RIVISTA TRIMESTRALE DI DIRITTO E PROCEDURA CIVILE
ISSN 0391-1896
Anno LXXII Fasc. 2 - 2018

Giusella Finocchiaro

IL CONTRATTO NELL'ERA DELL'INTELLIGENZA ARTIFICIALE

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

Giusella Finocchiaro
Ordinario dell'Università di Bologna

Il contratto nell'era dell'intelligenza artificiale

Sommario: 1. Introduzione. — 2. Metodo. — 3. L'identificazione delle parti. — 4. L'imputazione della volontà. — 5. L'oggetto del contratto. — 6. La forma del contratto. — 7. Limitazione dell'autonomia di non adempiere. — 8. Conclusioni con riguardo agli *smart contracts*. — 9. Questioni aperte.

1. — Le applicazioni di intelligenza artificiale sono ormai diffuse in ogni contesto, a cominciare dall'àmbito bancario e assicurativo.

Definire cosa sia l'intelligenza artificiale è impresa ardua. Come si legge in un recente rapporto dell'Aspen Institute Italia (1), « parafrasando Alan Turing — fra i padri fondatori della moderna intelligenza artificiale — l'IA può infatti essere definita la scienza di far fare ai *computers* cose che richiedono intelligenza quando vengono fatte dagli esseri umani; o, più propriamente, come quel settore dell'informatica che si occupa di creare macchine intelligenti in grado di eseguire compiti e risolvere problemi nuovi, di adattarsi all'ambiente e comprenderlo, e di capire il linguaggio naturale ».

È più semplice elencare le applicazioni più diffuse di intelligenza artificiale.

Secondo una recente analisi (2), le tecnologie che applicano intelligenza artificiale, considerate di maggior rilievo, sono: *Natural*

(1) Rapporto dell'Aspen Institute Italia, *Intelligenza artificiale come nuovo fattore di crescita*, luglio 2017, p. 1, che riprende le parole espresse da Turing, *Computing Machinery and Intelligence*, in *Mind*, New Series, 1950, v. 59, n. 236, pp. 433-460.

(2) Ricerca realizzata da Forrester, *TechRadar: Artificial Intelligence Technologies, Q1 2017*, richiamata nel rapporto dell'Aspen Institute Italia, *Intelligenza artificiale come nuovo fattore di crescita*, cit., p. 7.

Language Processing, Speech Recognition, *Virtual Agent*, Piattaforme di *Machine Learning, AI-optimized Hardware, Decision Management*, Piattaforme di *Deep Learning, Biometrica, Robotic Process Automation, Text Analytics.* Pur non addentrandosi nelle specifiche tecniche delle singole applicazioni, le diverse denominazioni suggeriscono lo scopo dei nuovi applicativi, costituito dal potenziamento dei meccanismi di ragionamento utilizzati per la soluzione di problemi e dal miglioramento del rapporto relazionale tra macchine e persona.

Le applicazioni basate sullo studio e la comprensione della lingua umana, per esempio, sono in grado di tradurre in linguaggio naturale informazioni originariamente codificate in linguaggio binario e viceversa, consentendo l'interazione tra persone e sistemi. Tale tecnologia viene utilizzata a partire da basilari servizi automatizzati di assistenza clienti, fino a sofisticati sistemi, come le c.d. *chat bot*, in grado di comprendere le esigenze del cliente e di fornire risposte personalizzate. Rimanendo nel campo delle relazioni macchina-utente, le tecnologie biometriche associate all'intelligenza artificiale rendono possibile l'instaurazione di interazioni che appaiono più naturali tra persona e sistemi informatici, sfruttando le capacità di riconoscimento basate non solo sul linguaggio e sulla voce, ma anche sull'immagine, sul tatto e sul linguaggio del corpo.

Ancora, le piattaforme di *machine learning* e *deep learning* permettono di implementare i sistemi di assunzione delle decisioni e di fare predizioni in maniera autonoma, al di là delle istruzioni inizialmente impartite. Si pensi, ad esempio, ai sistemi di intelligenza artificiale utilizzati dalle grandi piattaforme di *e-commerce* per predire gli acquisti della clientela, in base all'analisi di rilevanti quantità di dati concernenti preferenze, abitudini di consumo e caratteristiche personali.

L'utilizzo di queste tecnologie basate sull'intelligenza artificiale porta notevoli benefici, diminuendo i costi operativi, ma anche migliorando l'efficienza delle attività e della qualità di lavoro umano, con conseguente aumento del fatturato aziendale. In una ricerca condotta dal McKinsey Global Institute (3), ad esempio, viene calcolata una riduzione di costi operativi del 10-15% grazie

(3) McKinsey, *A Future That Works: Automation, Employment, and Productivity*, consultabile al *link http://www.mckinsey.com/global-themes/digital-disruption/harnes-*

all'automazione di un sistema di emergenza ospedaliero, del 25% nella manutenzione degli aerei, fino al 90% nella creazione automatizzata di mutui. In aggregato, l'incremento in produttività delle aziende si riflette in un fattore di crescita del +0.8-1.4% annuo.

2. — Ancora una volta un fenomeno nuovo impone al giurista di conoscerlo, di esaminarne le caratteristiche essenziali, di comprenderlo, di valutare se esso possa essere ricondotto alle categorie già esistenti dell'ordinamento giuridico, insomma di compiere quell'attività che gli è più propria, cioè l'attività di qualificazione.

Questa attività dovrà essere effettuata, anche in questo caso, con riferimento alle applicazioni dell'intelligenza artificiale nell'àmbito contrattuale e, in particolare, con riguardo agli *smart contracts*.

Gli *smart contracts* possono essere definiti come « protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale » (4).

Il loro inquadramento da un punto di vista giuridico richiede di approfondire una questione preliminare che attiene all'esatta ricostruzione del fenomeno: gli *smart contracts* sono contratti o sono atti di esecuzione di un contratto? In altri termini, la volontà contrattuale si esprime negli *smart contracts* o con gli *smart contracts* viene eseguita una volontà altrove dichiarata?

Problema non dissimile concettualmente si pose con riferimento ai contratti bancari e ai trasferimenti elettronici di fondi, che non sono contratti, ma atti di esecuzione di un contratto: ad esempio, il contratto di conto corrente.

In materia di *smart contracts* la questione risulta ulteriormente complessa. I cosiddetti *smart contracts*, infatti, possono assumere sia la natura di contratti, sia quella di atti di esecuzione di un contratto. Soltanto quelli che sono veri e propri contratti rivestono, però, un qualche interesse ai fini di questa trattazione.

Dunque, si esaminerà il normale corso di conclusione del contratto per verificare se, qualora di *smart contract* (in senso stretto)

sing-automation-for-a-future-that-works, richiamata nel rapporto dell'Aspen Institute Italia, *Intelligenza artificiale come nuovo fattore di crescita*, cit., p. 3.

(4) V. Wikipedia, *https://it.wikipedia.org/wiki/Smart_contract*, consultato il 10 aprile 2018.

si tratti, esso presenti aspetti di novità tali da imporre di rivedere le categorie giuridiche consolidate.

Va innanzitutto premesso che l'argomento costituito dalle applicazioni dell'intelligenza artificiale al diritto è estremamente suggestivo e riveste anche un fascino di natura letteraria, il quale ha colpito anche il Parlamento europeo che nella sua risoluzione del 16 febbraio 2017 (5) ha espressamente richiamato le tre leggi della robotica di Asimov.

Il tema non è talora esente da una certa retorica che indubbiamente rende la qualificazione giuridica del fenomeno, quanto meno in prima battuta, meno agevole. Si tende ad antropomorfizzare il fenomeno e a narrarlo come se le intelligenze artificiali coinvolte fossero emanazione di soggetti umani. Ciò ha condotto anche, seguendo la suggestione della narrazione, a riferirsi al programma informatico come « rappresentante » e, per giungere a questo risultato, a prospettare la necessità di configurare in capo al programma informatico una soggettività giuridica (6).

Tuttavia questa operazione pare non necessaria. Infatti, anche qualora si configurasse il *software* come rappresentante, ciò che rileverebbe comunque sarebbe, in termini di responsabilità, in ultima analisi, il patrimonio del rappresentante, al fine del risarcimento del danno. Dunque, occorrerebbe comunque attribuire un

(5) Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

La Commissione europea ha risposto alle osservazioni del Parlamento in un documento denominato « Follow up to the European Parliament resolution of 16 February 2017 on civil law rules on robotics », adottato il 16 maggio 2017, in cui dà atto delle raccomandazioni del Parlamento e conferma la propria disponibilità e cooperazione sul tema. A tal fine, il 9 marzo 2018 la Commissione europea ha annunciato l'istituzione di un gruppo di esperti sull'intelligenza artificiale che consigli e supporti la Commissione nelle decisioni e iniziative sul tema.

(6) In questo senso, la risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, p. 17.

Si v. inoltre il mio articolo *La conclusione del contratto telematico mediante i* « software agents »*: un falso problema giuridico?*, in *Contr. e impr.*, 2002, 2, pp. 500-509 e, nel medesimo volume, Sartor, *Gli agenti* software*: nuovi soggetti del* ciberdiritto, pp. 57-91.

patrimonio al rappresentante, cioè al *software*. Questa opzione è, infatti, contemplata dal Parlamento europeo (7).

L'esito della costruzione giuridica sintetizzata pare, alla fine, non particolarmente significativo, potendosi configurare in ogni caso una responsabilità in capo all'utilizzatore del programma, che è lo stesso risultato al quale conduce l'operazione di configurare il programma come rappresentante.

3. — Un primo problema che occorre esaminare è quello relativo all'identificazione delle parti.

Può essere rilevante ai fini della conclusione di un contratto conoscere con certezza l'identità dell'altro contraente. Ciò non è sempre agevole su *internet,* dove anzi è frequente che l'identità sia celata, con meccanismi di pseudonimizzazione o di anonimizzazione.

La pseudonimizzazione è definita dal nuovo regolamento (UE) n. 679 del 2016 (8) (regolamento generale sulla protezione dei dati) come« il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile » (art. 4, n. 5). I dati pseudonimizzati rimangono dati personali. La pseudonimizzazione, infatti, non esclude la possibilità di re-identificazione dell'interessato. Essa è piuttosto una misura di

(7) Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, p. 16.

(8) Regolamento (UE) n. 679 del 2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva CE n. 46 del 1995 (regolamento generale sulla protezione dei dati). Il regolamento sarà direttamente applicabile a partire dal 25 maggio 2018.

Per un'approfondita rassegna delle principali novità introdotte dalla nuova disciplina *privacy* si rinvia al volume da me curato, *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, 2017; AA.VV., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, a cura di Califano e Colapietro, Napoli, 2017 e Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016.

sicurezza che non modifica i presupposti di legittimità del trattamento dei dati personali. A conferma di ciò, il regolamento colloca la pseudonimizzazione, assieme alla cifratura, tra le misure che i titolari e i responsabili del trattamento sono tenuti a considerare, al fine di proteggere i dati personali trattati.

Il dato anonimo, invece, a cui non si applica la normativa in materia di protezione dei dati personali, è il dato che in origine o a séguito di trattamento non può essere associato a un interessato identificato o identificabile ([9]). Se si assume la definizione in senso assoluto, come dato non più identificabile, a prescindere dai costi e dai tempi necessari per la reidentificazione, è assai difficile che di dato anonimo si possa parlare *on line*. Al contrario, ove si intenda l'anonimato da interpretare secondo il criterio di ragionevolezza, dovrà farsi riferimento al grado di riferibilità dell'informazione a un determinato soggetto. Come sottolineato nel parere n. 4 del 2007 del Gruppo Art. 29 ([10]), la verifica dell'identificabilità è un concetto dinamico e dovrebbe considerare lo stato dell'arte al momento del trattamento del dato. Il dato anonimo, infatti, non è definito solo in relazione ad un soggetto, ma più in generale con riguardo ai costi, agli sforzi, al tempo, alle risorse e alla tecnologia che consente la reidentificazione. È dunque anche variabile nel tempo, in relazione allo sviluppo della tecnologia.

La famosa e ormai stracitata vignetta pubblicata sul New Yorker il 5 luglio 1993, che recita « On the Internet, nobody knows you're a dog », riassume uno scenario ancora attuale. La vignetta raffigura due cani: l'uno seduto su una sedia davanti a un *computer*; l'altro, a cui questa frase era rivolta, seduto sul pavimento. Da allora *internet* è cambiato, ma il problema dell'identità è rimasto e oggi l'identità digitale è un argomento di cruciale interesse. Gli ostacoli giuridici alla completa digitalizzazione dei processi sono stati rimossi, le

([9]) Tale definizione è prevista dall'art. 4, lett. *n*) d.lgs. 30 giugno 2003, n. 196, « Codice in materia di protezione dei dati personali », che tuttavia dovrebbe essere oggetto di abrogazione a séguito dell'approvazione dello schema di decreto legislativo di adeguamento dell'ordinamento interno al reg. (UE) n. 679 del 2016. Il regolamento, invece, non contiene un'espressa definizione in materia. La definizione prevista dal codice rimane in ogni caso valida, in quanto desumibile secondo un ragionamento « a contrario », a partire dalla definizione di dato personale.

([10]) Gruppo di lavoro *ex* art. 29 per la protezione dei dati personali, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007.

norme sul documento informatico e sulle firme elettroniche consentono di compiere con mezzi digitali sostanzialmente tutti gli atti giuridici che possono essere compiuti con strumenti cartacei, ma l'identificazione *on line* costituisce un problema cruciale oggi più di allora, soprattutto per lo sviluppo di alcuni servizi che richiedono un accertamento dell'identità.

Per dare risposta alle crescenti esigenze di certezza, il legislatore europeo ha cercato di promuovere meccanismi di identificazione delle parti, ritenendo l'identificazione utile, anche qualora non fosse richiesta dalla legge, per accrescere la fiducia e dunque favorire la conclusione di contratti *on line* e conseguentemente lo sviluppo del commercio elettronico.

Fin dal 1997, nei primi approfondimenti in materia della Commissione europea, è stata intrapresa questa direzione. Si è sempre ritenuto, infatti, che una delle cause più importanti del ritardato sviluppo del commercio elettronico fosse costituita dalla scarsa fiducia dei potenziali acquirenti, consumatori e non, nel mezzo di comunicazione. Per costruire la fiducia degli utilizzatori di *internet* sono state emanate numerose direttive, fra cui quella sul commercio elettronico. Anche la direttiva sulle firme elettroniche ([11]) persegue la medesima finalità ed è volta a rimuovere gli ostacoli giuridici allo sviluppo del commercio elettronico. Sotto questo profilo, la firma elettronica, consentendo di raggiungere una ragionevole certezza sull'identità del contraente, contribuisce a rafforzare la fiducia degli utenti nell'utilizzo delle tecnologie informatiche. Nel commercio fra privati, e dunque fatte salve le ragioni che hanno stimolato l'emanazione della normativa in esame nell'àmbito della pubblica amministrazione, la normativa in materia di firme informatiche non nasce solo per soddisfare esigenze tecnico-giuridiche di forma o di prova, ma soprattutto per creare fiducia nel commercio elettronico

Da ultimo, un importante passo nella risoluzione del problema dell'identificazione *on line* è stato l'emanazione del regolamento (UE) n. 910 del 2014 ([12]). Il regolamento è, in sigla, comunemente denominato « *eIDAS* », dove « *e* » sta per « *electronic* », « *ID* » per

([11]) Direttiva CE n. 93 del 1999 del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

([12]) Regolamento (UE) n. 910 del 2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva CE n. 93 del 1999.

« *identification* », « *A* » per « *authentication* » e « *S* » per « *signature* » (13). Oggetto del regolamento, infatti, oltre all'identificazione *on line* sono anche le firme elettroniche e i cosiddetti « servizi fiduciari » o « *trust service* ».

Innanzitutto, il regolamento distingue fra « identificazione elettronica » e « autenticazione elettronica ». L'identificazione elettronica (*electronic identification*) viene definita come il procedimento di utilizzo dei dati personali identificativi in forma elettronica al fine di rappresentare in modo univoco una persona fisica o giuridica, o la persona fisica che rappresenta una persona giuridica (14); mentre l'autenticazione (*authentication*) è definita come il processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, o l'origine e l'integrità dei dati in forma elettronica (15).

A queste definizioni fa riferimento anche il nostro ordinamento giuridico nazionale, e segnatamente il d.lgs. 7 marzo 2005, n. 82, codice dell'Amministrazione digitale (di séguito più brevemente « CAD »). A séguito delle modifiche apportate con d.lgs. 26 agosto 2016, n. 179, che ha inteso armonizzare le disposizioni nazionali al mutato quadro normativo europeo, il CAD opera un rinvio diretto alle definizioni contenute nel regolamento, abrogando quelle precedentemente previste (16).

(13) Per un approfondimento sul regolamento *e-IDAS*, si rinvia al volume da me curato con Delfini, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017.

(14) Art. 3, n. 1), regolamento *e-IDAS*.

(15) Art. 3, n. 5), regolamento *e-IDAS*.

(16) Nel CAD previgente, infatti, l'identificazione informatica era definita come la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso (art. 1, comma 1°, lett. *u-ter*). L'autenticazione, invece, non veniva riferita al soggetto che accede al sistema informatico, ma al documento informatico. Essa consiste nella validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione (art. 1, comma 1°, lett. *b*).

Una definizione più generale di autenticazione informatica è contenuta all'interno del codice in materia di protezione dei dati personali (art. 4, comma 3°, lett. *c*), ove l'autenticazione è definita come l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità. Come già riportato, il codice dovrebbe essere abrogato a séguito dell'approvazione dello schema di decreto legislativo di adeguamento dell'ordinamento interno al reg. (UE) n. 679 del 2016.

In materia di identità, l'obiettivo del regolamento *e-IDAS* è quello di rendere interoperabili gli strumenti di identificazione *on line* utilizzati negli Stati membri, rafforzando di conseguenza la sicurezza delle transazioni e degli scambi nel mercato interno.

In base al principio di neutralità tecnologica, non viene imposta l'adozione di un unico sistema di identificazione a livello europeo, ma si prevede che gli Stati membri possano notificare alla Commissione il sistema di identificazione *on line* utilizzato a livello nazionale, purché rispetti una serie di condizioni in termini di garanzia e sicurezza. Se il sistema ottiene l'approvazione della Commissione, deve essere riconosciuto anche dagli altri Stati membri e così anche i procedimenti di identificazione effettuati per mezzo di esso. In base al principio di mutuo riconoscimento, quindi, i cittadini europei potrebbero utilizzare le proprie identità digitali, rilasciate dai sistemi di identificazione nazionale notificati, per accedere a servizi o concludere contratti telematici nei diversi Stati membri, in tutti i casi in cui sia richiesta un'identificazione certa e digitale dell'utente.

Nell'ordinamento italiano, il sistema di identificazione elettronica è SPID (Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese), disciplinato dall'art. 64 del CAD ([17]). Le modifiche apportate al CAD dalla citata opera di coordinamento con il regolamento *e-IDAS*, hanno attribuito centralità al sistema di identificazione, dando nuovo impulso alla sua celere implementazione. Proprio nel dicembre 2017, alla luce della descritta facoltà di notifica prevista dalla normativa europea, l'Italia ha avviato il percorso per l'interoperabilità europea del proprio sistema di identità digitale, dando inizio alle procedure di pre-notifica di SPID alla Commissione europea.

Nel panorama globale, invece, la situazione è ancora incerta. Non esistono al momento sistemi di identificazioni condivisi, né regole comuni per garantire l'interoperabilità dei sistemi esistenti.

Sul tema sta lavorando, ormai da più di un anno, il *Working Group IV* sul commercio elettronico dell'Uncitral (Commissione

([17]) Lo SPID è inoltre disciplinato dal d.p.c.m. 24 ottobre 2014, « Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese », pubblicato in *Gazz. Uff.*, n. 285 del 9 dicembre 2014 e da una serie di regolamenti attuativi, pubblicati dall'Agid e reperibili al sito *http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid.*

delle Nazioni Unite per il diritto commerciale internazionale), il cui obiettivo è arrivare alla creazione di un sistema unificato a livello internazionale per l'identificazione nelle transazioni di *e-commerce*, al fine di assicurare uno sviluppo sicuro del mercato globale *on line*. In assenza di *standards* internazionali condivisi, la digitalizzazione degli scambi commerciali ha costretto numerosi attori dell'*e-commerce* a dotarsi di autonomi sistemi di identificazione, causando la proliferazione di una moltitudine di credenziali e modalità di accesso. Per ovviare a questo clima di incertezza, il lavoro del *Working Group* IV, quindi, è volto all'adozione di un *model law* che definisca requisiti minimi e condivisi per l'autenticazione internazionale degli utenti, nel rispetto delle diverse realtà nazionali.

4. — Le tecniche di imputazione della volontà nei contratti *on line* sono ormai consolidate.

Con le cosiddette « firme » elettroniche o digitali si è passati da un modello basato sull'autorialità ad un modello basato sulla responsabilità. In tal senso si è espresso anche il Consiglio di Stato nel parere del 7 febbraio 2005 (18). In materia di disconoscimento, si afferma che « sembra giusto superare i vecchi concetti di falso, strettamente legati al principio di "paternità" della firma e non a quello di "responsabilità" per la firma; dall'altro occorre fare assoluta chiarezza sulle ipotesi in cui è consentito dimostrare l'assenza di responsabilità ». La scrittura informatica è, infatti, impersonale e priva di grafia e l'apposizione della firma digitale non è, per sua stessa natura, un gesto personalissimo della mano del sottoscrittore. Si può dunque affermare che la particolare natura tecnologica della firma digitale e del documento informatico ha condotto all'elaborazione di una nuova tipologia di disconoscimento, che non ha ad oggetto né la sottoscrizione né la scrittura, caratteristiche esteriori del documento informatico, ma esclusivamente l'utilizzo del dispositivo di firma (19).

(18) Consiglio di Stato, parere del 7 febbraio 2005, n. 11995, sullo schema di d.lgs. recante il « Codice dell'amministrazione digitale, in attuazione della delega contenuta nell'articolo 10 della legge 29 luglio 2003, n. 229, Interventi in materia di qualità della regolazione, riassetto normativo e codificazione - Legge di semplificazione 2001 ».

(19) Cfr. mio contributo, *Tecniche di imputazione della volontà negoziale: le firme elettroniche e la firma digitale*, cit., p. 228.

Il termine « firma » va peraltro assunto come metaforico ed evocativo di un sistema di conoscenze (20). Sebbene il termine utilizzato sia « firma » in entrambi i casi, l'aggettivo (digitale, elettronica, elettronica qualificata, elettronica avanzata) che accompagna la firma informatica ne designa la diversa natura. Le firme informatiche si basano sulla tecnica, la sottoscrizione si basa sulla grafia. Le firme informatiche sono il risultato di una procedura tecnologica, mentre la sottoscrizione è il risultato di un gesto umano.

L'utilizzo del medesimo termine è foriero di conseguenze rilevanti sul piano della rappresentazione della conoscenza. Conduce ad associare naturalmente, quasi istintivamente, i due oggetti e a considerarli realtà assimilabili e quindi, in questo caso, sottoposti al medesimo regime giuridico.

E in questo caso si tratta di un'operazione di assunzione della firma come modello. Del modello si ha un'apprensione intuitiva e da esso si traggono liberamente inferenze. Il modello è una specie più generale di metafora. « Una metafora efficace ha il potere di mettere due domini separati in relazione cognitiva ed emotiva usando il linguaggio appropriato all'uno come una lente per vedere l'altro » (21). La metafora consente di mettere in relazione due domini di conoscenze.

Si tratta di una particolare applicazione dell'utilizzo della metafora a fini cognitivi (22).

Come scrive Galgano (23), illustrando l'utilizzo delle metafore nel diritto, esse costituiscono « utili sintesi verbali » e l'utilità della sintesi linguistica anche nel caso delle firme informatiche appare evidente.

L'approccio seguìto dal legislatore italiano nella normativa sulle

(20) Sul tema si rinvia al mio contributo, *La firma digitale*, in *Commentario del codice civile Scialoja-Branca*, diretto da Galgano, Bologna-Roma, 2000 e al più recente *La metafora e il diritto nella normativa sulla cosiddetta « firma grafometrica »*, in *Diritto informazione e informatica*, 2013, 1, pp. 1-16.

(21) Black, *Modelli Archetipi Metafore*, trad. it. a cura di Almansi e Paradisi, Parma, 1983, p. 87.

(22) Sulla funzione conoscitiva della metafora si rinvia a Eco, *Semiotica e filosofia del linguaggio*, Torino, 1984, p. 161 ss.

(23) Galgano con la consueta ricchezza culturale e profondità di analisi ha illustrato il tema della metafora nel diritto ne *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010, in particolare v. pp. 22-23.

firme informatiche si è basato sullo strumento cognitivo del modello e della metafora. Il legislatore italiano ha posto in relazione sottoscrizione autografa e firme informatiche. Il rapporto non è di identità, ma i due termini vengono associati sotto il profilo cognitivo. Si tratta di una relazione basata sul « come se », che usando lo strumento della metafora viene omesso, e non sull'« uguale » (24).

Il nostro ordinamento disciplina quattro diverse tipologie di firma: elettronica, elettronica avanzata, elettronica qualificata e digitale. La firma elettronica, non altrimenti qualificata, viene definita « dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare ». La definizione, che rinvia a quella prevista dall'art. 3 regolamento *e-IDAS*, differisce sostanzialmente da quella fornita precedentemente dal CAD, che la definiva « l'insieme dei dati in forma elettronica allegati, oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica ». Con il Regolamento *e-IDAS* si assiste ad un rafforzamento della funzione dichiarativa della firma elettronica, laddove quella identificativa è presupposta. Nel regolamento europeo la firma elettronica rappresenta uno strumento per firmare, da utilizzarsi per esprimere un consenso.

La firma elettronica avanzata è definita come una firma elettronica che soddisfa i requisiti elencati all'art. 26 regolamento *e-IDAS*, quindi: « *a*) è connessa unicamente al firmatario; *b*) è idonea a identificare il firmatario; *c*) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e *d*) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati ». La firma elettronica qualificata, invece, è « una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche ». Infine, la firma digitale, che non trova collocazione nel regolamento *e-IDAS*, è definita dal CAD come « un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma

(24) V. il mio contributo *La metafora e il diritto nella normativa sulla cosiddetta « firma grafometrica »*, cit., pp. 1-16.

elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici ».

Sotto il profilo probatorio, il documento informatico a cui sia associata una firma elettronica sarà diversamente valutabile in giudizio a seconda della tipologia di firma utilizzata.

Ai sensi dell'art. 20, comma 1°-*bis*, CAD, in tutti i casi in cui al documento non sia apposta alcuna firma o sia apposta una firma elettronica, non altrimenti qualificata, l'idoneità del documento a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili dal giudice, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità del documento stesso. Dunque, è una scelta del giudice a determinare il valore che la firma può assumere, caso per caso, a seconda delle circostanze concrete da lui esaminate.

Al contrario, lo stesso art. 20, comma 1°-*bis* stabilisce che il documento informatico a cui è apposta una firma digitale, qualificata o avanzata, ha l'efficacia prevista dall'art. 2702 c.c. per la scrittura privata. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare della firma elettronica, salvo che questi dia prova contraria. A queste tipologie di firme, le recenti modifiche al CAD, operate con d.lgs. 13 dicembre 2017, n. 217 ([25]), hanno affiancato un nuovo sistema di sottoscrizione, che si realizza nei casi in cui un documento sia « formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 ». Ai fini del valore probatorio, tale nuovo sistema è equiparato a una firma elettronica avanzata.

In materia contrattuale, un tema di grande interesse è quello dell'approvazione delle clausole vessatorie attraverso un sistema *point&click*.

Utilizzando tale tecnica, il contraente contro cui le clausole vessatorie sono previste esprime la propria volontà contrattuale

([25]) D.lgs. 13 dicembre 2017, n. 217, « Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche » (*Gazz. Uff.*, serie generale n. 9 del 12 gennaio 2018).

selezionando un'apposita icona o un *check-box*. La manifestazione del consenso può avvenire in qualunque modo, a meno che non sia richiesta la forma scritta, e dunque anche con un *click*. Ma si è discusso se tale sistema possa essere utilizzato anche per l'approvazione delle clausole vessatorie ai sensi dell'art. 1341, comma 2°, c.c.

Non v'è dubbio che in questo caso le manifestazioni di volontà debbano essere almeno due, una per l'approvazione del regolamento negoziale e una per l'approvazione specifica delle clausole vessatorie, come ribadito dalla decisione del Tribunale di Catanzaro ([26]) e del giudice di pace di Partanna ([27]), ma la questione è quale debba essere la forma dell'approvazione per iscritto: se la firma elettronica sia sufficiente o se debba farsi ricorso ad una particolare tipologia di firma elettronica (cioè alla firma elettronica avanzata o alla firma digitale).

Secondo la decisione della Corte di giustizia europea, del 21 maggio 2015, nella causa C-322/14 ([28]), la « procedura di accetta-

([26]) Trib. Catanzaro, (ord.) 30 aprile 2012. Nell'àmbito di una causa riguardante la disattivazione di un *account* professionale sul sito di *eBay*, il giudice ha l'opportunità di pronunciarsi sulla sottoscrizione da parte di un operatore commerciale di una clausola vessatoria (che attribuiva a *eBay* facoltà di recesso), contenuta nel contratto di *hosting*. Nel caso di specie, l'operatore commerciale aveva sottoscritto con un'unica selezione del « tasto negoziale » il contratto a lui sottoposto. Il giudice, quindi, rilevando la mancata specifica approvazione della clausola vessatoria, ne dichiarava la nullità.

Solo come *obiter dictum* nell'ordinanza si fa cenno alla circostanza che la sottoscrizione delle clausole vessatorie debba essere effettuata con firma digitale.

([27]) G.d.p. Partanna, sent. 1 febbraio 2002, n. 15. Il caso di specie concerneva la validità di una clausola derogatoria alla competenza territoriale, inserita nel regolamento contrattuale di un contratto B2B, concluso in via telematica. Il giudice, evidenziando la natura vessatoria della clausola di deroga convenzionale del foro, concludeva ritenendo necessaria la raccolta di un « un doppio assenso, premendo sull'apposito tasto: uno di adesione e l'altro di approvazione delle clausole cosiddette vessatorie, tra le quali va annoverata quella relativa alla deroga sul foro territorialmente competente ».

([28]) Il caso sottoposto alla Corte riguardava l'acquisto di un autoveicolo elettrico, da parte di una concessionaria di automobili, sul sito *web* della società venditrice. Quest'ultima, convenuta presso il tribunale competente, eccepiva la deroga della competenza in favore in un diverso giudice, in base ad una clausola contenuta nelle condizioni generali di vendita. L'acquirente ne contestava invece il valido inserimento, contestando la sussistenza di forma scritta, come richiesto dall'art. 23, par. 2, regolamento di Bruxelles I.

I giudici europei, in base alle risultanze del merito, rilevavano in primo luogo che l'acquirente doveva accettare espressamente, contrassegnando l'apposita casella, le condizioni generali di vendita del venditore prima di realizzare un acquisto. Tuttavia, l'operazione non comportava automaticamente l'apertura del documento contenente le

zione mediante “clic” delle condizioni generali di un contratto di vendita [...] concluso elettronicamente, che contengano una clausola attributiva di competenza, costituisce una comunicazione elettronica che permette di registrare durevolmente tale clausola, ai sensi di tale disposizione, allorché consente di stampare e di salvare il testo di dette condizioni prima della conclusione del contratto ».

5. — Tuttavia, un ulteriore problema si pone nel caso degli *smart contracts* ed è quello relativo all’effettiva conoscenza del contenuto del contratto. Il problema è dei più affascinanti, anche perché induce ad una rappresentazione in chiave antropomorfa dei programmi informatici (29).

Infatti, essendo il contratto concluso in maniera automatica al ricorrere di certi presupposti, le condizioni effettive attuali alle quali il contratto viene alla fine concluso possono non essere note al contraente, soprattutto se si tratta di un meccanismo decisionale complesso che prevede molte variabili. Ora, mentre è abbastanza semplice rappresentarsi, ad esempio, che il contratto sarà concluso se il prezzo relativo alla compravendita di un bene si attesterà all’interno di un *range* compreso fra 1 e 10, più difficile risulta la rappresentazione del contenuto del contratto se le variabili che lo determinano sono molte e se i meccanismi di combinazione sono, a loro volta, numerosi. Il che diviene ancora più complesso qualora il

condizioni generali del venditore, nelle quali era inclusa la clausola attributiva della competenza, per la quale era necessario un *click* ulteriore, su un apposito collegamento ipertestuale. In secondo luogo, la Corte analizzava il requisito di forma scritta richiesto ai sensi dell’art. 23, par. 2, regolamento di Bruxelles I, rilevando che la finalità di tale disposizione è quella di equiparare determinate forme di comunicazione elettronica alla forma per iscritto, in vista di semplificare la conclusione dei contratti con mezzi elettronici. Affinché la comunicazione elettronica possa offrire le stesse garanzie, in particolare in materia di prova, è sufficiente che sia possibile salvare e stampare le informazioni prima della conclusione del contratto.

Alla luce di ciò, i giudici europei concludevano ritenendo l’accettazione mediante *click* di una clausola attributiva di competenza, contenuta in un contratto concluso elettronicamente, valida e sufficiente.

(29) Problematiche analoghe furono analizzate agli inizi del secolo in relazione ai contratti conclusi attraverso i distributori automatici di beni e servizi e la dottrina più avvertita muoveva dal presupposto che con l’uso dell’automa si desse vita ad un negozio giuridico. Cfr. Cicu, *Gli automi nel diritto privato*, estratto da *Il Filangieri*, n. 8, Milano, 1901 e Scialoja, *L’offerta a persona indeterminata ed il contratto concluso mediante automatico*, Città di Castello, 1902.

programma sfrutti un sistema di auto-apprendimento e dunque « impari », per così dire, dalle circostanze. Qualche anno fa si sarebbe detto che la volontà era riconducibile comunque all'autore del programma ([30]). Oggi la volontà non può dirsi predeterminata o predeterminabile in modo sicuro, preso atto che esistono algoritmi i quali sono in grado di apprendere in modo autonomo e di prendere decisioni senza che le relazioni causa-effetto siano necessariamente comprese dall'uomo. È stata superata quella frontiera costituita dalla effettiva diffusione dei programmi di intelligenza artificiale.

L'oggetto del contratto in questo caso certamente non è determinato. Esso è determinabile, ma non sempre prevedibile, sulla base di criteri e di parametri che in taluni casi non consentono una rappresentazione anticipata. In questo caso, il contraente potrebbe non essere in condizione di conoscere in modo compiuto anticipatamente il contenuto del contratto che andrà a concludere. Ma avrà comunque espresso rispetto alla conclusione del contratto la propria dichiarazione positiva di volontà. Il contenuto del contratto è dunque determinabile, ma secondo modalità che non sempre consentono una pre-comprensione. Occorre dunque chiedersi se di volontà in senso stretto si tratta, anticipatamente dichiarata, rispetto all'effettivo formarsi delle condizioni contrattuali e quindi del contenuto negoziale, almeno in parte, oppure se non sia invece più aderente rappresentare tutto ciò nei termini di un sistema di assunzione del rischio. In altri termini, la narrazione giuridica può declinarsi affermando che il contraente ha accettato il rischio di concludere il contratto attraverso un dato sistema informatico che utilizza un programma di intelligenza artificiale, o affermando che lo stesso contraente ha concluso un contratto con oggetto determinabile attraverso un sistema di intelligenza artificiale.

6. — Il requisito della forma, ove la forma sia richiesta dalla legge, non offre particolari problematicità. Un ricco strumentario giuridico è reso disponibile dal legislatore italiano ed europeo.

Fin dal 1997, il legislatore italiano ha ritenuto di introdurre nel nostro ordinamento una definizione di documento informatico.

([30]) Questa era la tesi che io stessa ho sostenuto nel mio *I contratti informatici*, in *Trattato dir. comm. e pubbl. econ.*, diretto da Galgano, XXII, Padova, 1977.

L'operazione è stata ritenuta necessaria non tanto per ragioni tecnico-giuridiche, quanto piuttosto per abbattere un condizionamento culturale che porta a pensare il documento come necessariamente cartaceo, quando nulla obbliga in questo senso.

Carnelutti evidenziava l'irrilevanza della materia, affermando che « qualunque materia, atta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo » ([31]). Dunque, anche un documento costituito da soli *byte* sarebbe stato documento, essendo, pure in questo caso, la materia irrilevante. A rigore, neppure una normativa specifica in materia sarebbe stata necessaria a configurare il documento informatico come documento, sotto il profilo della materia che lo forma.

Come è noto, la normativa italiana non prevedeva la definizione di documento o, meglio, non l'ha prevista fino alla revisione del già citato d.lgs. 7 marzo 2005, n. 82, dettata dal d.lgs. 30 dicembre 2010, n. 235, che ha comportato la definizione di documento analogico. Solo con la diffusione del documento informatico è divenuto necessario definirlo e conseguentemente definire il documento analogico.

Ora, l'art. 1, comma 1°, CAD, armonizzato come ricordato alla disciplina europea del regolamento *e-IDAS*, prevede le seguenti definizioni di documento: « *p*) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti » e « *p-bis*) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti ».

Il CAD ha dunque riformulato la definizione di documento informatico in modo non soddisfacente. Infatti, la vigente definizione fa riferimento due volte al documento in quanto contenitore: si dispone che il documento informatico è il documento elettronico che contiene la rappresentazione. Oltre a ciò, il riferimento all'elettronico appare poco felice perché potrebbe essere inteso come se si volesse circoscrivere la definizione stessa di documento informatico all'utilizzo di quei supporti che prevedono una tecnologia esclusivamente elettronica (come le chiavette *USB*), non considerando altri supporti che si servono di una tecnologia non elettronica (es. *wi-fi*,

([31]) Carnelutti, voce *Documento* (*Teoria moderna*), in *Noviss. dig. it.*,VI, Torino, 1964, p. 86.

cd-rom). In realtà la tecnologia utilizzata e il supporto utilizzato dovrebbero essere irrilevanti ai fini definitori. Purtroppo, il nostro legislatore ha dovuto attenersi alla definizione fornita nel regolamento europeo.

In relazione all'idoneità del documento di integrare la forma scritta, l'art. 21, comma 2°-*bis*, CAD stabilisce che il documento informatico a cui è apposta una firma elettronica qualificata, digitale, è idoneo a soddisfare il requisito di forma scritta *ad substantiam*, previsto per le scritture private di cui all'art. 1350, comma 1°, nn. da 1 a 12, c.c. Gli atti di cui all'art. 1350, comma 1°, n. 13), c.c., invece, possono essere sottoscritti a pena di nullità non solo con firma elettronica qualificata o digitale, ma anche con firma elettronica avanzata ovvero sono formati con le ulteriori modalità di cui all'art. 20, comma 1°-*bis*, in precedenza menzionate.

In tutti gli altri casi, l'art. 20, comma 1°-*bis*, prevede che l'idoneità del documento ad integrare la forma scritta sia liberamente valutabile in giudizio, tenendo conto delle caratteristiche di sicurezza, integrità e immodificabilità.

7. — Un altro tema di interesse, secondo i primi commenti, è quello relativo all'impossibilità di non adempiere ([32]). In altri termini, il contratto sarebbe automaticamente eseguito e quindi il contraente non avrebbe possibilità materiale di non adempiere al contratto stesso. A ben vedere, però, l'adempimento, ove di pagamento si tratti, è atto dovuto, tanto che può essere effettuato anche dal debitore incapace. La questione è più correttamente posta se si imposta in termini di scelta relativa, per esempio, all'obbligazione alla quale adempiere, ponendosi un'alternativa fra due obbligazioni che, nel caso concreto, non possano essere entrambe adempiute. In questo caso la scelta relativa all'adempimento potrebbe essere automatica e così sfuggire alla volontà del debitore. Ancora, la revoca della dichiarazione contrattuale potrebbe essere tecnicamente non effettuabile, per la particolare tempistica della transazione, cioè perché non ci sarebbe neppure il tempo di revocarla.

([32]) Sull'argomento si v., tra gli altri, Di Sabato, *Gli* smart contracts*:* robot *che gestiscono il rischio contrattuale*, in *Contr. e impr.*, 2017, 2, pp. 378-402 e Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *Nuova giur. civ.*, 2017, 1, pp. 107-119.

8. — Si è passato in rassegna il normale percorso di conclusione del contratto e dei requisiti dello stesso, che rilevano nel caso specifico. All'esito di questo sintetico esame non pare che, nel caso in cui il contratto sia uno *smart contract*, sia richiesto al giurista di superare le categorie consolidate né di inventarne di nuove. Occorre certo comprendere appieno il fenomeno, sotto il profilo non soltanto tecnologico, ma anche sociologico, provocando esso nuovi comportamenti sociali, ma non occorre cercare nuove regole.

Peraltro non per ogni fenomeno occorre una nuova regola, come purtroppo frequentemente si sente invocare: spesso, infatti, viene richiesta una nuova legge per ogni nuovo fenomeno. Ma il giurista è interprete e non mero contabile del diritto e deve rivendicare con orgoglio il suo ruolo.

9. — Le applicazioni di intelligenza artificiale sollevano almeno due ulteriori ordini di questioni giuridiche: quella della responsabilità e quella dell'utilizzo dei dati.

Con riguardo alla prima questione, occorre chiedersi chi risponde dei danni causati da un *robot* o da un *software* a cui vengono delegate decisioni. Qualche anno fa si sarebbe risposto: è responsabile, o sono responsabili, alternativamente o cumulativamente, chi ha scritto il programma, il produttore o il venditore. Ma oggi lo scenario è più complesso, la risposta giuridica più articolata, a causa della pervasività dell'informatica nella società e nell'industria. Come si è illustrato, oggi esistono algoritmi in grado di apprendere in modo autonomo e di prendere decisioni senza che le relazioni causa-effetto siano necessariamente comprese dall'uomo. Inevitabilmente ciò investe i fondamenti giuridici della responsabilità giuridica: il paradigma basato sul dolo e sulla colpa non può essere sufficiente e occorre elaborare nuovi modelli di responsabilità.

D'altronde, chi avrebbe mai pensato di trovare citate le tre leggi della robotica di Asimov in un testo normativo? Eppure si leggono nella già citata risoluzione del Parlamento europeo del 16 febbraio 2017. Pur trattandosi di raccomandazioni e quindi di *soft law*, si affronta un tema che pochi anni fa sarebbe parso ai limiti della fantascienza: quello della responsabilità civile dei *robot* e dei programmi di intelligenza artificiale.

Con riguardo alla seconda questione, le attuali applicazioni di

intelligenza artificiale richiedono una grande mole di dati, i *Big Data* appunto, oggi disponibile. Una delle principali ragioni per cui finora l'intelligenza artificiale non aveva avuto un grande successo era proprio quella della mancanza di dati sui quali basare le applicazioni. Oggi la massa di dati necessaria c'è e spesso è fornita proprio dagli stessi soggetti cui i dati si riferiscono, per esempio attraverso i *social network*.

L'intelligenza artificiale ha bisogno dei *Big Data*. Come ha scritto *The Economist*, « The world's most valuable resource is no longer oil, but data » (33).

E intelligenza artificiale e *Big Data* richiedono la formulazione di nuovi paradigmi giuridici.

Pur nell'anno dell'applicazione in Europa del *GDPR* (*General Data Protection Regulation*, regolamento UE n. 679 del 2016) non si è ancora risolto un problema fondamentale ovvero della duplice natura del dato personale: insieme, oggetto di un diritto della personalità e bene giuridico.

Per risolvere questi problemi non è necessaria semplicemente una nuova normativa, ma è necessario un nuovo approccio. Occorre anche sotto il profilo giuridico un approccio « *disruptive* ». Senza dimenticare che il diritto certamente non può impedire la diffusione di nuove tecnologie, ma che la funzione del diritto è governarne gli sviluppi per prevenire i conflitti. E il campo di gioco in questo caso non è europeo, ma globale.

(33) *The Economist*, *The world's most valuable resource is no longer oil, but data*, pubblicato il 6 maggio 2017.