutti-i-problemi/>.

NICOTRA, SARZANA, DISANT'IPPOLITO, Diritto della blockchain, intelligenza artificiale e IoT, Ipsoa, 2018.

ONIDA, La globalizzazione aumenta o riduce disuguaglianze e povertà?, in *Il mulino*, 1, 2002.

PAECH, The governance of blockchain financial networks, in *Modern law review*, 2017.

PAGLIERI, Bitcoin and the future of money, Triumph books, Chicago, 2014.

PANDILOV, DUKOVSKY, Comparison of the characteristics between serial and parallel robots, *Acta tehnica corviniensis, Bulletin of engineering*, 1.

PARDOLESI, DAVOLA, «Smart contract», cit., p. 308.

PARDOLESI, DAVOLA, «Smart contract»: lusinghe ed equivoci dell'innovazione purchessia, in CAPRIGLIONE (a cura di), *Liber amicorum Guido Alpa*, Milano, Cedam, 2019, p. 302.

PAROLA, MERATI, GAVOTTI, Blockchain e smart contract: questioni giuridiche aperte, in *Contratti*, 2018.

PASQUALE, The black – box society. The secret algorithms that control money and information, Harvard University press, 2015.

PERUGINI, Distributed ledger technologies e sistemi di blockchain: digital currency, smart contract e altre applicazioni, Key editore, 2018.

RASKIN, The law and legality of smart contracts, 1 *Geo. L. Tech. Rev.*, 305, 2017.

REIJERS, O'BROLCHÀIN, HAYNES, Governance in blockchain technologies & social contract theories, *Ledger*, 2016.

Report Fintech: regulatory sandboxes and innovation hubs. JC 2018/74, ESMA, EBA, EIOPA, gennaio 2019, in www.esma.europa.eu.

RIFKIN, L'era dell'accesso, Milano, 2000.

ROCO, BAINBRIDGE, Overview, in ROCO, BAINBRIDGE, *Converging technologies for improving human performance nanotechnology, biotechnology, information technology and cognitive science*, Arlington, Virginia, 2002.

RUFFOLO, Intelligenza Artificiale, machine learning e responsabilità da algoritmo, in *Giur. It.*

RUFFOLO, MUREDEN, “Intelligenza artificiale” e diritto, autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense, in *Giur. It.*, 7, 2019.

RUFFOLO, Self-driving car, auto driverless e responsabilità, in RUFFOLO (a cura di), *Intelligenza Artificiale e responsabilità*, Milano, 2017.

RUGGIU, Diritti e temporalità. I diritti umani nell’era delle tecnologie emergenti, Bologna, Il Mulino, 2012.

SANTOSUOSSO (a cura di), *Le neuroscienze e il diritto*, Ibis, Como – Pavia, 2009.

SANTOSUOSSO, Bioetica e diritto, in BARNI, SANTOSUOSSO (a cura di), *Medicina e diritto. Prospettive e responsabilità della professione medica oggi*, Milano Giuffrè, 1995.

SANTOSUOSSO, BOSCARATO, CAROLEO, Robot e diritto: una prima ricognizione, in *NGCC*, 2012.

SANTOSUOSSO, *Corpo e libertà. Una storia tra diritto e scienza*, Milano, Raffaello Cortina editore, 2001.

SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, Padova, Cedam, 2016, p. 2.

SARTOR, OMICINI, The autonomy of technological systems and responsibilities for their use, in BHUTA, BECK, GEISS, KRESS, LIU, *Autonomous weapons systems: law, ethics, policy*, Cambridge University Press, 2016.

SAVELYEV, Contract law 2.0: “smart” contract as the beginning of the end of classic contract law, in *Information & communication technology law*, 116, 2017.

SAVELYEV, Contract Law 2.0: “Smart” contracts as the beginning of the end of classic contract law, in *Higher School of Economics Research Paper n. WP BRP 71/LAW/2016*.

SCHREPEL, Collusion by Blockchain and smart contract, in *www.ssrn.com*, 2019.

SCHUEFFEL, Taming the Beast: A Scientific Definition of Fintech, in *Journal of Innovation Management*, vol. 4, n° 4, 9 marzo 2017.

SCILLIGO, Stato dell’io e correlati neurali, in *Psicologia, psicoterapia e salute*, vol. 9, n. 2, 2003.

STARK, Making sense of blockchain smart contracts, in *www.coindesk.com*.

SWAN, *Blockchain, Blueprint for a New Economy*, O'Reilly, 2015.

SWANSON, Great chain of numbers: a guide to smart contracts, smart property and trustless asset management, 2014, 14.

SZABO, Formalizing and securing relationships on public networks. In *first Monday* 2, in *ojphi.org*, 1997.

SZABO, Smart contracts, in www.virtualschool.edu, 1994.

SZABO, Smart contracts: Building blocks for digital markets, in www.fon.hum.uva.nl, 1996.

TEITEL, Comparative constitutional law in a Global age, in 117 Harv. L. Rev., 2004.

TROIANO, Fintech tra innovazione e regolamentazione, Relazione al Convegno “Fintech: prime esperienze e prospettive di regolamentazione”, Università La Sapienza, Roma, 4 dicembre 2017.

TURING, Computing machinery and intelligence, in Mind, New series, n. 236, 1950.

VERUGGIO, EURON roboethics roadmap, january 2007, in www.roboethics.org.

VISCOMI, Diligenza e prestazioni di lavoro, Torino, Giappichelli, 1997.

WRIGHT, DE FILIPPI, Decentralized blockchain technology and the rise of lex cryptographia, in ssrn.com.

RINGRAZIAMENTI

A conclusione di questo elaborato, vorrei dedicare qualche riga a tutti coloro che mi sono stati vicini in questo percorso di crescita personale e professionale.

Un sentito grazie al mio relatore, Valerio Lemma, per la sua infinita disponibilità e tempestività, nonché per l'interesse mostrato verso il mio lavoro e gli utili consigli con i quali sono stata indirizzata per la stesura della tesi.

Ringrazio di cuore i miei genitori: siete il mio esempio e la mia sicurezza. Grazie per essere sempre presenti, comprendermi e supportarmi nei momenti di difficoltà ma soprattutto spronarmi ad inseguire i miei sogni e non fermarmi davanti a nessun ostacolo.

Un grazie a mia sorella Giulia, parte fondamentale della mia vita, la mia complice e confidente. Anche se a volte ci scontriamo so che potrò sempre contare su di te. Grazie perché mi comprendi meglio di chiunque altro, mi fai sentire importante in ogni tuo gesto o piccola attenzione e, con la tua positività, porti allegria nella famiglia e in ogni mia giornata.

Un grazie immenso ai miei compagni in questa avventura: i miei colleghi e amici. Avete contribuito alla mia crescita arricchendomi con le vostre esperienze e punti di vista, mi avete insegnato l'importanza del team e gioito insieme a me per i traguardi raggiunti.

In particolare grazie alle mie migliori amiche Annabella, Margherita, Federica, Carlotta, Cristiana e Giulia: non potrei immaginare la mia vita senza di voi. Mi avete accolta come una sorella, facendomi sentire a casa anche quando questa è lontana, mi avete regalato risate, spensieratezza e tantissimi momenti che rimarranno per sempre indelebili nel mio cuore.

Infine, un ringraziamento speciale alla mia amica Elena, costante punto di riferimento e confronto nonostante la distanza. Grazie per aver sempre creduto in me e ricordarmi che dopo ogni caduta ci si deve rialzare più forti di prima. Non servono tante parole perché tu già lo sai, sei insostituibile.