
CALL FOR PAPERS
INNOVAZIONE TECNOLOGICA
NUOVE PROSPETTIVE PER
L'INDAGINE GIURIDICA E PER
LA PROFESSIONE FORENSE
RISOLUZIONI
QUESTIONI
AGAT
CALL FOR PAPERS
RACCOLTA DEI CONTRIBUTI
SPONSORED BY
intesa
4cLegal
www.4cLegal.com
Qi net
ASSOCIAZIONE
AVVOCATI TORINO GIOVANI
AGA

PREFAZIONE

L'AGAT - Associazione Giovani Avvocati Torino ha voluto promuovere un dibatto sul tema del rapporto tra diritto e tecnologia, secondo il modello del *call for papers*. L'iniziativa ha avuto un'adesione superiore alle aspettative dei suoi organizzatori e può dirsi che sia stato conseguito l'obbiettivo prefissato: far emergere, da un lato, l'impatto multidisciplinare delle nuove tecnologie sul mondo del diritto e, dall'altro, descriverne la ricaduta sulla professione forense e, comunque, sull'attività pratica degli operatori del diritto.

Per merito dell'impegno dei relatori che hanno voluto cimentarsi con l'argomento, il tema è stato analizzato "ad ampio spettro": i contributi ricevuti hanno infatti approfondito i temi più classici (quale l'utilizzo dell'intelligenza artificiale nelle dinamiche processuali, l'incrocio tra intelligenza artificiale e responsabilità civile), ma anche temi di grande attualità (ad esempio la disciplina del cyberbullismo) o di ampio respiro culturale (quali i profili etici connessi all'utilizzo delle nuove tecnologie).
Nella prospettiva maggiormente pratica, non è mancato chi ha ritenuto di trattare le ricadute delle innovazioni sull'organizzazione degli studi legali, sull'attività della pubblica amministrazione e sulle modalità di conclusione dei contratti (*blockchain* e criptovalute).

All'evento del 18 luglio 2019, presso la Fondazione Fulvio Croce, gli autori dei migliori elaborati hanno avuto la possibilità di presentare il loro *paper* confrontandosi con i membri della commissione di valutazione e dando vita ad uno stimolante ed apprezzato dibattito.
Il Direttivo dell'AGAT ha pertanto deciso di pubblicare una selezione dei lavori, con l'auspicio che essi possano contribuire all'ampio dibattito in corso.

L'Associazione rinnova il proprio ringraziamento a tutti coloro che hanno presentato gli elaborati e alle persone che, con il loro impegno, hanno reso possibile l'evento, ricordando in questa sede – per tutti – i membri della commissione di valutazione dei *papers* Francesca Lagioia, Eva Desana, Corrado Druetta e Antonio Maria Morone.

NICOLÒ MAGGIORA – FEDERICO RESTANO

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

SPONSORED BY

intesa

4cLegal
www.4cLegal.com

Qi net

ASSOCIAZIONE GIOVANI AVVOCATI TORINO

AGA

IL DUBBIO DEL ROBOT DI FRONTE ALLA LEGGE

DI ENRICO AUTERO

1) Introduzione [1]

Il presente lavoro si pone l'obiettivo di analizzare il tema della prevedibilità delle decisioni giuridiche nel caso in cui queste fossero prese da un giudice robot. La questione è infatti di grande interesse e importanza nella società odierna, in cui l'informatizzazione e l'automatizzazione sono componenti sempre più essenziali del vivere.

In particolare, nella prima parte dello scritto ci si soffermerà sulla cosiddetta prevedibilità delle decisioni giuridiche (ovvero di "diritto calcolabile"), mettendo in evidenza come, in realtà, si tratti di una questione affatto nuova.

Successivamente verranno analizzate le modalità cognitive proprie del ragionamento robotico, ciascuna con le proprie peculiarità. Si vedrà inoltre se tali schemi cognitivi siano o meno applicabili al mondo giuridico, con attenzione particolare al processo interpretativo.

Infine, si valuterà la possibilità che un giudice robot possa, oggi, sostituirsi all'attività umana, al punto da poter dubitare della stessa legge che è chiamato ad applicare, sino alla sollevazione della questione di legittimità alla Corte Costituzionale.

2) La nozione di diritto prevedibile

L'uomo è naturalmente portato a voler conoscere ciò che sarà. Tutti desidererebbero scrutare nel domani per prendere le decisioni di oggi. La natura profondamente umana di anticipare il futuro coinvolge quindi tutti gli aspetti dell'esistenza, con particolare riferimento alle relazioni sociali ed economiche. E il diritto, in quanto caratterizzato da forti componenti sociali ed economiche, non si sottrae alla volontà umana di conoscere quel che sarà.

La natura stessa del fenomeno giuridico si predispone a un'anticipazione degli eventi futuri a causa del principio della certezza del diritto. Se il diritto non fosse infatti connotato da un elevato grado di certezza – la violazione di una norma giuridica deve avere delle conseguenze – esso non sarebbe in grado di fungere da regolatore della società. Non è un caso che una delle esigenze primarie dei legislatori di ogni tempo sia stata quella di creare dei meccanismi volti a prevedere, al verificarsi di una certa fattispecie, una conseguenza certa e determinata. Si pensi ad esempio alla prima legislazione scritta, il codice di Hammurabi, in cui ad ogni comportamento illecito era associata una sanzione precisa. Si ricordi poi il sistema delle *actiones* romane, in cui la tutela di un diritto era subordinata alla presenza di un'azione *ad hoc* e predeterminata[2]. Com'è noto, la certezza del diritto ha poi subito un duro colpo nel corso del Medioevo e del Rinascimento. Ciò è stato determinato da una serie di fattori diversi tra loro: in primo luogo, l'insorgere del cosiddetto "ius personae", per cui ogni individuo invocava per sé l'applicazione di un diritto diverso in base al proprio censo, alla propria corporazione

---

[1] di Enrico Autero

[2] V. ARANGIO RUIZ, "*Istituzioni di Diritto Romano*", Napoli, Jovene, 1984.

o al proprio titolo[3]; in secondo luogo, con l'avvento delle monarchie assolute e le innovazioni legislative imprevedibili, si è perso quel riferimento che soltanto una norma stabile e duratura può conferire (in questo senso è emblematica la frase attribuita al Re Sole: "È legale perché lo voglio io!"). Di contro, dopo la Rivoluzione Francese la certezza del diritto è assunta a valore cardine dell'ordinamento, soprattutto grazie all'elaborazione di Montesquieu e alla sua visione del giudice che, come un automa, avrebbe dovuto essere una semplice "*bouche de la loi*"[4]. Tale concezione del giudice, pur con tutte le sue evoluzioni, si riverbera ancora oggi negli ordinamenti giuridici moderni di civil law: non è un caso che l'art. 101 della Costituzione Italiana preveda che "*i giudici sono soggetti soltanto alla legge*".

Come visto, l'esigenza di un diritto certo (e per questo prevedibile) ha attraversato tutti i secoli della storia umana. Occorre ora affrontare come si atteggia oggi il principio della certezza del diritto, con particolare riferimento al ruolo svolto dai giudici.

a) Le basi del diritto "calcolabile"

Il risvolto della certezza del diritto che qui preme maggiormente analizzare parrebbe essere, in realtà, una sua naturale conseguenza. Se infatti il diritto è certo, o dovrebbe essere tale, allora dovrebbe essere possibile sapere l'esito di un'eventuale controversia con sicurezza e in anticipo, senza doversi rivolgere al giudice. Tale fenomeno è certamente un valore da perseguire ma non è, al momento, completamente attuabile. A tal fine, si prendano ad esempio i due principali metodi elaborati dagli ordinamenti giuridici per supportare la certezza del diritto: il sistema del precedente vincolante e la norma generale e astratta. Con riferimento al primo sistema, è innegabile (e umano) che i giudici abbiano sempre cercato di adottare delle decisioni uniformi relative a casi simili. Questo perché, se un certo orientamento giurisprudenziale riesce ad affermarsi, allora sarà possibile sapere in anticipo che una controversia simile a quelle già decise in passato avrà un'alta probabilità di essere decisa in modo conforme. Il riferirsi al precedente è senz'altro valido per fornire garanzie di uniformità di decisioni, tuttavia esso presenta alcuni limiti:

- l'affermarsi di un orientamento giurisprudenziale dipende in modo stretto dalla quantità di sentenze consultabili;

- le fattispecie che vengono sottoposte alle corti non sono mai del tutto identiche, pertanto non si fa, in realtà, riferimento alle peculiarità del caso di specie, quanto piuttosto alla motivazione e al ragionamento giuridico espressi dal precedente giudice (e, quindi, alla sua capacità persuasiva);

- e di fronte a casi del tutto nuovi - come quelli portati dall'innovazione tecnologica - la certezza del diritto non è garantita fino a che non vi sia l'affermazione di un chiaro indirizzo giurisprudenziale.

Al contrario del sistema del precedente vincolante, tipico dei sistemi di common law, nel diritto continentale si è preferito affidare la tutela della certezza del diritto alla chiarezza della norma giuridica. Nel civil law, infatti, il punto di riferimento per la decisione non è la sentenza precedentemente assunta, bensì la disposizione normativa che, in quanto generale e astratta, si può

---

[3] G. S. PENE VIDARI, "*Storia del Diritto – Età Medievale e Contemporanea*", Torino, Giappichelli, 2014.

[4] MONTESQUIEU, "*Lo spirito delle leggi*", Torino, UTET, 2005.

applicare a un numero indefinito di casi. Il precedente non è peraltro sconosciuto nel civil law, ma esso si attesta solo nella sua veste persuasiva. Ogni giudice può invero discostarsi dalle decisioni pregresse assunte dagli organi a esso superiori in virtù dell'art. 107 comma terzo Cost, salvo il rigoroso obbligo di motivare la propria diversa opinione. Tuttavia, anche la predisposizione di un insieme coerente di norme generali e astratte non è in grado di garantire in via assoluta il perseguimento della certezza del diritto. Di fronte alla norma astratta è infatti impossibile prescindere dal procedimento interpretativo, che presenta – inevitabilmente – dei margini di incertezza dovuti dalla diversa sensibilità del giudicante.

b) La giustizia predittiva

Si è detto sopra che la diversità dei giudici, intesi quali persone fisiche, incide inevitabilmente sulla possibilità di avere una giustizia predittiva. Infatti la fisiologica diversità di esperienze, formazioni, capacità e percorsi logici propri di ciascun giudice non può che portare a diverse visioni del fenomeno giuridico, con differenti ricadute sulle relative pronunce giurisdizionali. Quello che possiamo oggi porre in essere sono delle previsioni sull'esito della sentenza, da formulare sulla base di vari fattori: caratteristiche del caso di specie, orientamenti giurisprudenziali dominanti, precedenti decisioni del giudice chiamato a decidere. Appare però chiaro come prevedere l'esito di una causa non sia lo stesso che predire l'esito dello stesso processo. Infatti, mentre la previsione, basata su congetture formulate con raziocinio, può comunque essere errata, la predizione invece non può mai sbagliare, in quanto essa è l'effettiva anticipazione dell'evento futuro[5]. In questo senso pare potersi cogliere il pensiero di Max Weber che, nell'individuare il profilo di agire razionale dell'imprenditore nei confronti del diritto, parlava della necessità di una giustizia predittiva e non di una giustizia prevedibile[6].

Ad oggi, dunque, non pare ancora possibile realizzare la previsione formulata da Leibnitz secondo cui "*un giorno le parti, di fronte a una controversia, potranno sedersi a un tavolo ed effettuare un calcolo per risolvere il loro problema*"[7]. Infatti la certezza del diritto, per quanto sia un valore imprescindibile degli ordinamenti odierni, non può ancora spingersi a garantire l'assoluta uniformità di decisioni da parte dei vari organi giudicanti. Però, forse, si sta assistendo a un cambio radicale di paradigma. I progressi nel campo della robotica e dell'intelligenza artificiale hanno portato gli studiosi e gli scienziati a interrogarsi sulla possibilità effettiva di un giudice robot. In questo senso il dibattito è molto accesso sulla effettiva implementazione di giudici robot nelle aule giudiziarie (al pari della permanenza di molte altre figure legate al mondo del diritto, come gli avvocati).[8] A prescindere da come verrà gestita l'innovazione tecnologica in ambito giuridico, pare innegabile che le intelligenze artificiali avranno un ruolo (più o meno incisivo) nell'amministrazione della giustizia.

---

[5] M. DE FELICE, "*Calcolabilità e probabilità. Per discutere di 'incontrollabile soggettivismo della decisione'*" in A. Carleo (a cura di), "*Calcolabilità giuridica*", Bologna, Il Mulino, 2017, pag.40.

[6] M. WEBER, "*Economia e società*", Volume I – Teoria delle Categorie Sociologiche, Torino, Edizioni di Comunità, 1995.

[7] LEIBNIZ, "*Dissertatio de Ars Combinatoria, in Qua, Ex Arithmeticae Fundamentis*", 1666, attualmente Parigi, Hachette, 2012.

[8] Si veda M. MOCCHEGIANI, "*Algoritmi e diritto: i nuovi orizzonti (più o meno rassicuranti) della decisione robotica*", relazione al Convegno "*Decisione Robotica*" tenutosi all'Accademia dei Lincei a Roma il 5 luglio 2018.

3) Robotica e diritto: il robot come possibile giudice e interprete delle leggi

Affrontate nel paragrafo precedente le nozioni di giustizia predittiva e di prevedibilità del diritto (concetti che, come visto, non sono affatto nuovi), occorre ora trasporre tali concetti in ambito robotico.

a) Funzionamento del ragionamento robotico

Occorre preliminarmente indagare le modalità con cui il robot pone in essere i propri ragionamenti. Infatti, in quanto intelligenze artificiali, i robot effettuano dei veri e propri ragionamenti, solo con percorsi diversi da quelli della mente umana. Tali ragionamenti, pur nelle loro differenti modalità, presentano sempre due costanti:

- si svolgono mediante algoritmi, ovverosia una serie di operazioni predeterminate che pongono una successione "di regole talmente chiare, inequivoche, complete, precise da poter essere applicate in maniera immediata" e che consentono, al termine della loro esecuzione, di raggiungere un certo risultato[9];

- e hanno la possibilità di raccogliere, impiegare ed elaborare (contemporaneamente) una quantità di dati e informazioni che non è possibile per la mente umana. Si parla quindi dell'impiego di big data nell'intelligenza artificiale[10].

In particolare, il ragionamento robotico (*rectius*, dell'intelligenza artificiale) può oggi operare tramite:

1) machine learning;
2) rete neurale;
3) e deep learning.

Ciascuno di tali procedimenti robotici opera secondo alcune specificità.

1) Attraverso il machine learning, che rappresenta forse il procedimento più semplice, viene inserita nel robot una grande quantità di dati (i cosiddetti Big Data) e il programmatore pone delle regole di definizione e classificazione di tali informazioni. In questo modo, semplificando, l'I.A. procede, tramite un algoritmo, a classificare quanto in proprio possesso, fino a raggiungere una situazione in cui ogni dato viene inserito in una categoria precisa e uniforme. Tale operazione viene rappresentata tramite una struttura ad "albero", in cui i vari passaggi della categorizzazione dei dati ne costituiscono i rami, mentre i risultati finali le foglie (chiamati anche, appunto, "nodi foglia"). Il machine learning presenta però un problema non irrilevante: il cosiddetto "overfitting", ovverosia la presenza di un numero elevato di criteri di classificazione. Infatti è stato dimostrato che, all'aumentare dei criteri di definizione dei dati, non corrisponde altresì un aumentare della precisione dell'I.A. nella suddivisione delle informazioni in suo possesso.

---

[9] R. BORRUSO, "*L'impatto dell'informatica sulle professioni forensi*", pubblicato sul sito dell'Ordine degli Avvocati di Trani.

[10] Sul funzionamento del robot non si può prescindere da I. Asimov che nel racconto "Runaround" del 1941 (in italiano tradotto come "*Girotondo*" o anche "*Circolo Vizioso*") formula per la prima volta le tre leggi della robotica, ovverosia: "*1. Un robot non può recare danno agli esseri umani, né può permettere che, a causa del suo mancato intervento, gli esseri umani ricevano un danno. 2. Un robot deve obbedire agli ordini degli esseri umani, tranne nel caso che tali ordini contrastino con la Prima Legge. 3. Un Robot deve salvaguardare la propria esistenza, purché ciò non contrasti con la Prima e la Seconda legge*."

Anzi, si è visto che l'accuratezza raggiunta dalla macchina decresce oltre un certo numero di criteri di definizione. Tale fenomeno controintuitivo è quindi una caratteristica di cui tenere conto nell'applicazione del machine learning[11].

2) Mentre il machine learning è strutturato per operare tramite una sola macchina, la rete neurale prevede invece la cooperazione simultanea di diverse I.A.. Tale sistema è strutturato come una sequenza di diversi livelli, detti "neuroni artificiali", ciascuno costituito da una diversa I.A. e ognuno con un compito diverso. In particolare, i neuroni artificiali si possono classificare secondo le loro funzioni in "neuroni input", "neuroni di elaborazione" e "neuroni output". Il funzionamento dell'intero sistema si basa proprio sulla differenziazione dei compiti di questi neuroni artificiali. Infatti, per arrivare all'elaborazione del risultato finale, i neuroni input ricevono le informazioni che sono loro trasmesse e le veicolano ai neuroni di elaborazione. Tali neuroni di elaborazione (il cui numero è variabile, ma comunque superiore a due) assegnano poi dei valori ai dati ricevuti, raggruppandoli in categorie sempre più precise ad ogni passaggio, in modo non troppo dissimile dal machine learning. Infine, al termine della catena dei neuroni di elaborazione, il risultato finale viene consegnato al neurone di output, che provvede a comunicarlo all'esterno. Il passaggio dei dati attraverso più neuroni di elaborazione consente quindi di limitare il fenomeno di overfitting e di ottenere un risultato più accurato[12].

3) Infine, il deep learning (o rete neurale profonda) altro non è che l'applicazione della tecnologia della rete neurale tramite un numero elevatissimo di dati da elaborare e di passaggi da svolgere. Infatti, mentre la rete neurale si basa su di un numero di neuroni artificiali tutto sommato contenuto (nell'ordine di qualche decina) il deep learning comporta l'impiego di milioni di neuroni di connessione, con anche miliardi di relazioni tra loro. Questa estrema capillarità dei collegamenti tra i neuroni conferisce la possibilità di analizzare una grande quantità di dati, con un livello di accuratezza molto elevato[13].

b) Applicazione del ragionamento robotico al diritto

Come visto, il ragionamento robotico opera tramite algoritmi e Big Data. Dunque, affinché il robot possa operare con il diritto, è necessario che esso possa comprendere il fenomeno giuridico. È fondamentale che il diritto sia traducibile in un linguaggio comprensibile alla macchina la quale, come visto, elabora Big Data tramite algoritmi. Sul punto, non paiono sorgere problemi circa l'individuazione di Big Data in ambito giuridico: basti pensare a quante nuove normative vengono costantemente emanate o, ancora, all'elevato numero di pronunce giurisdizionali a cui è possibile accedere. Se quindi i Big Data sono presenti nel diritto, occorre allora soffermarsi circa la configurabilità dei procedimenti giuridici come algoritmi.

---

[11] Per una introduzione semplice e intuitiva del machine learning si veda *http://www.r2d3.us/una-introduzione-visuale- al-machine-learning-1/*, nonché *http://www.r2d3.us/visual-intro-to-machine-learning-part-2/*.

[12] Si veda http://www.intelligenzaartificiale.it/reti-neurali/.

[13] S. CAVALLI e L. FERRAROTTI, "*Deep Learning*", 2015, in https://areeweb.polito.it/didattica.

La presenza di algoritmi nell'ordinamento giuridico non è esclusa dalla dottrina. Ricordando la definizione di algoritmo sopra data[14], essa non pare, nella sua struttura logica, discostarsi dall'interpretazione di un fatto storico, la quale richiede una serie di passaggi ben precisi[15]. Infatti, di fronte a una fattispecie da inquadrare giuridicamente, occorre innanzitutto ricostruire il fatto storico, individuare poi la disposizione di riferimento (o, se questa manca, adoperare i canoni interpretativi a nostra disposizione) e, una volta ricavata la norma, applicare la regola alla fattispecie[16]. Un esempio forse ancora più lampante è costituito dal processo di fronte all'autorità giudiziaria. Dopotutto ogni processo - a prescindere dalla giurisdizione - è costituito da una serie di passaggi predefiniti e posti in una sequenza obbligatoria, al cui termine viene emessa una sentenza, che rappresenta il risultato di tutte le operazioni del processo. La struttura processuale è quindi un algoritmo[17] e, come tale, comprensibile per un robot.

Alcuni studiosi si sono poi spinti sino a scrivere il procedimento interpretativo come una formula matematica (la quale rappresenta l'algoritmo per eccellenza). In particolare, è stata proposta una vera e propria equazione per ricavare la norma da applicare al caso di specie[18]. Brevemente, tale interessante equazione traduce in linguaggio matematico i dettami interpretavi posti dal Legislatore con l'art. 12 Preleggi[19]: di fronte a un caso occorre individuare la disposizione che lo regola, e, in primo luogo fare riferimento al significato letterale delle parole e, in subordine, orientare l'interpretazione alla *ratio* con cui la disposizione è stata scritta. Solo se non presente una disposizione che regoli il caso o se essa, seppur presente, non sia univocamente interpretabile, sarà allora possibile adoperare (prima) l'analogia *legis* e (dopo) l'analogia *iuris*. Benché non sia questa la sede per approfondire questa nuova tipologia di indagine giuridica, pare innegabile che tale concezione matematica sia fondamentale per la possibilità di un robot interprete e, perfino, giudice del diritto. Infatti la formula matematica è quanto di più comprensibile ci sia per l'I.A., la quale potrebbe quindi adoperare la formula matematica per rivolvere le questioni giuridiche che le vengono sottoposte.

c) Prevedibilità delle decisioni robotiche come caratteristica del giudice robot

Se è possibile la traduzione del fenomeno giuridico in un linguaggio comprensibile per un robot, allora è altrettanto possibile l'applicazione dell'I.A. nell'amministrazione della giustizia. Anzi, i recenti sviluppi fanno pensare che sia solo una questione di tempo prima che l'I.A. applicata al diritto faccia il proprio ingresso nei tribunali[2021]. Nonostante i veloci progressi compiuti dalla tecnologia, ad oggi non si è in grado di stabilire se, effettivamente, in futuro le nostre corti saranno presiedute da giudici robot.

---

[14] Vedi supra nota n. 9.

[15] R. BORRUSO, ult. op. cit..

[16] F. MODUGNO, "*Interpretazione Giuridica*", Padova, Cedam, 2012.

[17] L. VIOLA, "Interpretazione della legge con modelli matematici – Processo, A.D.R., giustizia predittiva", Milano, Centro Studi Diritto Avanzato Edizioni, 2018.

[18] L. VIOLA, ult. op. cit..

[19] L'art. 12 delle Preleggi dispone: "*1. Nell'applicare la legge non si può ad essa attribuire altro senso che quello fatto palese dal significato proprio delle parole secondo la connessione di esse, e dalla intenzione del legislatore. 2. Se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe; se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato*."

Quello che oggi sembra lo scenario più verosimile è quello dell'I.A. come assistente del giudice umano, in grado di fornirgli un accesso chiaro e ordinato alle (sempre più sterminate) fonti del diritto. In ogni caso, visto che l'evoluzione tecnologica è solita sovvertire le previsioni che le vengono rivolte[22], pare utile porsi sin da ora il problema delle decisioni di un eventuale prossimo giudice robot.

In questo senso, sulla base delle nostre conoscenze sulla robotica, possiamo considerare da due fattori che potrebbero essere costanti:

1) che il robot difficilmente potrà replicare il giudice umano;

2) e che le decisioni del robot, in quanto frutto di processi algoritmici, sarebbero maggiormente legate alla modifica della sua programmazione rispetto alla molteplicità di casi da risolvere.

1) Le conseguenze legate a questo aspetto della robotica sono molteplici e non possono essere analizzate compiutamente in questa sede. Pare però necessario evidenziare che questa differenza tra essere umano e robot è legata essenzialmente a un fattore: la presenza di una pregressa programmazione in senso tecnico. Infatti, benché in un certo senso anche l'essere umano subisca una "programmazione"[23], quest'ultima non è vincolante per una persona, consentendole di parametrare il proprio agire sulla base delle particolarità di ogni situazione. Al contrario, un robot non può prescindere dalla propria programmazione: non può contraddirla ma solo agire secondo essa. Naturalmente è possibile raffinare sempre di più gli input e gli algoritmi adibiti ad elaborarli, ma difficilmente si potrà avere una potenza di calcolo tale da prevedere ogni possibile fattispecie da decidere[24]. In altre parole, mentre un essere umano, posto di fronte a una situazione nuova, potrà affrontarla adattandosi all'ambiente, il robot potrà invece risolverla solo se la sua programmazione prevede quella specifica situazione, altrimenti esso non potrà agire[25]. Ne consegue che il robot non sarebbe in grado di affrontare casi nuovi e, quindi, si avrebbe come ulteriore conseguenza il venire meno di quella spinta innovativa che negli anni ha portato, grazie alla giurisprudenza, alla nascita di nuovi diritti[26]. A questa ricostruzione pare peraltro possibile un'obiezione: se l'algoritmo del robot non prevede come risolvere la nuova situazione, sarebbe allora sufficiente riprogrammare l'I.A. aggiornando l'algoritmo stesso. Tuttavia tale soluzione non risolve il problema, anzi lo complica.

---

[20] Negli studi legali il fenomeno sta già prendendo piede, si veda M. IASELLI, "*Robot lawyer: nuovi progressi dell'intelligenza artificiale nel settore legale ma...*" in www.altalex.it.

[21] Tra le prime in Italia ad effettuare una sperimentazione simile vi è la Corte d'Appello di Brescia, su cui si veda la relazione di C. Castelli e D. Piana, "Giustizia predittiva. La qualità della giustizia in due tempi" su *Questione giustizia on line*, 15 maggio 2018, www.questionegiustizia.it/articolo/giustizia-predittiva-la-qualità-della-giustizia-in-due-tempi:15-05-2018.php; nonché C. Morelli, "Giustizia predittiva: il progetto (concreto) della Corte d'appello di Brescia" inwww.altalex.it.

[22] Gli esempi sono i più disparati, dalla diffusione delle automobili ai telefoni cellulari.

[23] Lo stesso Sigmund Freud, con la sua teoria della psicanalisi, individuò come parte fondamentale della mente umana il Super-Ego, ovverosia il condizionamento psichico che le varie sovrastrutture sociali esercitano sull'individuo. S. FREUD, "*L'interpretazione dei sogni*", Torino, Bollati Boringhieri, 2011.

[24] Per fare un parallelismo con le scienze fisiche, si ricordi il principio di aumento dell'entropia formulato da Rudolf Clausius, per cui in un sistema le variabili da calcolare sono imprescindibili dall'entropia (ovverosia il disordine del sistema stesso), la quale aumenta con il semplice passare del tempo. In altre parole, la quantità di entropia in un sistema è destinata ad aumentare e, con essa, l'ammontare delle variabili da calcolare. Per approfondire http://www.fe.infn.it/u/ciullo/fisica_mate/Disuguaglianza_di_Clausius-dispensa.pdf.

Occorre infatti ricordare che ogni aggiornamento dell'algoritmo deliberativo presuppone un intervento esterno al robot. Tale intervento sarebbe eseguito necessariamente da un essere umano, in quanto è dalla nostra opera che discende l'I.A. stessa. Questa dinamica comporterebbe però, di fatto, l'esternalizzazione della decisione giudiziaria, ponendola in capo allo stesso programmatore dell'algoritmo. Una simile allocazione della decisione non sarebbe rispettosa dei principi costituzionali che regolano il nostro sistema giudiziario e che impongono al giudice, non a soggetti esterni, di decidere la controversia. Pertanto, non sembra possibile la sostituzione integrale dell'essere umano nel ruolo del giudice.

2) Come visto, la natura dell'algoritmo presuppone una ripetitività di operazioni sempre identiche, le quali a loro volta porteranno sempre a uno stesso risultato. Mentre quanto appena visto al punto 1) ha una connotazione tendenzialmente negativa, invece l'uniformità delle decisioni robotiche potrebbe rappresentare un vantaggio. Se infatti il robot non potesse occuparsi di casi nuovi o di quelli che coinvolgono principi etici, la risoluzione di controversie di modesto valore e di limitata complessità potrebbe trovare un vantaggio nell'essere affidata a un'I.A.. Ad esempio, sarebbe forse possibile affidare l'emanazione dei provvedimenti monitori (che rappresentano un importante carico di lavoro per i tribunali) a un robot, il quale potrebbe decidere se emettere il decreto ingiuntivo in completa autonomia. Tuttavia l'emissione del decreto ingiuntivo non sarebbe l'unico ambito di operatività del giudice robot: esso potrebbe anche trovare spazio in tutti quei procedimenti caratterizzati da una bassa "discrezionalità" del giudice, ovverosia quando il magistrato deve sostanzialmente verificare la conformità di una situazione rispetto a un chiaro quadro normativo (si pensi alle opposizioni alle sanzioni amministrative relative alle violazioni del Codice della Strada).

In conclusione, benché non paia possibile l'integrale robotizzazione della magistratura, non è da escludere un ruolo sempre più importante dell'I.A. all'interno dell'amministrazione della giustizia. Proprio a causa di questa prevedibile diffusione sembra opportuno analizzare nel prossimo paragrafo un "caso limite" che potrebbe essere interessante: la possibile proposizione di una questione di legittimità costituzionale da parte di un giudice robot.

4) Il giudice robot di fronte alla questione di legittimità costituzionale della legge

a) La struttura logico-giuridica della remissione alla Corte Costituzionale[27]

Com'è noto, nel nostro ordinamento il controllo sulla legittimità delle leggi non è affidato al sindacato diffuso di tutti i componenti della magistratura (come avviene invece nei sistemi giuridici di Common Law). Infatti la Costituzione Italiana ha disposto che l'unico ente in grado di pronunciarsi sulla costituzionalità di un atto normativo sia la Corte Costituzionale[28]. Tuttavia, se formalmente il controllo sulla legittimità è accentrato in un unico organo, la nostra carta fondamentale ha in realtà previsto una sorta di controllo "decentrato".

---

[25] Si pensi all'esperimento tenutosi nel 2014 presso i Bristol Robotics Laboratory dall'equipe del prof. Alan Winfield, in cui un robot, dovendo scegliere chi salvare tra due automi (che simulavano due esseri umani) in pericolo non riusciva, quasi nel 50% dei casi, a decidere chi salvare per primo, cagionando così la "morte" dei robot in pericolo. Si veda https://www.bristolroboticslab.com/.

[26] Si pensi alla privacy o, ancora più recente, al diritto all'oblio.

[27] Per semplicità espositiva e per attinenza al tema trattato, si farà riferimento alla sola remissione da parte della magistratura e non alle altre forme di controllo esercitate dalla Corte Costituzionale.

[28] L'art. 134 della Costituzione recita infatti: "*la Corte Costituzionale giudica sulle controversie relative alla legittimità costituzionale delle leggi e degli atti, aventi forza di legge, dello Stato e delle Regioni* (...)".

Ogni magistrato può infatti sollevare alla Corte Costituzionale la questione di legittimità costituzionale di una norma che deve applicare per risolvere il caso che è chiamato a decidere. In questo modo si è cercato di valorizzare la funzione di "vigilanza" del potere giudiziario sulla correttezza delle disposizioni emanate sia dal potere legislativo sia dal potere esecutivo (funzione che deriva proprio dal pensiero di Montesquieu, già citato)[29].

In ogni caso, pur con la funzione di salvaguardare i principi della nostra Costituzione, il magistrato non è libero di sollevare la questione di legittimità costituzionale *ad nutum*. Egli è infatti soggetto a particolari requisiti, che trovano la propria fonte sia nella Costituzione sia nell'elaborazione giurisprudenziale della Corte Costituzionale[30]. In particolare, per brevità, il magistrato può sollevare la questione alla Corte Costituzionale se egli:

- dubita della legittimità di una norma di legge alla luce dei principi costituzionali;

- deve pronunciare sentenza nel corso di un procedimento in cui sia coinvolta la norma la cui legittimità è in dubbio (non è quindi possibile, per il magistrato rimettente, sollevare questioni in via indipendente dalla decisione di un processo);

- e non ravvisi la possibilità di un'interpretazione costituzionalmente orientata della norma sospettata di illegittimità[31].

Tra questi requisiti quello che suscita il maggiore interesse in ambito robotico è il necessario dubbio di legittimità, che non è affatto scontato sia replicabile (o quantomeno simulabile) in un'I.A..

b) In particolare, la natura del "dubbio" interpretativo

Cosa significa dubitare di una disposizione di legge? La domanda, prima che giuridica, è filosofica. La parola "dubbio" è intrinsecamente legata alla presenza di (almeno) due possibilità. Infatti, etimologicamente, la parola "dubbio" ha come radice "*du*", derivante dal greco "*duos*", ovverosia il numero due in greco[32]. Inoltre il dubbio è tale proprio perché le alternative che esso coinvolge sono sostanzialmente equiparabili. Come si potrebbe parlare di dubbio quando una delle opzioni possibili sia manifestamente preferibile all'altra? Infine, la soluzione del dubbio (o inteso anche come dilemma) è raramente rinvenibile dal solo soggetto che pone il dubbio. Anzi, solitamente la risoluzione del problema è demandata a un soggetto terzo che, per le proprie qualità, è in grado di prendere una decisione.

Tanto chiarito in via generale, in ambito giuridico è possibile parlare di dubbio "interpretativo". Esso sorge quando, dall'applicazione dei canoni ermeneutici alla disposizione, non emerge una soluzione chiara e univoca. Si pensi ad esempio al caso in cui una stessa disposizione (magari a causa di una leggerezza del legislatore) è scritta in modo tale da ricavare più significati possibili dall'insieme delle sue parole ai sensi dell'art. 12 Preleggi. In questa circostanza, in considerazione dell'obbligo di pronunciarsi a cui è soggetto il giudice, è comunque necessario pervenire a una decisione scegliendo, tra quelle possibili, la più coerente con i principi dell'ordinamento. Da ciò il detto "decidere è scegliere"[33].

---

[29] MONTESQUIEU, ult. op. cit..
[30] R. BIN e G. PETRUZZELLA, "*Diritto Costituzionale*", Torino, Giappichelli, 2018.

[31] L. IANNICUCCILLI, "*L'interpretazione* secundum costitutionem *tra Corte Costituzionale e giudici comuni – brevi note sul tema*" in *https://www.cortecostituzionale.it/documenti/convegni_seminari/Interpretazione_quaderno_stu.pdf*.

[32] N. IRTI, "Un diritto incalcolabile", Torino, Giappichelli, 2016, pag. 117 e ss.. / [33] A. CARLEO (a cura di), "Calcolabilità giuridica", Bologna, Il Mulino, 2017.

In particolare, se il dubbio interpretativo può nascere dalla lettura di una sola disposizione, nel caso della remissione alla Corte costituzionale è ovviamente necessario procedere in modo più articolato. Infatti non è solo necessario interpretare la singola disposizione (fugando nel mentre eventuali dubbi), ma anche compararla con la norma costituzionale che si intende violata. Da ciò discende che occorrerà:

- in primo luogo individuare la norma di rango costituzionale;

- in secondo luogo interpretare la disposizione da applicare;

- in terzo luogo, se i due risultati non sono coordinati (ferma la prevalenza della norma costituzionale), verificare la possibile interpretazione costituzionalmente orientata della disposizione "sospetta";

- e infine, se non emerge una soluzione ammissibile per l'ordinamento, sollevare la questione di legittimità alla Corte Costituzionale.

c) Può il giudice robot dubitare della legge?

Le considerazioni che precedono conducono quindi alla domanda principale di questo lavoro: ammettendo la configurabilità di un giudice robotico, questo potrebbe dubitare della legge che è chiamato ad applicare, tanto da sollevare la questione di legittimità costituzionale?[34]

Per rispondere, è opportuno ricordare brevemente il funzionamento della mente robotica. In particolare:

1) che il ragionamento robotico è lineare e pensato per giungere a una soluzione univoca;

2) e che il robot non è in grado di operare da solo, ma necessita sempre di un insieme di dati e di regole per elaborarli.

In merito al primo punto, pare che una I.A. non possa realmente esprimere un dubbio di fronte al problema che deve risolvere. Se, come visto, il dubbio è la contemporanea presenza di due o più alternative possibili e sostanzialmente equivalenti, il robot ha bisogno di una regola che gli fornisca un criterio di preferenza tra le scelte. Non si crea quindi un vero e proprio dubbio, quanto piuttosto una risoluzione immediata del problema tramite l'applicazione di un criterio preferenziale etero-imposto. Tuttavia questa operazione può funzionare solo se le regole del robot sono in grado di coprire tutti i casi che esso è chiamato a risolvere. Se, invece, la macchina si trova di fronte a una situazione in cui essa ha di fronte a sé più alternative equivalenti senza un criterio preferenziale, allora essa andrà in crisi e non potrà scegliere da sola la soluzione da adottare[35]. Sul punto, si potrebbe però obiettare che nel diritto esistono dei criteri interpretativi certi a cui fare riferimento, fissati dall'art. 12 Preleggi. Infatti è sulla base di tale articolo che è stata elaborata la formula matematica di cui sopra sull'interpretazione della legge. Pertanto, in ipotesi, sarebbe possibile che l'operatore si limitasse a riprodurre i criteri legali d'interpretazione nel programmare il robot, eliminando così il rischio di un "blocco". Non pare tuttavia che una simile impostazione sia in grado di superare il problema. È noto infatti che gli operatori giuridici adoperano, oltre ai criteri legali, anche altri criteri interpretativi non espressamente scritti nella legge: si pensi al criterio storico o a quello "per assurdo". Inoltre, mettendo in disparte le disposizioni scritte, si pone il problema dell'interpretazione dei principi e dei valori giuridici.

---

[34] Ovviamente presupponendo che, in quanto raggiunto lo status di magistrato, il robot possa proporre la questione di legittimità esattamente come l'essere umano.

[35] Si veda *supra* nota n. 25.

In questo caso non è applicabile tout-court il disposto dell'art. 12 Preleggi (manca un testo scritto da cui partire), bisogna invece fare riferimento a criteri di sistema, a volte anche extra-giuridici[36]. Il robot però non può comprendere i principi e i valori dell'ordinamento, in quanto non sono "scritti" in un linguaggio comprensibile alla macchina. Sarebbe quindi necessario che qualcuno "traduca" i principi e i valori giuridici per l'I.A..

Questo consente di analizzare il secondo punto sopra evidenziato: qualunque sia la modalità di ragionamento adottata dal robot, essa presuppone sempre, a monte, un intervento di programmazione. Allo stato, questo significa che il robot non può operare autonomamente senza dati forniti dall'esterno e senza gli algoritmi disposti dal programmatore. Questa circostanza, che in ambito tecnico può sembrare una semplice conseguenza operativa, ha invece degli importantissimi risvolti in ambito giuridico.

Infatti, da quanto appena detto discende che il robot non potrà mai giungere da solo a una interpretazione del testo legislativo, ma muoverà sempre:

- dai dati che gli vengono messi a disposizione;

- e dall'algoritmo con cui il robot viene programmato, ovverosia dalle regole di preferenza che gli vengono impartite.

Sul punto, le perplessità che emergono sono numerose. In primo luogo, allora sarebbe possibile condizionare la scelta del robot fornendogli, come dati da elaborare, soltanto informazioni giuridiche parziali. In secondo luogo, si avrebbe l'indesiderabile effetto di "spostare" l'effettiva decisone del caso dal robot (magistrato) al suo programmatore: sarebbe infatti quest'ultimo che, scrivendo l'algoritmo, deciderebbe in anticipo come la propria macchina risolverà un certo problema. Tali questioni espongono il fianco a incisive censure di costituzionalità nella parte in cui consentono che la decisione giurisdizionale sia presa da soggetti (quali i programmatori) non titolati per adottarla. Per esemplificare il quadro che ci si potrebbe trovare ad affrontare, si pensi al frequente caso di contrasto di orientamenti giurisprudenziali sull'interpretazione di una disposizione. Affidando la composizione del contrasto al robot la si affiderebbe in realtà al programmatore perché:

- sarebbe il programmatore a decidere quali sentenze "caricare" nell'I.A., con il rischio di inserire un maggior numero di casi di un orientamento rispetto a un altro, ledendo quindi l'imparzialità del giudicante;

- e sarebbe sempre il programmatore a scrivere l'algoritmo che risolverebbe il contrasto, per cui egli ben potrebbe scrivere il codice favorendo un preciso orientamento piuttosto che un altro.

Le criticità appena evidenziate non sono in realtà nuove in ambito robotico. Molti studiosi si sono infatti già interrogati sulla riferibilità dell'azione robotica e sulle sue conseguenze. Si tratta del cosiddetto fenomeno del "*picciotto robotto*": se si programma un robot per uccidere, il programmatore è (in teoria) responsabile degli omicidi come se, al posto del robot, avesse usato un fucile[37].

Le considerazioni appena svolte consentono già di per sé di escludere che il robot possa genuinamente dubitare della legge e, di conseguenza, sollevare la questione di legittimità costituzionale.

---

[36] G. ZAGREBELSKY, "*La legge e la sua giustizia*", Bologna, il Mulino, 2017.

[37] U. PAGALLO, "*The Laws of Robots – Crimes, contracts and torts*", Londra, Springer, 2013.

Occorre peraltro segnalare un'altra circostanza ostativa alla questione di legittimità "robotica", specifica per questa remissione. La nostra Costituzione ha il compito di tutelare i diritti fondamentali della persona, la cui protezione investe spesso anche questioni morali, non soltanto giuridiche. Nel decidere su tali questioni, il giudice non è un mero operatore del diritto chiamato a effettuare un calcolo, ma deve invece farsi interprete del diritto anche alla luce dell'evoluzione del sentire sociale. In tal senso sono emblematici i casi relativi alla questione del fine vita prima che entrasse in vigore l'attuale legge sul bio-testamento[38]. Casi simili non si risolvono con una semplice operazione matematica sulla base della norma da applicare, ma richiedono un attentissimo bilanciamento tra i valori del nostro ordinamento, i quali non possono mai essere elisi del tutto[39]. Inoltre tali operazioni di bilanciamento non potrebbero essere condotte dal robot perché esso, come detto, non sarebbe in grado di capire i principi e i valori generali non scritti, ma gli dovrebbero essere "suggeriti" dal suo programmatore.

In conclusione, l'eventuale giudice robot non potrebbe quindi sollevare la questione di legittimità alla Corte costituzionale. E questo perché:

- non è in grado di dubitare della legge che deve applicare;

- e non può, da solo, comprendere i principi e i valori dell'ordinamento, inderogabili parametri di riferimento per la costituzionalità delle disposizioni.

5) Conclusioni

Le osservazioni appena svolte, pur nella loro brevità, hanno mostrato come l'eventuale giudice robot non possa spingersi sino a sollevare una questione di legittimità alla Corte Costituzionale. In sede conclusiva sembra tuttavia esserci spazio per alcune considerazioni "*de jure condendo*".

In primo luogo, si rammenta che il presente lavoro è tarato sulla tecnologia oggi esistente e, pertanto, le relative conclusioni sono limitate allo stato attuale delle ricerche sull'intelligenza artificiale. Tale considerazione, che parrebbe pleonastica in altri ambiti, non lo è invece per la scienza robotica. Infatti questo ramo del sapere, seppur nato da poco[40], ha visto uno sviluppo eccezionale in un arco di tempo molto ristretto. Gli approdi delle ricerche sull'intelligenza artificiale sono continui e quasi ogni giorno vi sono importanti avanzamenti. Tale velocità del progresso robotico non esclude pertanto che, un domani - forse neanche troppo lontano - si riuscirà a sviluppare una vera Intelligenza Artificiale, in grado di replicare esattamente il cervello e il pensiero umano. Una simile tecnologia porterebbe con sé delle implicazioni enormi (una su tutte: diverrebbe possibile, alla morte, trasferire la nostra mente in un robot per ottenere l'immortalità?), che non possono essere affrontate oggi. Tuttavia, in tale scenario "fantascientifico" diverrebbe allora possibile, per quanto qui rileva, che il robot sostituisca integralmente il giudice umano nelle sue funzioni. E questo perché, ottenendo l'autonomia di ragionamento tipica del pensiero umano, il robot verrebbe svincolato dalle attuali regole.

---

[38] Ora si veda la legge n. 219 del 22 dicembre 2017, pubblicata sulla Gazzetta Ufficiale della Repubblica Italiana del 16 gennaio 2018.

[39] M. DOGLIANI (a cura di), "*Il libro delle leggi strapazzato e la sua manutenzione*", Torino, Giappichelli, 2012.

[40] Le prime applicazioni della robotica risalgono al braccio meccanico per uso industriale progettato da Joseph Engelberger e George Devol ed entrato in funzione nel 1961 presso la General Motors.

Infatti:

- il robot non sarebbe più limitato dalle informazioni fornite dal programmatore (potendosene procurare di nuove);

- e il robot potrebbe arrivare a superare la propria programmazione originaria (evolvendosi e e "adattando" da solo i propri algoritmi).

In tale futuribile scenario l'interpretazione del diritto da parte del robot sarebbe, forse, questione talmente ovvia da non richiedere particolari attenzioni.

In secondo luogo, immaginando invece un orizzonte degli eventi più verosimilmente vicino a noi, l'adozione di intelligenze artificiali a supporto dell'autorità giudiziaria è senz'altro un tema da porsi. È pacifico infatti che la nostra società si stia informatizzando sempre più e che tenda a realizzare una tecnologia volta ad assistere - non a sostituire - l'essere umano, per sgravarlo dai compiti più tediosi e faticosi,[41] ovvero per migliorare le sue prestazioni in alcuni ambiti[42]. In questo senso non è difficile immaginare che, nei prossimi anni, ci saranno intelligenze artificiali a supporto dei magistrati, col compito di facilitare il compito di ricerca giuridica, di analisi dei documenti e di stesura della sentenza. Del resto, come detto sopra, simili tecnologie sono già oggi adoperate da alcuni studi legali[43]. Inoltre, in alcuni fori la sperimentazione di alcune forme di intelligenza artificiale è già realtà[44].

In conclusione, il progresso tecnologico a cui stiamo assistendo, senza precedenti nella storia umana, ci pone davanti a orizzonti estremamente stimolanti e, al contempo, forieri di quesiti etici, morali e giuridici mai visti prima. Sarà quindi compito nostro decidere come dirigere il futuro sviluppo della robotica in ambito giuridico, magari proprio come avrebbe voluto Leibniz, sedendoci a un tavolo e operando un calcolo.

---

[41] Gli esempi più immediati vanno ai robot nelle fabbriche o, più semplicemente, ai robot aspirapolvere.

[42] Si pensi ai robot chirurghi che aumentano la precisione del medico o, addirittura, lo sostituiscono.

[43] Si veda M. IASELLI, ult. op. cit..

[44] Si ricorda il programma avviato dalla Corte d'Appello di Brescia (v. *supra* nota n. 21), mentre negli Stati Uniti molte Corte adoperano il programma Compas, il quale però ha sollevato non poche polemiche con il caso "Loomis".

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA
NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

SPONSORED BY

ASSOCIAZIONE GIOVANI AVVOCATI TORINO

BLOCKCHAINS AND SMART CONTRACTS: GENERAL OVERVIEW, AND ASPECTS OF GOVERNANCE AND LIABILITY

DI LUIGI CANTISANI, LL.M. - SUSHMA SATHYANARAYANAN, LL.M.

Index

Introduction

‘Blockchain’ is the new buzzword in the technology sector. It has come to the forefront in recent years. The topic that was interesting to a specific group of technology enthusiasts, has now taken the interest of people of various streams, learning and incorporating it into their businesses. Blockchain, in simple words, is a distributed ledger, meaning it is a list of transactions that are distributed over a network of computers rather than being stored on a single network/server. It is a general-purpose tool for creating a peer-to-peer application that is secure and decentralized.

Though the concept of a distributed ledger technology (hereinafter also referred to as the ‘DLT’) is not new, it became more popular with the invention/creation of ‘bitcoin’, a currency that could be traded digitally through the blockchain. The credit of the creation of bitcoin goes to researcher(s) under the pseudonym of Satoshi Nakamoto.[1] Though recently in May 2019, one Craig Write claims that he is Satoshi and to prove this, he has copyrighted the original white paper of bitcoin; and many of the technology enthusiasts have refuted his claim saying that anyone can get a copyright and that the Copyright Office in the USA does not go to the lengths to verify the credibility/ authenticity of such claims.[2]

While we discussed how blockchain came to the limelight, we need to know what blockchain is, how does it work and if it is a legally valid mode of transaction. The main objective of blockchain was to establish a peer-to-peer transaction system whereby effectively eliminating the need to have intermediaries. There are various claims that blockchain does not only mean bitcoin or other cryptocurrencies,[3] but it can be used in various businesses including simple day-to-day applications. Many media houses covered blockchain as the ‘next big thing’ in the technological revolution that is happening.[4]

Broadly speaking, blockchain is a network of data that is spread across multiple systems, stored in sync with all the systems with no single point of ownership. Any data addition is based on some type of consensus mechanism where all the other systems on the network called ‘nodes’ approve the data entered and then a block is created. Any unauthorized modification to an existing block triggers a warning to all the other nodes on the network. This ensures that the existing blocks are not tampered, and that any new data entered is stored only on the approval of the majority of the nodes to authenticate the modification.

---

[1] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008.

[2] *See*, https://news.bitcoin.com/us-copyright-office-responds-to-craig-wrights-bitcoin-registrations/.

[3] A cryptocurrency is a digital currency issued through a cryptography-based system. A digital or virtual currency can be defined as a “medium of exchange existing entirely in intangible form that is not legal tender, but which can substitute for legal tender.” See Hughes S. J., Middlebrook S. T., Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries, in Yale Journal on Regulation Volume 32 (New Haven, Connecticut, United States, 2015), 504, available at http://yalejreg.com/.

[4] *See*, among the other, https://www.catalysts.cc/en/big-data/blockchain-the-next-big-thing/.

The next main aspect of this technological revolution we as attorneys look at is smart contracts. Smart contract is a technology that gained traction with the development and popularity of blockchain, though as a concept, 'smart contract' is decades old. The concept of smart contracts was delivered by Nick Szabo, who said that a contract can be converted into a computer code to ensure an automatic execution.

Many are of the opinion that this is the underlying idea behind the vending machines, where we insert money and get the desired product, an automatic execution where there is no need for further assistance. The evolution of blockchain facilitated the practical application of self-executing transactions further from just vending machines, where regular documents can be converted into codes and hosted on secure platforms for its execution. These documents can be hosted on specific blockchain networks, which are secure and tamper-proof.

In 1994, Nick Szabo defined smart contracts "*as a set of promises, specified in digital form, including protocols within which the parties perform on the other promises. He also said that the smart contracts would enable a self-enforcing contract, where both parties could observe and verify the performance of the contract*".[5] They are event- driven codes where the prerequisites/conditions of the execution of the contract are already programmed and upon meeting the aforementioned criteria, the contractual obligation is performed.

While all of this is a step forward, a major hindrance that many nations are facing at the moment that is stopping a widespread use of blockchain system is the lack of clarity in the legality of its use. While there are many rules and regulations governing various aspects of every transaction or business, there is no rule-set that governs the use and implementation of blockchain or the distributed ledger technology in general. Many nation-states such as the United States of America (hereinafter referred to as "USA"), various nations in the European Union (hereinafter referred to as "EU"), Middle Eastern, and Asian nations have taken steps towards creating rules that determine the legality of blockchain and its uses. An early example in legalizing blockchain and its associated uses is from UNCITRAL:[6] this organization is working on soft law on the role of electronic communication and e-commerce and trying to frame the formation of a smart contract as an offer and acceptance in a transaction which are expressed and stored in a block.[7]

---

[5] *See*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/ LOTwinterschool2006/ szabo.best.vwh.net/smart_contracts_2.html.

[6] 'UNCITRAL' means the United Nations Commission on International Trade Law (UNCITRAL), an organization established by the United Nations General Assembly by resolution 2205 (XXI) of 17 December 1966 (see annex I), whose mandate is to further the progressive harmonization and modernization of the law of international trade by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law.

[7] *See,* http://cornellilj.org/smart-contracts-another-feather-in-uncitrals-cap/

When speaking of transactions on a blockchain or smart contracts, we need to look closely on some of the fundamental legal issues we will face during the transactions. We know that all contracts are bound by a geographical location or a jurisdiction to handle any disputes/issues if it arises, the inherent nature of blockchain being borderless creates a unique problem; but many of the users say that a code can be inserted specifying the jurisdiction on where the dispute will be resolved. This seems like a stop-gap solution that many of them are willing to try and create smart contracts accordingly.

The bigger question is in manifolds of (a) who is liable or responsible when something goes wrong in a blockchain/smart contract-based transaction? (b) Can we use the existing laws that govern liability put in place for these transactions as well? (c) Can we have a smart contract in place listing out the liability of each party to the transaction; if so, which party's law/jurisdiction will be applied to make this determination? (d) Even if we do have the liabilities listed out, can it be held right in a court of law?

This paper deals with the interrelationships between blockchain, smart contracts, and certain elements of liability, intending to clear the clutter and give some clarity on the existing realities. Before we get to the part of untangling the lights, we need to see the technical aspects of the blockchain technology, determining the governance of the blockchain and so the management of the smart contracts that run on it. Also, we aim to examine how the world has fared in creating a valid legal space for these technological advancements.

1. The governance of the blockchains

In order to examine the notion of liability within a blockchain-based system, it is important to first map the players involved in the use and governance of a blockchain.

The functioning of a blockchain involves a network of participants interested in concluding transactions based on the cryptocurrency issued on that very blockchain. It is a peer-to-peer network,[8] in simple terms a network where the computers are connected together in an equal way and contribute to maintain the blockchain infrastructure by providing the computational power. They constantly exchange the latest blockchain data with each other, so all nodes stay up to date.

Maintaining the infrastructure essentially means exchanging data, storing and validating transactions taking place on the blockchain. Usually, each computing device that contributes to the maintenance of the blockchain is deemed to be node. Generally speaking, nodes operate and validate transactions according to the consensus algorithm adopted by the blockchain.

For instance, in the Bitcoin's blockchain the so-called "full node" is a complete copy of the blockchain and is able to verify all transactions since the beginning, and then relay them to other nodes. A "pruning node" is one that has verified all prior transactions; however, it has deleted all blocks below a certain space requirement, but still has a copy of the UXTO set. It is almost useless to the community but takes less resources on the computer (can be under 1GB of drive space). A "mining node" or, simply, a "miner" is a node that extends the chain by creating new blocks with the new transactions relayed from other nodes.

---

[8] Schollmeier R., *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications*, in *Proceedings of the First International Conference on Peer-to-Peer*

Computing (Piscataway, New Jersey, United States, 2001), 101-102. Also see, Saroiu S. P., Gummandi K., and Gribble S. D., *Measurement Study of Peer-to-Peer File Sharing Systems*, in *SPIE Proceedings of Multimedia Computing and Networking*, Volume 4673, 2002 (San Jose, California, United States, 2001), available at http://dx.doi.org/10.1117/12.449977.

When a miner attempts to add a new block to the chain, it broadcasts the block to all the nodes on the network. Based on the block's legitimacy (validity of signature and transactions), nodes can accept or reject the block. Each node decides irrespective of how other nodes act. The consensus algorithm adopted by Bitcoin is named "proof-of- work" and it provides that the participants in the blockchain invest resources - i.e. computational power and consequently electricity (sometimes jointly referred to as 'mining power') - to solve a computational puzzle, before proposing a valid block. Miners are rewarded in cryptocurrency for their activities. The cryptocurrency is generated by the algorithm that governs the blockchain. The new block created at the end of this process is stored by the other types of node so as to verify it with other nodes in the future, while miners do not need to know about all prior blocks (except for the prior one) with very few exceptions.

Theoretically, a blockchain could run on a single node, but in such a case, it would be extremely vulnerable to things like power outages or cyber-attacks. Above all, such a restriction would not make any sense, economically speaking. The Bitcoin's blockchain has basically introduced a model for decentralizing sharing economy,[9] a model in which each participant gives something (computing power, and so energy consumption) in return for something (a cryptocurrency), without the process being governed by a central authority acting as an intermediary, and where the safety of the process is guaranteed by consensus protocols that require the presence of multiple nodes and immutability of the data recorded on each block.

Ideally, no trusted third party is required in a system meant to be trustless and to self- regulate its cryptocurrency.

What would happen if most of the nodes were held by one single player? A "51% attack" indicates a situation in which the 51% of the nodes get controlled by the same player, who can then block transactions or reverse them.[10] Simply put, the more nodes a blockchain is running on, the better its resilience is against such attacks. When the blockchain data is spread across so many nodes, i.e. devices, it will be very hard to corrupt the network and its functioning.

The good functioning of the network may, in turn, encourage its use, thus increasing the generation and expenditure of cryptocurrency, with a consequent growth of the crypto economy. The more secure and engaging the system is, more transactions take place, and appreciation towards the cryptocurrency increases.

However, as we all know, Bitcoin was only the first - although it is still the most important - implementation of a blockchain. Ethereum has introduced, alongside the Bitcoin- inspired tokenomic model, smart contracts as a tool for governing and even self- executing transactions.[11]

---

[9] D. Kosten, *Bitcoin Mission Statement. Or What Does It Mean Sharing Economy and Distributed Trust?* (October 31, 2015). Available at SSRN: https://ssrn.com/abstract=2684256 or http://dx.doi.org/10.2139/ ssrn.2684256.

[10] Krypton and Shift, two Ethereum-based blockchains, have suffered this kind of attack. *See*, https:// blockgeeks.com/ guides/hypothetical-attacks-on-cryptocurrencies/.

[11] Buterin V., *Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform* (2014).

Within a few years, various purposes of using blockchain technology emerged, and as a result, various models of blockchain governance, eventually suitable for those purposes, came to light. Each model essentially determines two aspects:

- - who can participate in the blockchain network;

- - who can write/read data;

- - who validates transactions?

  If the rules of the game change, the roles of the players change as well. Having more or less power to affect what happens on a blockchain leads to reflections on the liability of the players involved.

  Hence, the first important distinction is between ‘public’ and ‘private’ blockchains. The ownership of nodes is at stake here: in a public blockchain there is no central organization, company or other kind of legal entity that owns and governs nodes, while in a private blockchain there is a player or a group of players (in this case we are dealing with a “federated” blockchain) that owns and governs nodes.

  The second important distinction is between ‘permissionless’ and ‘permissioned’ blockchains. Fully permissionless blockchains, such as Bitcoin, are open for all: there is no authority that grants the permission to propose transactions or take part on consensus; everything is ruled by the protocol governing the blockchain. There are no identity restrictions for participating as a user or provider of system functions. On the contrary, permissioned blockchains, such as Ripple, require an organization and governance structure regulating at least who is permitted to participate on a deeper level and usually the basis upon which they may participate. In other words, a central authority decides who can do what. So, for instance, the organization decides who can participate in the consensus mechanism, or can even differentiate roles between nodes, so that certain nodes serve as validators, others serve as transaction-initiators, and others deploy or execute smart contracts. One or many participants in the network may have the authority to manage different levels of access. In any case, a permissioned blockchain implies some sort of user authorization.

  Thus, Bitcoin is the fully decentralized blockchain by definition, since it is not managed by any central authority and is completely public and permissionless. Everyone can potentially do everything (including validating transactions), everyone can view everything. On the contrary, private permissioned blockchain can be described as blockchain-ish versions of intranet for internal management. Hyperledger Fabric is an interesting example: it is managed by the Hyperledger Consortium, so a group of entities, and it is permissioned since the Fabric platform assigns different access levels to nodes based on their role within the organization. For these reasons, Hyperledger Fabric is commonly referred to as a ‘federated blockchain.’ Finally, Ripple and EOS are deemed to be public permissioned blockchains, since anyone can join the network, but

only certain nodes are authorized for certain operations, including validating transactions.

On the one hand, supporters of full decentralization believe that public permissionless blockchains are the way forward. This model certainly served the purpose of early cryptocurrencies, which were designed to work in trustless environments on the assumption that no authority is reliable and therefore the system must be able to govern itself. As a result, these blockchains implemented consensus mechanisms meant to ensure that no single party controls the addition of new blocks, which proved to be slower and more electricity-demanding that those adopted by the permissioned models.

On the other hand, not all blockchain-based platforms need to operate in trustless environments. Thus, depending on the purpose they serve, blockchains may avoid costly consensus mechanisms by re-introducing trusted intermediaries that control the blockchain. In many instances, consumers may be more inclined to trust reputable companies managing blockchains for certain business and citizens may do the same with government agencies willing to provide certain services, like public utilities.

1.1. Vulnerabilities in the blockchain space

Regardless of which blockchain governance model has the greatest appeal, it is undeniable that each model significantly changes the roles of the players and that in a permissioned network it is way more intuitive to identify players who are somehow accountable for what happens within the blockchain-based network.

After all, while blockchains are deemed to be way more secure than traditional centralized ledgers, recent notable events raise questions about who will bear losses and liability for damages occurring in an ecosystem based on blockchain.

Indeed, of the cases examined below, only the so-called “The DAO case" has seen a real sabotage of the blockchain-smart contracts ecosystem; the other cases concern rather hacks occurred to other channels outside the blockchain, i.e. exchanges of cryptocurrencies. Nevertheless, all these events contributed to create a climate of distrust in the eyes of those who are not inside the blockchain's technicalities, which is exactly the opposite of one of the goals the blockchain aims at, that is to solve the problem of trust/mistrust between the parties of a transaction.

These events include hacks to the most important Bitcoin exchanges, such as Mt. Gox (which subsequently declared bankruptcy, citing losses from the hack amounting to USD 473 million),[12] Bitstamp (loss of 19,000 Bitcoins, valued at about USD 5.1 million),[13] Bitfinex (loss of 119,756 Bitcoins, valued between USD 66 and 72 million).

Among all, the event that more than any other has shown the vulnerabilities of blockchain space is The DAO case, namely the attack inflicted to a decentralized autonomous organization launched on Ethereum, named “The DAO.”[14]
The DAO was conceived of and programmed by the team behind the German startup Slock.it. It was meant to serve as a decentralized venture capital fund and to act as a hub for large and small investors willing to initiate blockchain-based projects. The DAO launched on 30 April 2016, collecting over USD 150 million from thousands of individuals across the world within a 28-day crowdfunding window, thus completing the largest crowdfunding campaign on record.[15]

---

[12] *See* Cawrey D., *Mt. Gox Trading Halts as Bitcoin Businesses Move to Assure Investors*, COINDESK (Feb. 25, 2014, 5:12 PM), http://www.coindesk.com/mt-gox-trading-halts-bitcoin-businesses-moveassure investors; Conway B., *Mt. Gox Bitcoin Exchange Files for Bankruptcy Protections*, BARRON’S (Feb. 28, 2014, 8:35 AM), https://barrons.com/articles/mt-gox-bitcoin-exchange-files-for- bankruptcyprotection-1393594521.

[13] Moon M., *Bitcoin Exchange Loses $5 Million in Security Breach*, ENGADGET (Jan. 6, 2015), http://www.engadget.com/2015/01/06/bitstamp-bitcoin-exchange-hack.

[14] “Decentralized autonomous organization” means an organization solely managed via blockchain and smart contracts, without any person holding decision-making power and any oversight at all.

[15] Popper N., *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, in *New York Times* (May 21, 2016), at https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html.

Once the crowd-sale was over, there was much discussion of first addressing the vulnerabilities before starting to fund proposals. In particular, Stephan Tual, one of The DAO's creators, announced on 12 June 2016, that a ‘recursive call bug’ had been
found in the software but that no DAO funds were at risk.[16] Unfortunately, while programmers were working on fixing this and other problems, an unknown hacker took advantage of that bug to start draining The DAO of Ether (which is the cryptocurrency for operations on Ethereum) collected from the sale of its tokens. No one had the ability to fix the code because no one was truly in control of the organization, and therefore able to timely update the software. As a result, The DOA kept on working as established in the original smart contracts, leading to a loss of over USD 50 million worth of Ether in just a few hours of operation.[17]

In response, the majority of the users in the blockchain decided to recapture the funds, thereby allowing the alteration of the chain itself. In an unprecedented move, core Ethereum developers effectively rewrote the history of their blockchain in order to undo the hack and restore the funds to all investors via a hard fork.[18] This process was unprecedented at the time and brought down the ideology of the blockchain as an irreversible record of all transactions. The decentralized networks proved to be vulnerable to coalitions, which combine enough technological prowess, computing power, or force of persuasion to implement their proposals on the development of the blockchain.[19]

For all these reasons, we believe that designing governance models that allow a certain degree of accountability is crucial both to generate confidence in users towards the use of a given blockchain-based system. In addition, as we will see in Chapter 3, blockchain governance models determine how certain types of liability are distributed between the parties that keep a given ecosystem alive.

Siegel D., *Understanding The DAO Attack* (June 25, 2016), at http://www.coindesk.com/

16 understanding-dao-hack-journalists/.

17 Finley K., *A $150 Million Hack Just Showed that the DAO Was All Too Human*, in *Wired* (June 18, 2016), at https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human.

18 The Ethers originally collected in the DAO, which had then siphoned off to a child DAO by the attacker and to yet another DAO by friendly hackers (white hats), were restored to a Withdraw DAO recovery contract. The token holders can reclaim their investments in this way. See Wilke J., To fork or not to fork (July 15, 2016), at https://blog.ethereum.org/2016/07/15/to-fork-ornot-to-fork/.

19 Hacker P., *Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations* (2017), 16. Available via SSRN.

2. Legal Recognition of the Blockchains and Smart Contracts

Interest in the technologically advanced blockchain increased in 2009, and it exponentially piqued interest in the legal fraternity in the beginning of 2017, with a significant increase in the idea to use smart contracts and blockchain technology in day- to-day business. According to Ron Quaranta, the founder and Chairman of Wall Street Blockchain Alliance, the legal industry was one of the fastest growing sectors in the Blockchain Alliance. David Fisher, the co-founder of Integra Law opined that on a blockchain, once a contract is signed, it is available now and forever, and we can confirm the details at any time we want.[20]

Aaron Wright, a Professor at Cardozo Law School, chair of legal working group of EEA and the co-author of the book 'Blockchain and the Law'[21], in his opinion says that "blockchain can be used as a 'spine' in the entire legal industry and use blockchain to build more efficient systems, decreased legal costs and ensure that people get the legal services they need."[22]

He also says, "with an immutable record of the finalized contracts, with time-stamped signatures, there will be less room for disputes".[23]

While all these words are true to a certain extent, the biggest hindrance is the lack of clear regulations on the use and the legalities of this technology. While many states like Vermont, passed its laws in 2017 legalizing the use of blockchain and digital signatures and making such documents/records admissible in its courts of law,[24] there are many nations still on the backfoot.

In the next paragraph, we will provide a brief overview of the various nations and their regulations in favor of blockchain.

2.1. Regulations of the Blockchains in the USA

The Blockchain initiatives in the USA can be traced from the so-called Delaware Blockchain. Such a reform process was a response to administrative inefficiencies related to the 'mergers and acquisitions' field, often resulting in litigation. With approximately two-thirds of Fortune 500 companies incorporated in Delaware, a considerable portion of USA corporate litigation occurs in that state. Two disputes, in particular, were characteristic examples of transactional litigation that arises out of administrative inefficiencies, namely *In re Appraisal of Dell, Inc.* and *In re Dole Food Co., Inc.* The Delaware Blockchain Initiative was introduced in 2016 by the Delaware then-Governor Jack Markell. As a result, on 1 August 2017, the Delaware General Corporate Law was amended through Senate Bill 69, namely the so-called "Blockchain Bill." In the aftermath of the Delaware Blockchain Initiative, many states within the U.S. are taking a variety of actions to open the door to regulated implementations of blockchain technology.

---

[20] See https://bnanews.bna.com/daily-labor-report/how-blockchain-technology-is-transforming-the-legal- industry.

[21] Blockchain and the Law: The Rule of Code by Primavera De Filippi, Aaron Wright Published April 9th, 2018 by Harvard University Press.

[22] See https://www.linealservices.com/how-blockchain-will-transform-and-benefit-the-legal-sector/. [23] See https://www.darslaw.com/bitcoin-blockchain-and-beyone?journal=258.

[24] See https://cointelegraph.com/news/vermont-considering-blockchain-tech-for-state-records-smart- contracts.

Below is a brief summary of the current scenario.

- Delaware – The State of Delaware is one of the first states to have come up with regulations relating to this technology in July 2017, making it effective from August 2017. The law intends to provide a specific statutory authority to oversee the use of blockchain technology by the corporations in Delaware and for maintaining the corporate ledgers.[25] It is a part of a new initiative that is aimed at developing the small scale industries to equip themselves with the latest technology and improve their businesses. This initiative promoted the expansion of these businesses by developing exports.

- Wyoming – The state of Wyoming passed a Bill – HB 70 in March 2018, relating to the ease in the use of blockchain in the day-to-day course of businesses, the users are free from being subjected to specific security laws.[26] The representatives have agreed on a bill – HB 101, which is aimed at complementing the Wyoming Business Corporations Act, where the blockchain created, used and operated for the purposes of storing records, shareholder identification and vote acceptance are authorized by the State.[27]

c. California – The state of California has passed a Bill that will enable the state to update its records on a blockchain; this Bill defines what blockchain means and evaluates a number of uses of the technology.[28] Clause "h" of Section 1633.2 of the Civil Code of California includes blockchain as an electronic record – "*Electronic record' means a record created, generated, sent, communicated, received, or stored by electronic means. A record that is secured through blockchain technology is an electronic record.*"[29]

- Connecticut – the State of Connecticut has two Bills passed dealing with blockchain technology. the first deals with the establishment of the Connecticut Blockchain Working group, creating plans for fostering the expansion and growth of the blockchain industry in the state. It also recommends policies and state investments to make Connecticut the world leader in blockchain technology.[30] The second bill deals with studying the impacts of digital currency, blockchain and smart contracts have on state law and businesses.[31]

---

[25] *See*, https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69.

[26] *See*, https://legiscan.com/WY/bill/HB0070/2018.
[27] *See*, https://www.wyoleg.gov/2018/Enroll/HB0101.pdf.

[28] *See*, https://legiscan.com/CA/text/AB2658/2017.
[29] *See*, https://legiscan.com/CA/text/AB2658/id/1776109.
[30] *See*, https://www.cga.ct.gov/2018/ACT/sa/2018SA-00008-R00SB-00443-SA.htm.

[31] *See*, https://www.cga.ct.gov/2018/FC/2018SB-00513-R000553-FC.htm.

- Illinois – The government of Illinois creates the Blockchain Technology Act, that provides for the use of blockchain technology in various transactions, the limitation of the use, clearly defining its boundaries of the use and implementation of the new technology. It also provides certain restrictions for the use of blockchain technology in its local government.[32]

The list of states can go on with an increasing number of states adding the blockchain technology in their legislative pool. There are many other states like Arizona, Colorado, Florida, Michigan etc., joining the blockchain flow aiming to create a legally powered environment for the use and development of blockchain technology.

2.2. Regulations of the Blockchains in the EU

While many European states have provided certain clarity on the legality of cryptocurrency, there are very few states that have actually catered to the need of having a legislation on blockchain technology on its own. Therefore, the EU is starting certain initiatives the launch of the "EU Blockchain Observatory and Forum" to encourage blockchain initiatives within the European Union.[33] Also, in April 2018, many nations came together to sign a Declaration creating the European Blockchain Partnership.[34] Five more nations, including Italy joined the Partnership later that year in September. The main focus of the Partnership, however, is on cybersecurity, privacy, energy efficiency and interoperability, all in full compliance with the laws of the EU.[35]

The southern European states of France, Italy, Spain, Malta, Cyprus, Portugal and Spain signed a joint declaration in 2018, to promote the adoption of blockchain in the region in order to "transform" their economies. They further committed to collaborating on the development of the technology in order to become "*a leading region in this sector.*"[36]

That being said, we provide below a brief overview of the regulatory interventions that have taken place in some EU countries.

a. Malta – The state of Malta has taken a huge step in the first regulatory framework for the use of blockchain technology, or widely classified as 'Distributed Ledger Technology' (DLT). Malta has passed 3 Acts that cater to the regulatory impact on varying degrees.

I. Malta Digital Innovation Authority Act (MDIA Act) - this Act establishes the legal legitimacy of the DLTs, the internal governance of the processes and outlines the duties and responsibilities of competent authorities to certify the platforms being in use. This Act also provides legal certainty for prospective users to make use of any established DLT platform.[37]

---

[32] *See*, http://www.ilga.gov/legislation/100/HB/PDF/10000HB5553lv.pdf.

[33] *See*, https://www.eublockchainforum.eu/about.

[34] See, https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership;

https://www.finextra.com/blogposting/15256/european-blockchain-partnership-great-leap-forward. [35] *See*, http://www.europarl.europa.eu/doceo/document/TA-8-2018-0528_EN.pdf?redirect.

[36] Dichiarazione%20MED7%20versione%20in%20inglese .pdf.

See, https://www.mise.gov.it/images/stories/documenti/

[37] *See*, https://parlament.mt/media/94210/bill-45-malta-digital-innovation-authority-bill.pdf.

b.

II. Innovative Technology Arrangement and Services Act (ITAS Act) – this Act primarily deals with the certification of DLTs that are established for the purposes of companies involved in cryptocurrency trading.[38]

III. Virtual Financial Assets Act (VFA Act) – this Act is exclusively enacted for the purposes of governing the ICO trading. It is intended to have a regulatory authority over companies or individuals who engage in trading in cryptocurrencies, ICO trading, providing wallet facilities for cryptocurrencies etc.[39]

Italy - Italy has not yet adopted specific legislation in this area, but in the meantime has recognized the legal validity of the blockchains. Article 8-*ter* (1) of the Italian Decree Law no. 135 of 2018 provides that "*Technologies based on distributed registers" are defined as technologies and computer protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralized register on cryptographic bases, such as to allow the recording, validation, updating and archiving of data both in plain text and further protected by cryptography verifiable by each participant, which cannot be altered or modified.*

2.3 Regulations of the Blockchains in the Non-EU countries of the European continent

Outside the European Union, some states geographically located in the European continent have adopted legislation in the blockchain area quite extensive and relevant. The small size of these states, with all that comes with it in terms of streamlining the legislative and bureaucratic machine has undoubtedly helped the adoption of regulations of a significant scope, certainly aimed at turning these states into hubs for investors and blockchain-related projects. There are also countries in the Eastern European parts who are trying to create a flourishing environment for the development of blockchain based businesses.

Below is a brief overview.

a. Gibraltar– In 2017, Gibraltar passed its "Financial Services (Distributed Ledger Technology Providers) Regulations 2017", where the Act aimed at providing businesses or companies who intended to engage in the service provision through distributed ledger technology, to obtain a license to carry out a controlled and regulated form of business of the service provision. The Act also focuses on disciplining such businesses from a financial point of view as a part of the Gibraltar Financial Services Commission (GFSC).[40]

---

[38] *See,* https://parlament.mt/media/94207/bill-43-innovative-technology-arrangements-and-servicesbill.pdf. [39] *See*, https://parlament.mt/media/94209/bill-44-virtual-financial-assets-bill.pdf.

[40] *See*, http://www.gfsc.gi/uploads/DLT%20regulations%20121017%20(2).pdf/.

The GFSC operates on 9 main principles that are made for the application of blockchain/distributed ledger technology that all the companies have to adhere to - honesty and integrity; customer care;

adequate resources; effective risk management; protection of client assets; effective corporate governance; systems and security access; financial crime prevention; and resilience.[41]

The Act also provides for various exemptions on legislations on financial institutions once the companies have applied and obtained specific operating licenses for the use of blockchain technology.

- Belarus - Often little cited, this country was among the first ones in the European continent adopt a regulatory framework for the blockchain industry. The 'Digital Economy Development Ordinance' has been in effect since March 2018. This Bill has provided for the creation of a Hi-Tech Park (HTP) to cater and nourish blockchain and cryptocurrency-based businesses. The Bill provides for the categorization of the HTP as a special zone with special tax and legal regime for the businesses based on blockchain and cryptocurrency.[42] The further blockchain law imposed by the government in 2018 focused on the prevention of terrorism financing, money laundering, and propagation of weapons of mass destruction by means of any blockchain-related activities.[43]

- San Marino – The Delegated Decree no. 37 issued by the Republic of San Marino on February 27, 2019, in order to regulate the Initial Token Offerings, gave a very precise definition of blockchain under Article 1 (1) (a): "*a Distributed Ledger composed of validated and confirmed transaction blocks organized in a sequential chain to which only new blocks can be added through the use of connections based on cryptographic hash functions or equivalent technologies designed to be able to withstand tampering and provide an immutable archive of the transactions recorded*."
  A more concise style is certainly appreciated when compared with the definition provided by Italian legislation, which makes sense to use as a benchmark since both provisions are likely to have been conceived in Italian language.

d.

Nevertheless, the reference to "*transactions recorded*" sounds rather limiting since the information that can be hashed and stored on a blockchain can be very different in nature. Moreover, saying that a blockchain can "*withstand tampering*" is a vague expression that can be referred to the design of many technologies, so perhaps this provision should have given some more detail. Probably the urgency of regulating the Initial Token Offerings sector has resulted in rushing the defining elements of the blockchain and the total omission of the smart contracts component which, in our opinion, should be the fundamental basis for building any regulatory system gravitating of the blockchain matters.

Liechtenstein– As a latest addition to the regulations on blockchain, Liechtenstein has unanimously passed the Liechtenstein Blockchain Act, on October 3, 2019. This Act will come into effect from January 1, 2020. It aims at providing investor protection, transparency and an anti-money laundering measure. This Act provides for the direct tokenization of physical assets or rights to assets. The most intriguing aspect of this Act is that both the digital data and physical data have to be synchronized to maintain the same information.

---

[41] *See*, http://www.gibraltarlaw.com/wp-content/uploads/2017/10/DLT-Regulatory-FrameworkBrochure-v3.pdf;

http://www.gibraltarlaw.com/dlt-regulation-gibraltar/; http://www.gfsc.gi/dlt.
[42] *See*, https://eng.belta.by/infographica/view/digital-economy-development-ordinance-3071/. [43] *See*, http://www.park.by/topic-faq/?lng=en.

Liechtenstein also amended its civil laws to accommodate the provisions in the Blockchain Act and to protect the tokenized assets which is prone to the threat of theft.

2.4 Regulations of the Blockchains in the Middle East and Asia

Many Middle Eastern and Asian countries are moving forward with the use and implementation of blockchain and cryptocurrencies. While they have not focused on creating regulations on blockchain technology itself, they have various provisions in place to regulate the use of cryptocurrencies.

a. Middle East - Blockchain is the "ongoing phenomenon" in the middle east. Though there are no specific laws in place for the governance of blockchain technology, they are making progress in trying to implement it in as many spheres of businesses as possible. Countries like UAE, Bahrain and Saudi Arabia have already implemented blockchain in its financial and healthcare sectors.

The United Arab Emirates (UAE) is the first of all the Middle Eastern countries to have established a Blockchain Court. This court is established in collaboration with the Smart Dubai initiative by the Dubai International Financial Center (DIFC).[44] This is aimed at creating the base for a blockchain based judiciary system, focused and equipped with the knowledge to handle disputes arising out of blockchain transactions.

Smart Dubai is another initiative taken up by the emirate to further nourish the blockchain development and implementation. It aims at making Dubai a fully blockchain powered and run economy by 2020, making it the first paperless economy in the world. This also aids in easing out processes in various sectors of governance, enhancing efficiency and creating new specialized sectors to achieve global leadership.[45]

Dubai is also the home for the world's first blockchain council – Global Blockchain Council, established to bring people together to discuss the current trends and future possibilities of blockchain technology.[46]

b. Asia - Asia is also getting ahead in the blockchain game. While many Asian countries do not have any regulations exclusively relating to blockchain like America or many European states, countries like Singapore and Malaysia enabling parts of the technology by providing regulations for the issuance and use of cryptocurrencies.

China, in particular is interesting because, while the Chinese State Counsel welcome blockchain and cryptocurrencies, the People's Bank of China banned the use of cryptocurrencies and shutdown all the exchange houses that transacted with cryptocurrencies, and following this move, the Ministry of Industry and Information Technology launched a program called 'Trusted Blockchain Open Lab' promoting the exploration of blockchain technology, independent of the cryptocurrency issuance or trade.

---

[44] *See*, https://www.difccourts.ae/2018/07/30/difc-courts-and-smart-dubai-launch-joint-taskforce-for-worlds- first-court-of-the-blockchain/.

[45] *See*, https://scgn.smartdubai.ae/pdf/dubai-blockchain-strategy.pdf.

[46] *See*, https://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/.

The Malaysian Central Bank has regulations in place regarding the use and transaction for cryptocurrencies where all entities dealing with the currency have to register their complete details

with the virtual currency exchange houses. This regulation is focused on anti-money laundering and anti-terrorism financing.[47]

Singapore also has guidelines in place for the regulation of cryptocurrencies. The Monetary Authority of Singapore (MAS) is the issuing agency of these guidelines, focusing on regulating the use of cryptocurrency as a capital market product.[48]

Unlike fellow neighboring countries, India still has a long path to take for dealing with the new technology. While the use of cryptocurrencies has seen an increase, the Reserve Bank of India (RBI) has issued a statement that cryptocurrencies are not considered as a legal tender within the territory of India and any such entities dealing with these are to do so on their personal risk.[49]

Uzbekistan, another Asian country has seen a huge leap in the development of the regulations regarding blockchain/DLT. The President endorsed a decree on the development and integration of blockchain technology with the goal of modernizing the state administration system.[50]

2.5 Regulations of Smart Contracts

It is an accepted fact that all transactions are a form of a contractual obligation. While the world is moving forward decades at a time, the laws we follow are centuries old and these same laws pose a significant challenge when dealing with issues of the new world.

Let us focus on one aspect of the laws, the contract law. The world laws are broadly classified into common law jurisdictions and civil law jurisdictions, and these two jurisdictions differ widely in their contract laws. An easy illustration of the vast difference is the concept of ‘good faith’ that is essential for a contract in the civil law jurisdiction but is entirely absent in the common law jurisdiction or its requirement is not mandatory. This alone gives us a glimpse of how different the world is when it comes to laws.

This line becomes further blurred when these jurisdictions are removed entirely, and this is the case when it comes to the governing of smart contracts. These borderless smart contracts make it difficult to ascertain a standard rule or even a legal status for its operations.

---

[47] *See*, https://news.bitcoin.com/new-malaysian-cryptocurrency-regulation-come-into-effect/.

[48] *See*,http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/

Securities%20Futures%20and%20Fund%20Management/Regulations

%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offeri things%20%2014%20Nov%202017.pdf.

[49] *See*,https://www.businesstoday.in/current/economy-politics/rbi-ban-banks-trading-incryptocurrencies- bitcoin-investors/story/274312.html.

[50] *See*,https://cointelegraph.com/news/president-of-uzbekistan-signs-decree-on-blockchain-integrationtax- exclusions-for-crypto.

In light of this, UNCITRAL is developing laws on the role of electronic communication, trying to categorize the information in the smart contracts as offer and acceptanceand once the transaction is

expressed and stored in a block, the contract is signed and is legally enforceable.[51] Meanwhile, certain countries are trying to provide for definitions or basic regulation for smart contracts.

Below are a few regulations around the world that has created a guideline for the governance of smart contracts.

1. RegulationsintheUSA

a. Arizona – in the House Bill 2417, the State of Arizona defines a smart contract as 'an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.' It also validates smart contracts as contracts similar to the conventional paper written contracts and assigns a legal status to these contracts making them admissible in courts.[52]

b. Tennessee – The State of Tennessee passed a Senate Bill, Bill 1662 that recognizes the legal authority of the use of smart contracts. Section 2 of the Bill defines it as 'an event driven computer program that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) Take custody over and instruct transfer of assets on that ledger; (B) Create and distribute electronic assets; (C) Synchronize information; or (D) Manage identity and user access to software applications.' The Bill also protects the ownership rights of information stored on distributed ledger technology.[53]

c. Nebraska – the State of Nebraska has a pending Legislative Bill, Bill 695 that defines smart contracts as 'an event driven program or computerized transaction protocol that runs on a distributed, decentralized, shared, and replicated ledger that executes a contract or any provision or provisions of a contract by taking custody over and instructing transfer of assets on the ledger.'[54]

d. New York - The State of New York has a pending General Assembly Bill 8780, which aims at providing legal status for all transactions carried out through smart contracts.[55]

e. Ohio – The Ohio State Bill 300 was drafted to revise the Electronic Transactions Act to include blockchain and smart contracts within its scope. The Bill also aims to clarify that because a contract is digitally made, it does not lose its validity of being a contract.[56]

---

[51] *See*, http://cornellilj.org/smart-contracts-another-feather-in-uncitrals-cap/. [52] See, https://legiscan.com/AZ/text/HB2417/2017.

[53] *See*, https://legiscan.com/TN/text/SB1662/2017.

[54] *See*, https://legiscan.com/NE/text/LB695/2017.

[55] *See*, https://legiscan.com/NY/drafts/A08780/2017.

[56] *See*, https://legiscan.com/OH/text/SB300/2017.

2. Regulations in Europe

Though there are not many regulations on the governance of smart contracts specifically, we can find some provisions regarding smart contracts in the broad regulations relating to blockchain and its uses.

a. Malta - The Maltese government passed 3 Acts regarding the governance of blockchain. 2 of the 3 Acts provide for a definition on smart contract.

The Virtual Finance Assets Bill and Malta Digital Innovation Authority Bill defines smart contract as – "*a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form which is automatable and enforceable by execution of computer code, although some parts may require human input and control, and which may also be enforceable by ordinary legal methods or by a mixture of both*"[57] and the third Bill, the Innovative Technology Arrangements and Services Bill lists out the governance provisions made for smart contracts.[58]

b. Gibraltar– Inspired from Malta, Gibraltar also is trying to give a legal status to smart contract and trying to incorporate smart contracts into its blockchain framework.

c. Italy - As already illustrated with regard to the blockchains, Italy has not yet regulated smart contracts; it just defined them and set the boundaries for their legal validity. Indeed, Article 8-*ter* (2) of the Italian Decree Law no. 135 of 2018 provides that smart contracts are software based on DLTs which, once the relevant ledger entry has been validated, automatically give effect to the relevant terms agreed between two or more parties. Smart contracts are deemed by law to be equivalent for certain purposes (i.e., consensus formation and evidentiary value) to traditional written contracts to the extent that the digital authentication of the parties is made in accordance with the procedure to be established by AgID.[59]

This last clarification opens the door to the issues of electronic documents and electronic signatures, and therefore of compliance with the eIDAS Regulation (Regulation (EU) N°910/2014); aspects that cannot be examined here as they are complex and deserve dedicated analysis. In any case, the procedure that was meant to set by AgiD by mid-May 2019 has not been finalized yet, and therefore no technical standards is available and applicable as of today.

---

57 *See*, https://parlament.mt/media/94209/bill-44-virtual-financial-assets-bill.pdf;

https://parlament.mt/media/94210/bill-45-malta-digital-innovation-authority-bill.pdf

58 *See*, https://parlament.mt/media/94207/bill-43-innovative-technology-arrangements-and-servicesbill.pdf.

59 "AgID" means "Agenzia per l'Italia Digitale" and it is a governmental agency whose mandate is pursuing the highest level of technological innovation in the organisation and development of public administration and in the service of citizens and businesses.

3. Regulations in the Middle East and Asia

a. Middle East - UAE, in the Middle East is the torch bearer for all the advancements in the field of blockchain and smart contracts. As said before, though there are no specific regulations governing blockchain and smart contracts, a smart contract can be considered a legally valid contract if it satisfies the requirements of the contractual obligations under the UAE Civil Code.[60] However the main character of irrevocability of a smart contract can be challenged in its enforcement. Article 12 of the Federal Law No.1 of 2006 on Electronic Commerce and Transactions considers smart contracts as valid contracts as it provides valid and legally enforceable contracts, but only in the form of computer codes.[61]

b. Asia - Asia on the other hand, is more concerned on keeping an eye on cryptocurrencies than on smart contracts.

The recognition of the legal validity of smart contracts is certainly an important first step, but it is not enough in our opinion. How - we will better explain in the next chapter, a solution to fully regulate a smart contract is to have a pre-written contract, that has all the requisites of jurisdiction, and the existing contract laws of the said jurisdiction govern the execution of the contract and then the contract is converted into a smart contract.

And above all, it is evident that, no legislative intervention has gone so far as to provide a basic framework for addressing the problem of the responsibility of the players on a blockchain, or on a platform based on blockchain technology.

3. Elements of liability

In the light of what has been said in Chapter 1, we may argue that the nodes are the players who carry out the activities within a blockchain. Based on the legal recognition that blockchains and smart contracts obtain in a given country, as per Chapter 2, we can then speculate on a number of scenarios to address the issue of liability. Obviously, the identification of some kind of liability is closely related to the model of blockchain governance adopted, and therefore to the management of nodes.

Though the technology is constantly evolving, the corresponding evolution of the legal systems regarding these technologies are not happening since most laws were not drafted keeping this boom in mind. And as a result of this lag, governing the proliferation of technology, especially something as impactful as blockchain/DLT and smart contracts is an uphill battle. Standards and regulations are to be set by the governments, who many a times might not fully comprehend and understand what they are trying to regulate and legislate. And along with these challenges, liability is one of the biggest hurdles that most of us are trying to simplify and provide ways to solve this issue.

---

[60] *See,* http://www.quantumconsult.org/wp-content/uploads/2012/01/copyUAE-Civil-Code.pdf. [61] *See*, http://www.wipo.int/edocs/lexdocs/laws/en/ae/ae027en.pdf

3.1. On decentralized network for mining cryptocurrencies

In a fully decentralized blockchain, presumably no one controls the nodes, so there is no there is such a thing as an accountable central authority.

In our opinion, this scenario may be framed as a sort of unlimited mutual liability of the nodes, precisely of people or entities controlling the nodes. So the unfair player (possibly someone who controls the 51% on the nodes, which is not practically feasible on the Bitcoin's blockchain due to the insane amount of computational power and electric energy required, but plausible on other small blockchains for minor cryptocurrencies) who attacks a blockchain, thus subverting the rules of the network, should be considered liable for the damage caused to the other participants in the network. However, establishing compensation for damage is really complicated in practice, if not undoable, since:

1. identifying the liable person or entity is difficult due to the pseudonymization of the participants on which public permissionless blockchains such as Bitcoin and Ethereum are based;

2. quantifying damages in terms of actual loss there the participants do not lose any asset, but it is highly likely that as a result of the cyber-attack the cryptocurrency issued by that blockchain will partially lose value;

3. quantifying damages in terms of loss of profit is difficult due to the volatility of the cryptocurrencies;

4. the fact could not really be considered illegal since there is no breach of contract in such a governance model, and there is no breach of law due to the absence of laws regulating attacks to the blockchain (i.e. what is commonly referred to as "attack" is indeed a mere way of opportunistically exploiting the rules of the IT protocol that governs the blockchain).

In light of the above, fully decentralized and automated governance on the basis of an IT protocol tend to result in a lack of accountability. In this regard, FINRA, in its January 2017 report, said: "*Recent events have shown that lack of a central governing body for the evolving Bitcoin Network has created concerns for the network, as participants try to determine an approach to handle increased transaction volume. Therefore, a network based on the use of a trustless network, where no party is responsible or accountable for the proper operation of the system, may present risks to markets and investors.*"[62]

3.2. Contractual liability for breach of smart contract

When we talk about the decentralized technologies, the first thing that comes to our minds is its borderlessness. This very nature makes them very intriguing and interesting. With the systems and data spread across the whole world, the main question of who or what is liable for the dispute or losses comes into the picture and many of us are trying to figure this out, leading to this robust chapter dedicated to finding an answer.

---

[62] FINRA means Financial Industry Regulatory Authority, Inc., which is a private corporation headquartered in Washington D.C. that acts as a self-regulatory organization within the U.S. *See*, FINRA's *Report Distributed Ledger Technology: Implications of Blockchain for the Securities Industry* (January 2017).

In any contract, nothing works without liability; we can describe contracts as an "agreement creating obligations that are enforceable by law"[63] or as the law "based on the liability for the breach of promises."[64] And in a broad since, every transaction is a form of a contract and non-compliance of the rules of the transaction amounts to a breach, giving rise to remedies to compensate for the deviation; and it is these remedies that are liabilities in the legal world.

When we talk so much about liability, it is important to understand what 'liability' means. It is defined in many ways by many scholars, but the most relevant one for the legal fraternity is in the 10th edition of Black's law dictionary which defines liability as "*The quality, state, or condition of being legally obligated or accountable; legal responsibility to another or to society, enforceable by civil remedy or criminal punishment.*" And going by this definition, the concept of liability is non-existent in a blockchain world as there is no one person or a sole entity to handle the responsibilities, the system is spread across the globe, making the identification of jurisdiction an issue, and with no jurisdiction to tie the law down to, which society will the parties to the contract be responsible/answerable to? While these questions will remain unanswered for the most part, we are making an attempt to clear the chaos in the system. Below we will see the various aspects in which blockchain will or will not be answering the question of liability.

We know that a traditional paper contract is not the only kind contract in existence, there are digitized contracts that are called smart contracts that are self-executory and immutable contracts hosted on a blockchain. While talking about smart contracts, we need to question if this works exactly like a traditional contract in the legal sense, where it is mandatory to have an offer an acceptance, a remuneration and an obligation to complete the transaction. By now, we know that though smart contracts and traditional contracts vary in their own right, they are very similar when it comes to deciding if a code is a contract or not. And with this, there is a question of liability that follows. What happens when a smart contract is breached? What/who is liable for its contractual obligations?

3.3. Ricardian Contracts

To answer these questions, we need to introduce ourselves to what is called a 'Ricardian contract', which is a hybrid of a traditional paper contract and a smart contract. The Ricardian contract is one where a contract is executed and is a legally binding agreement on a blockchain. It is a conventional paper-based document, that is both human and machine readable. This type of contract was first introduced by Ian Gregg in 1995, who says a Ricardian contract, "*is a form of digital documents that act as an agreement between the two parties on the terms and conditions for an interaction between the agreed parties.*"[65] This form of contract was named after the 19th century British Economist, David Ricardo who is famous for his contribution in the trade theory.

---

[63] The Proposed Regulation on a Common European Sales Law defines 'contract' as 'an agreement intended to give rise to obligations or other legal effects' (Chitty on Contracts, 2018, at 1-025).

[64] H.G. Beale, W.D. Bishop, and M.P. Furmston. 2008. Contract Cases and Materials. 5th Edition. Oxford: Oxford University Press, p.3

[65] Grigg, Ian: Financial Cryptography in 7 Layers, 1998-2000; Grigg, Ian: The Ricardian Contract.

The distinctive features of this contract are that they are,
a. both machine and human readable
b. all forms of the document – displayed, printed and coded are all equivalent
c. it is signed by the users
d. they can be identified securely and any changes to this document in any form is impractical

Ricardian contracts revisit the concept of contract-automation from a different angle; which potentially will benefit a section of users and will eventually transform the practice of law. It is a human-readable and machine convertible contract which defines the intention of both parties. The basic features of Ricardian contracts that trump over smart contracts are:

A. *Purpose* – the contract lists and records the purpose of creation of the document

B. *Flow* – it can automate operations/execution of the contractual terms on the blockchain based platform it is uploaded in

C. *Validity* – since these contracts are pre-written and signed as a paper document which is legally binding and valid, and then converted into codes, these contracts are enforceable by law unlike the status of smart contracts in most countries.

D. *Element of time* – Ricardian contracts have a specific term like the conventional contracts. They decide on the time that can be taken for the execution or completion of the contract

E. *Versatility* – A Ricardian contract can be a smart contract, but not every Ricardian contract is a smart contract, there is a choice; whereas no smart contract can be a Ricardian contract

F. *Reliability* – Since the Ricardian contracts are both human and machine readable, there is no question of ambiguity. The contracts are written in the conventional manner, having all the clauses, definitions and terms in place, there is no further room for any ambiguity once these contracts are converted to codes

The main intention of introducing Ricardian contracts here is to highlight its main benefits in the blockchain sphere.

A. *Cost effective* – similar to all blockchain and smart contract related transactions, the Ricardian contracts are also cost effective. These will also take a step further, where it is clear on terms of the contract, where they will also help save time and money when a litigation or dispute arises

B. *Legally Binding* – since these documents are first written and signed, they have a definite jurisdiction and all other clauses in place that make the document legally enforceable in a court of law. Unlike smart contracts, the Ricardian contracts bind both parties, whose identity is known to each other and in case of disputes, legal remedies can be sought.

C. *Acts like a smart contract* – the Ricardian contracts are documents, like a paper contract that outline the intentions and actions that will be undertaken and a smart contract that controls and organizes the arrival of events. In short, Ricardian contract is the best efforts to record the agreement and smart contract is the execution of that agreement.

Since these contracts are both physical and cryptographically signed and verified, it can provide for a robust and fool-proof process to trade or carry out any business on the internet. And since they use cryptographic signatures, they as secure as well.

Ricardian contracts have many more advantages when compared to smart contracts. Even though it is a decades-old idea, the blockchain technology makes it possible to make the most out of it. Blockchain allows us to notarize these contracts, secure them on a blockchain network, and keep a complete reference of the matter.

And this feature of the Ricardian contracts can help us tackle the question of contractual liability. We can have:

A. A clause or term identifying the jurisdiction which brings in a clarity for the borderless nature of smart contracts

B. This can have a set clause for liability or limitation thereof in place to determine the role of each party to the contract

C. The nature of the blockchain – private or public, permissioned or permissionless - does not make an impact while Ricardian contracts are integrated in a blockchain platform as the legally binding terms are already laid down

With some of the main questions that most blockchain enthusiasts are being cleared out one by one through the Ricardian contracts, they can be seen as something that will come into the limelight soon.

OpenBazaar[66], a P2P e-commerce marketplace is a live example of the use of Ricardian contracts in its transactions, which legally binds the parties to the terms of the contract and assigns liability to both the parties according to their role of being a buyer or a seller. Every time a new transaction is made, a new Ricardian contract is automatically created. Some of the other blockchain based platforms that use Ricardian contracts instead of smart contracts are SciDex, BOSCoin and Kadena.

3.4. Smart Contract Developer Liability

While the issue of who is liable on a smart contract is a burning question, there is one person/regulator trying to clear the clutter by identifying the potential actors who can be liable for violations through smart contracts.

Commissioner Brian Quintenz of the Commodity Futures Trading Commission opined his belief that the smart contract developers can be held liable for the violation of the CFTC rules if it could be seen that the smart contract created was intended to violate/ circumvent the CFTC rules. He categorizes all the parties involved in a smart contract into 4 sections;

1. Thecoredevelopersoftheblockchainsoftware
   2. Theminers/nodesthatvalidatethetransactions
   3. Smartcontractcodeandapplicationdevelopersand 4. Theendusersofthesmartcontract

---

[66] See OpenBazaar Tokens and Smart Contracts - https://openbazaar.org/blog/openbazaar-tokens-and- smart-contracts/

He goes by the process of elimination to determine the most likely actor who can be held liable for violations. He opines that the core developers, the nodes and the end users are less likely to be responsible as they would not be in a position to determine if a natural person will use these coded to violate the regulations and determine the legality of each transaction held on the blockchain. He also suggests that both, the creators and the particular users of an improper smart contract should be held liable for their actions.

He urges the idea that both CFTC and smart contract developers could work in nexus with each other and ensure that the smart contracts coded are compliant with the existing rules and pursue engagement instead of enforcement of the rules.[67]

3.5. Liability for platforms/service providers using blockchains as part of their infrastructure

While Ricardian contracts can help parties entering into a contract in limiting their liability, we should not discard the liability regime to be determined for the digital platforms that host these contracts. They can be either contractual or non-contractual. But the main question of who is liable still remains.

Most of the famous blockchain platforms like bitcoin blockchain or the Ethereum blockchain have taken some measures in place by adding disclaimers in their terms of use, which limits the liability of the platform. This is a major step in safeguarding the platform and the nodes involved from being adversely affected in case of any disruption.

As we have seen before, there is a possibility that there can be a defective or compromised node that controls the majority of the operations or transactions while adding or editing blocks that are added, we cannot fully be sure that they do not have any malicious intent.

---

[67] See *Jonathan Marcus, Trevor Levine, Daniel O'Connell, Skadden, Arps, Slate, Meagher & Flom LLP - Commodity Exchange Act Liability for Smart Contract Coders - https://corpgov.law.harvard.edu/2019/03/03/commodity-exchange-act- liability-for-smart-contract-coders/*

The Bitcoin blockchain has an MIT License in place,[68] which goes as below:

"THE MIT LICENSE (MIT)
Copyright (c) 2009-2019 the bitcoin core developers Copyright (c) 2009-2019 bitcoin developers

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "software"), to deal in the software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the software, and to permit persons to whom the software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the software.

THE SOFTWARE IS PROVIDED "AS IS "WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.'"

This and other similar disclaimers will help the blockchain developers limit their liability to a large extent.

The main area where these disclaimers play a major role is in Initial Coin Offerings (ICO), which detail their own terms and conditions, including limiting their liabilities. AKM Global,[69] and Lympo Token[70] are the recent ICOs that have joined this bandwagon to safeguard their platform and the nodes involved. The Blockchain Luxembourg S.A User Agreement[71] details all the various terms and conditions for the user when they enter to use the platform.

These disclaimers ease a huge burden on the blockchain platforms that do not have any safety net by the legal regulations in most parts of the world. They also serve as a guiding text in case of any dispute that might arise against the blockchain platform itself.

3.6. Liabilities under EU Data Protection Law

The advent of the General Data Protection Regulation (hereinafter: the "GDPR" or the "Regulation)[72] has generated controversy among blockchain enthusiasts because of the nature of such a technology conflicts somehow with certain provisions contained in the Regulation.

---

[68] *See*, https://github.com/Veil-Project/veil/blob/master/COPYING.

[69] *See*, https://akminvest.com/wp-content/uploads/2017/11/Terms-and-conditions.pdf.

[70] *See*, https://akminvest.com/wp-content/uploads/2017/11/Terms-and-conditions.pdf.

[71] *See*, https://www.blockchain.com/legal/terms.

[72] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Tt is important to specify how this regulation acts:

- on a vertical level, attributing a sanctioning power to the data protection authorities of the countries belonging to the European Union with regard to the subjects involved in the processing of personal data; and

- on a horizontal level, integrating the contractual relationship between the data controller and the data processor, which are required to sign a data processing agreement according to Art. 28 GDPR, and the contractual relationship between the data subject and the data controller.

Article 4 (1) of the GDPR defines personal data as "*any information relating to an identified or identifiable natural person*." According to Article 3, the GDPR applies to "*the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*", as well as to companies outside the EU where their processing activities related to offering goods or services to data subjects in the EU or to the monitoring of their behaviors.
Moreover, 'data processing' means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission.*"[73] That means that any personal data stored on a blockchain is subject to the GDPR if the controller or the processor acts in the EU or process EU citizens' data somewhere else. It is implied that the reform is meant for centralized data processing systems, where there is a clear controller of the data ('data controller') and defined third parties who merely process the data ('data processors').[74]
Briefly, according to the GDPR, the data controller is the party that determines the purposes and means of processing, while the data processor follows the controller's instructions and process data on behalf of the controller. Under the GDPR, such parties need to determine their roles as controllers or processors and agree a contract that sets out their responsibilities, i.e. the aforementioned data processing agreement according to Art. 28 GDPR. But how is it possible to define who falls within those roles where data processing is managed through a blockchain, which runs on nodes, supposedly spread all over the world, and therefore it is decentralized in its nature? Technically, every person who accesses the network, and therefore every node contributing to the blockchain, may be considered a data controller.

Before going deeper, it is worth remembering that the distinction between permissioned and permissionless blockchains is related to participation in the network, execution of the consensus protocol and maintenance of the shared ledger. A permissioned blockchain acts as a closed ecosystem, where only selected participants can validate transactions or executing other operations depending on the authorization level granted by the central authority that controls the ecosystem. On the contrary, a permissionless blockchain allows anyone to validate transactions.

Hence, assuming that a company implements a permissioned blockchain for business purposes and that business involves processing personal data of EU residents, such a company is - legally speaking - the central party that determines the purpose and means of processing data.

---

[73] *See*, Article 4 (2) of the GDPR.

[74] *See*, Chapter IV, Section 1 of the GDPR.

For this reason, this company should be considered the sole data controller. If an external body is empowered by the company to oversee the permissioned network, this body could play the role of a data processor, but if it contributes to determine the purpose and means of processing, then it should be considered joint controller. Moreover, other parties and so other nodes could serve as data processors: in this example, the data processor agreement might consist of signing terms and conditions for contributing to the network maintenance. These nodes should not be considered data controllers because they do not determine the purpose and the means of processing.

This a purely speculative and extremely simplistic theoretical scheme, that does not take into account where nodes are located, which node at what precise moment is processing the personal data, the data of who is being processed at that moment (EU or non-EU residents?) and all the technical peculiarities of that very blockchain. Things in practice are much more complicated. Moreover, such a scheme for GDPR cannot address public permissionless blockchains.

Indeed, the lack of a central party governing the blockchain - which characterizes public permissionless blockchains – makes *de facto* implausible to have a 'data controller' within the meaning expressed in the GDPR. As a consequence, it is also difficult to determine who plays the role of 'data processor'. In such a case, nodes and miners do not concretely have the power to determine the means and purposes of the processing, and therefore they should not be recognized as data controllers. At the same time, they

should not be considered data processors, because otherwise data controllers – whoever they are - would be obliged to conclude data processing agreements with a potentially unlimited number of nodes, which is practically not feasible in a permissionless distributed network where everyone can operate and validate transactions without any authorization being required.

All the points examined so far are serious issues because reveal uncertainty about who falls within the territorial scope of the GDPR, which role the parties exactly play, and therefore who carries certain obligations and liabilities under the GDPR.

Going further, the GDPR grants citizens the 'right to rectification' and the right to be forgotten', namely the rights of the data subject to obtain from the controller the rectification of inaccurate personal data or deletion of data.[75] Therefore, let us assume, for example, that a user decides to use a service managed by a blockchain-based platform: the user will accept the terms and conditions of the service, then will express consent to the processing of personal data. What happens if personal data is only stored on the blockchain? Can the user obtain the rectification or deletion of data? How can he obtain such measures if the blockchain is supposed to be immutable in its nature?

The principle 'privacy by design' contained in Article 25 - which basically states that privacy needs to be inherent to systems and processes, and that includes the technological architecture used by businesses – in conjunction with Article 32 suggests using pseudonymization and cryptography to improve security.

---

[75] *See*, Article 16 and Article 17 of the GDPR. Article 17 which provides that the controller is obliged to erase personal data where: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Pseudonymization means that personal data are related to pseudonyms. Hence, a potential solution might be recording pseudonymized personal data on blockchain, and separately storing information necessary to reconnect those pseudonymized profiles with true identities on a GDPR-compliant centralized database ('off-chain' records), possibly relying on a special mapping function that will be hosted outside of the blockchain.[76]

As regards cryptography, relying on 'hashing' – namely, a process that transforms data into an unreadable piece of information (called 'hash') through cryptography would make it possible to keep the information secret. Who does not hold the necessary private key to decrypt information, cannot read it? Accordingly, blockchain technology can be used to hide the actual identity of users by using hashing and by assigning them a unique identifier such as an encrypted key. Hence, if a user asks for destroying the key, that would mean preventing anyone else from accessing his/her personal data.[77] But is it really like erasing data? Indeed, if someone holds the code to decrypt that key, then the encrypted key may still constitute personal data under the GDPR.[78]

Things get even more complicated if we consider that the Article 29 Working Party,[79] in its Opinion 05/2014, recognized hashing as a technique of pseudonymization, not anonymization, therefore it is sufficient for a hash to permit records to be linked for a piece of information to constitute personal data. As a result, can a hash that represents - for instance - a wallet be considered personal data? For all these reasons, it is pretty tough at the moment to conciliate blockchain technology with the legal framework established by the GDPR.

Companies willing to implement blockchain should first carefully work on the governance of the blockchain. In light of the above, permissioned blockchain may obviously serve better business purposes and compliance with the GDPR, as well as with KYC and AML requirements. Fitting centralized governance of the blockchain agreements between the parties that will control the nodes and will grant authorizations to other nodes in order to address the rights and obligations, and to properly allocate responsibilities of each participant.

On the other hand, the EU institutions cannot ignore what business companies demand, nor technological advancements. As a matter of fact, The European Commission has recently launched the EU Blockchain Observatory and Forum, which aims to promote blockchain throughout Europe. Moreover, the Forum recently ran a series of workshops on the impact of the GDPR on blockchain technology.

---

[76] Such a kind of implementation has been tested within the MyHeathMyData. See Koscina M., and Baye A., *When Blockchain Meets the Right To Be Forgotten: Technology Versus Law*, in *Global Engage* at http:// www.global-engage.com/life-science/when-blockchain-meets-the-right-to-be-forgotten-technology-versus- law/.

[77] *See idem*, which reports that this approach has been proposed by BC Diploma.

[78] Bennet B.C., *The GDPR and Blockchain*, in *The National Law Review* (Chicago, Illinois, July 24, 2018), at https:// www.natlawreview.com/article/gdpr-and-blockchain.

[79] Article 29 Working Party is the short name for the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States. The Working Party comprises all the representatives of the national supervisory authorities in EU Member States.

In its first report, most of the concerns discussed here have been confirmed, including the fact that GDPR was tailored on a centralized database and the difficulties in identifying data controllers on permissionless blockchains.[80] It also defined such a reconciliation process as "*a challenge for lawmakers*,"[81] thus implying that a new legislative intervention, fitting with the idea of distributed networks, is desirable.

In the meantime, favorable interpretations by EU regulators, as well as by Article 29 Working Party, would be necessary to prevent clashes between the GDPR and blockchains.

As regards to companies producing software and designing blockchain for business, it is imperative to explore all the possibilities offered by such a flexible technology, in order to develop GDPR compliant solutions.

4. Conclusions

While we have seen a glimpse of what blockchain is, what smart contract is and what a Ricardian contract is, we have also tried to answer a few questions when it came to the legal question mark of liability.

Unlike traditional ledgers and contracts, blockchain and smart contracts can go beyond the jurisdictional boundaries defying the geographical borders. While this technology can be an essential tool for many businesses, it can also expose these businesses to unexplored new risks. A firm's successful adoption of any new technology depends on its ability to manage the risks that come with that new technology; therefore, a company must establish strong governance, risk management strategies, and frameworks of control.

Our Research so far has pointed towards some possible solutions when answering this question of liability through the integration and implementation of Ricardian contracts, blockchain platform disclaimers and ICO disclaimers. This is also substantiated by various researchers and scholars who also have dedicated time and energy in trying to clear the clutter and find a plausible solution, which have been highlighted during the course of this paper.

On the other hand, an opinion of one of the most influencing commissions of the US, the Commodity Futures Trading Commission (CFTC) has stood by the opinion of its commissioner, Brian Quintenz in implying that if the purpose of the smart contract or the smart contract itself resembles any of the products that come under the purview of CFTC to review, then the coder of such contract should be held liable. This makes a very valid assignment of liability and makes it easier for the jurors who often have to deal with ambiguity get a clear picture of the situation.

---

[80] *Blockchain innovation in Europe, A thematic report prepared by the European Union Blockchain Observatory & Forum*, 16-17, at https://www.eublockchainforum.eu/reports.

[81] *Ibidem*, 17.

The other main enabler is the laws that make it challenging to enable this growing technology. While countries like the USA are making progress in making their regulations accommodative of blockchain technology, the European Union on the other hand has a stringent set of rules to be followed by institutions and businesses that are operating on a digital platform. While the EU also agrees that the growing demand for blockchain friendly laws cannot be ignored, it is yet to come up with a uniform set of regulations like the GDPR, but which is more blockchain and other distributed ledger technology friendly.

It is imperative for us, as attorneys in this ever-changing and constantly evolving arena of technology to find a suitable balance between the legal hindrances and technical

advancements and enable the smooth functioning of the use of the technologies in various businesses.

In conclusion, and answering the questions posed in earlier in the paper, it can be said that going forward, Ricardian contracts will be an important part of agreements used in

most of the blockchains. This inclusion will bring in the much-needed legal clarity for the deals made atop blockchain platforms. While Ricardian contracts are enabling legal clarity on one hand, the GDPR has views that bring out a plethora of information to light regarding data privacy and liability.

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

RISOLUZIONI QUESTIONI GIURIDICHE

IMPATTO VITA

FRODI INFORMATICHE

INTELLIGENZA ARTIFICIALE

AGAT

CRIPTOVALUTE

BIOTECNOLOGIE

BLOCKCHAIN

STRUMENTI TECNOLOGICI

ETICA E DIRITTO

DUE DILIGENCE

ROBOTICA

BIG DATA

PROCEDURA CIVILE

FRODI INFORMATICHE

NUOVE TECNOLOGIE

SOCIAL MEDIA

PROVE DIGITALI

IMPATTO VITA

FURTO DI IMMAGINI INTERNET DELLE COSE

ETICA E DIRITTO

LEGAL DESIGN

OPERE MULTIMEDIALI

COPYRIGHT

INTERNET DELLE COSE

PROCEDURA PENALE

CYBERSECURITY

PHISHING

IP

PROVA

RICERCA

E-PRIVACY

INTELLIGENZA ARTIFICIALE

SERVICE PROVIDER

SMART CONTRACT

CRIPTOVALUTE

ROBOTICA DUE DILIGENCE

FURTO DI IMMAGINI

IMPATTO VITA

PROCEDURA CIVILE

INTERNET DELLE COSE

GDPR

ROBOTICA

FRODI INFORMATICHE

BIG DATA

NUOVE TECNOLOGIE

ETICA E DIRITTO

PROCEDURA CIVILE

SPONSORED BY

intesa

4cLegal
www.4cLegal.com

Qi net

ASSOCIAZIONE AVVOCATI GIOVANI TORINO

AGA

INNOVAZIONE TECNOLOGICA E NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

DI PIER GIORGIO CHIARA

La responsabilità civile dei sistemi intelligenti autonomi: stato dell'arte e prospettive nell'esperienza comunitaria.

ABSTRACT

L'elaborato, dimostrando come l'attuale normativa di responsabilità da prodotto difettoso non offra risposte soddisfacenti al fine di assicurare l'adeguata allocazione dell'onere probatorio, propone un'analisi multilivello delle teorie di responsabilità extra-contrattuale, applicate ad un'ideale tripartizione delle tecnologie di IA, in relazione alla loro complessità ed autonomia.

KEYWORDS

Regolazione – Sistemi Intelligenti Autonomi – Robotica – IA – Responsabilità Civile – Risarcimento del Danno

TABLE OF CONTENTS

1. Introduzione

Dinanzi alla necessità di confrontarsi con una tecnologia variabile nelle sue caratteristiche, è opportuno operare delle strategie speculative di fondo nell'ottica di definire un panorama coerente con la previsione, benché instabile, delle future dinamiche. In tal senso è bene sottolineare, in via di approssimazione, come le cd. tecnologie digitali emergenti, tra cui l'intelligenza artificiale (IA), l'interazione di quest'ultima con la robotica e i sistemi di IoT (*Internet of Things*) conducano verso la creazione di nuovi prodotti e servizi, inesplorate opportunità per l'economia e il benessere delle nostre società[1].

[1] Cfr. Commission Staff Working Document, *Liability for Emerging Digital Technologies,* Bruxelles, 2018.

Nella circostanza in cui una delle tecnologie in esame *cagioni* un danno, l'allocazione della responsabilità extra-contrattuale può risultare difficoltosa in virtù delle caratteristiche delle tecnologie emergenti. Pertanto, è necessario analizzare il panorama legislativo europeo in tema di responsabilità e sicurezza per vagliarne l'applicabilità a questa nuova categoria di agenti, senza trascurare, d'altra parte, l'esigenza dei produttori di operare all'interno di un sistema connotato dalla certezza e dalla trasparenza.

Di tale elemento di complessità sembra aver preso maggiore coscienza il legislatore comunitario[2], avendo posto le basi per un percorso di ripensamento e revisione delle principali normative in vigore nell'Unione (in primis, la Direttiva sulla responsabilità da prodotto difettoso[3]) in conseguenza dell'affermarsi delle tecnologie connesse al fenomeno dell'intelligenza artificiale[4].

2. Le coordinate concettuali del problema

Nel ricostruire un sistema riconducibile all'alveo della responsabilità civile, idoneo a regolare le conseguenze di possibili eventi lesivi derivanti dalla tendenza a lasciare sempre più autonomia nell'interazione di queste tecnologie, il primo aspetto degno di nota è la profonda incertezza che permea lo sviluppo tecnologico e, conseguentemente, le proprietà che tali applicazioni sono suscettibili di assumere nel medio e nel lungo periodo.

2.1 Una prospettiva verticale

È opportuno, innanzitutto, delineare i confini concettuali delle tecnologie sotto indagine. A tal proposito, si propone, in un'ottica verticale, come livello d'astrazione, una ideale tripartizione di questi sistemi, avendo come criterio distintivo il tratto dell'autonomia[5].

---

[2] Diverse le azioni delle istituzioni europee in tal senso. *Ex multis*, si vedano: Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti

norme di diritto civile sulla robotica, 2015/2103 (INL); Commission Staff Working Document on Advancing the Internet of Things in Europe - Reaping the full benefits of a Digital Single Market, SWD (2016) 110 final.

[3] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al *ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi*.

[4] Si veda la recente nomina da parte della Commissione europea di un *expert group* al fine di revisionare l'attuale normativa in materia di responsabilità civile e di responsabilità da prodotto

difettoso in conformità alle caratteristiche delle nuove tecnologie basate sull'utilizzo di intelligenze artificiali: https:// ec.europa.eu/digital-single-market/highlevel-group-artificial-intelligence.

[5] Imponente la letteratura a riguardo dell'autonomia dei cd. *artificial agents*. Si veda, *ex multis*, LEROUX**,** C., et al., *Suggestion for a green paper on legal issues in robotic*, 2012, disponibile a: https:// www.unipv-lawtech.eu/files/ euRobotics-legal-issues-in-robotics-DRAFT_6j6ryjyp.pdf. Il concetto di autonomia, in questo contesto, può essere infatti tripartito a seconda che l'osservatore sia un ingegnere, un giurista od un filosofo. Secondo il primo, l'autonomia corrisponderebbe a "the capacity to operate in the real-world environment without any form of external control, once the machine is activated and at least in some areas of operation, for extended periods of time" (LIN, P., ABNEY, K., BEKEY, G., *Robot ethics: Mapping the issues for a mechanized world*, in *Artificial Intelligence* 175, 2011, p. 943); l'osservatore giuridico invece indicherebbe per autonomia "ogni possibilità di autodeterminazione e, quindi, le capacità attive, i poteri, i diritti soggettivi [...] o, più specificamente, la potestà di darsi un ordinamento giuridico" (ROMANO, S., *Frammenti di un dizionario giuridico*, Giuffrè, 1947, p. 14 ss.); infine, la prospettiva filosofica implicherebbe una più generale riflessione sull'auto-determinazione dell'individuo.

Primo osservabile di tale livello sarà la classe dei robot senza autonomia[6] che, in una prospettiva storica, può essere ricondotta alla categoria dei robot industriali. Il secondo punto d'osservazione è invece rappresentato da applicazioni robotiche con autonomia limitata[7], come taluni service robot[8]; come per le applicazioni industriali automatizzate, la scelta di questa categoria merceologica ha ragioni di chiarificazione espositiva che debbono sfuggire all'equazione generalizzante che vorrebbe tutti gli appartenenti a questa classe condividere il medesimo grado di autonomia.
Infine, il terzo osservabile prende in analisi i sistemi avanzati di IA. Le ultime tendenze nella ricerca sono testimoni di un rinnovato interesse nella cd. IA in senso forte[9]; se i progetti moderni infatti possono fare affidamento su *hardware* più potenti, gli sviluppi compiuti nell'ingegneria del *software* e nella neuroscienza computazionale[10] hanno contribuito a rinnovare il vigore di questi progetti.

Si prenda il caso di *OpenAI*, una realtà no-profit sostenuta da Elon Musk; paradossalmente, a dispetto di quanto suggerisca il nome, l'azienda ha deciso di non rendere pubblica la ricerca su un modello di generatore testuale con IA, chiamato GPT2. Il sistema, chiamato ad elaborare un testo -dopo aver ricevuto un *input,* ancorché ridotto- basato sulle proprie predizioni, ha valicato nettamente il confine delle potenzialità che i suoi creatori avevano idealmente tracciato[11].

---

[6] La maggior parte dei robot industriali utilizzati non sono innovativi, non sono autonomi, non imparano dai propri errori, non si adattano in fretta all'ambiente circostante: un grado diverso di autonomia non è necessario, anziché no desiderato nella stragrande maggioranza delle applicazioni industriali. Si veda GRAEFE, V., e BISCHOFF, R., *From Ancient Machines to Intelligent Robots - A Technical Evolution* – in *The Ninth International Conference on Electronic Measurement & Instruments,* IEEE, 2009, p. 420

[7] Lo scenario qui evocato può essere ricondotto al paradigma della cd. *weak autonomy*: il sistema artificiale porterà a termine un incarico per raggiungere un risultato fissato dall'essere umano. L'eterodirezione è caratteristica determinante affinché l'autonomia possa dirsi debole. Cfr., *ex multis*, BERTOLINI, A., *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, Law, Innovation and Technology, 2013, pp. 225-226

[8] La Federazione Mondiale sugli Standard (ISO 8373/2012) considera come lo spettro di autonomia dei *service* robots spazi da un livello parziale (interazione uomo-macchina) fino alla piena autonomia

(nessun intervento umano). Si veda SCHRAFT, R. D. et al., *Service Robots: The Appropriate Level of Automation and the Role of Users/Operators in the Task Execution*, Proceedings of IEEE Systems Man and Cybernetics Conference – SMC, 1993, p. 164

[9] Cfr, tra gli altri, NILSSON, J. N., *The Quest for Artificial Intelligence: A History of Ideas and Achievements*, Cambridge University Press, 2009, p. 319 e SEARLE, J. R., *Minds, Brains and Programs*

in *The Behavioral and Brain Science*, 1980, p. 417

[10] Si veda BOSTROM, N., *Superintelligence: paths, dangers, strategies*, Oxford University Press, 2014, p. 35

[11] Si veda HERN, A., *New AI fake text generator may be too dangerous to release, say creators,* The Guardian, 14/02/2019, disponibile a: https://www.theguardian.com/technology/2019/feb/14/elon-musk- backed-ai-writes-convincing-news-fiction: "*both in terms of the quality of the output, and the wide variety of potential uses is so good and the risk of malicious use so high that it is breaking from its normal practice of releasing the full research to the public in order to allow more time to discuss the ramifications of the technological breakthrough*".

Inoltre, per pervenire a questi risultati, questi modelli avanzati di *deep learning* sono stati addestrati su *datasets* 15 volte più grandi dei precedenti modelli di IA[12]. Ebbene, recenti ricerche dell'MIT hanno dimostrato come l'elevata dispendiosità computazionale di tale approccio si accompagni ad un forte consumo di energia: le emissioni di tali *training* possono superare i 290.000 kg di diossido di carbonio -approssimativamente cinque volte tanto l'emissione di una macchina media statunitense.[13]

2.2 Una prospettiva orizzontale

Il livello di astrazione prescelto, tripartito per semplicità in macro-categorie di applicazioni tecnologiche nella sezione precedente, è destinato ad avere incidenza sempre maggiore su diverse sfere del diritto privato quali: la responsabilità contrattuale ed extra-contrattuale, diritti di proprietà intellettuale, nonché questioni legate a privacy e *data protection*[14]. La decisione di evidenziare aspetti di responsabilità civile nasce dall'esigenza di rispondere alla complessità dell'allocazione del danno secondo gli schemi tradizionali, ove le tecnologie autonome siano coinvolte[15].

3. La responsabilità da prodotto difettoso

Operando una distinzione di massima tra la normativa di matrice nordamericana -suscettibile di essere valutata dai singoli stati, pur orientata al rispetto dei principi delineati dal c.d. *Third Restatement*[16]- e quella europea, è opportuno sottolineare come quest'ultima si presti, in virtù della direttiva sulla responsabilità da prodotto difettoso (in prosieguo: Direttiva)[17], ad un'analisi unitaria.

---

12 Id.: secondo Dario Amodei, direttore alla ricerca di OpenAI, GPT2 sarebbe rivoluzionaria principalmente sotto due aspetti. In primo luogo, la qualità dell'*output* è influenzata direttamente

dall'uso di un'enorme quantità di dati per il *training*; in secondo luogo, GPT2 riesce a comprendere profondamente la struttura del testo che sta analizzando, in modo tale da poterlo riassumere, destrutturare e sintetizzare.

13 Si veda HAO, K., *Training a single AI model can emit as much carbon as five cars in their lifetimes,* The MIT technology review, 2019.

14 Si veda PALMERINI, E., et al., *RoboLaw - Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics*, 2014, disponibile a: http://www.robolaw.eu/, p. 19

15 Si veda SARTOR, G., e OMICINI, A., *The Autonomy of Technological Systems and Responsibilities for their Use* in BHUTA, N., BECK, S., GEISS, R., LIU, H.-Y., KRESS, C., (a cura di), *Autonomous weapons systems: law, ethics, policy, Cambridge University Press, 2016, pp. 64-65*

16 The American Law Institute, *Restatement of the Law, (Third), Torts: Products Liability,* 1998.

17 Council Directive 85/374/EEC of 25 July 1985 *on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, http://eur- lex.europa.eu/legalcontent/EN/TXT/?uri=celex:31985L0374*.

Gli oneri probatori richiesti dalla normativa UE sono, essenzialmente, affini a quelli previsti per la prova del difetto nella disciplina USA[18]: la parte attrice è tenuta a dimostrare che il prodotto *per se* non è adatto all'attività per la quale era stato messo in commercio (*design defect*) od alternativamente che, benché astrattamente idoneo a svolgere la propria funzione, lo specifico prodotto venduto è difettoso, e, di conseguenza, ha tenuto una condotta anomala (*manufacturing defect*).

In aggiunta a ciò, gli ordinamenti domestici degli Stati Membri si presentano profondamente eterogenea, declinando in diverse maniere l'interpretazione degli elementi necessari a provare la causalità tra difetto del prodotto ed evento lesivo[19]. L'ampio spettro rappresentato dalle interpretazioni delle corti nazionali varia da posizioni prossime a forme di responsabilità semi-oggettiva (invertendo l'onere della prova e ponendolo in capo al produttore), fino a opinioni diametralmente opposte, addossando interamente l'onere della prova sull'attore[20].
Recentemente, la Commissione europea ha constatato come la normativa sulla responsabilità da prodotto difettoso, così come elaborata nel 1985, stia creando impedimenti sostanziali per l'effettivo accesso al risarcimento da parte delle vittime di illeciti; pertanto, ha incaricato un gruppo di esperti di formulare una proposta di revisione del relativo *corpus* normativo[21].

4. Criticità nell'applicazione del regime di responsabilità da prodotto difettoso alle tecnologie emergenti

Riprendendo il livello d'astrazione iniziale, è possibile ipotizzare come dall'incontro della tripartizione delle tecnologie emergenti e la responsabilità da prodotto difettoso possano nascere diversi scenari di difficile interpretazione per il giurista.
Il primo osservabile, rappresentato da robot senza autonomia, difficilmente può essere considerato destabilizzante dal momento che queste applicazioni sono guidate dall'uomo, che fissa l'obiettivo della macchina unitamente al percorso necessario per raggiungerlo: ciò rende questa classe "tecnologica" non dissimile dai prodotti tradizionali, facendola pertanto ricadere nel campo d'applicazione della direttiva[22].

I casi della *weak AI*, ossia il secondo osservabile del nostro modello, e dei sistemi avanzati di intelligenza artificiale, terzo ed ultimo grado di complessità, comportano di converso diverse difficoltà tecniche ed interpretative nel contesto della responsabilità da prodotto.

---

[18] Si veda WAGNER, G., *Robot Liability*, in LOHSSE, S., SCHULZE, R., STAUDENMAYER, D., (a cura di), *Liability for Robotics and in the Internet of Things: Munster Colloquia on Eu Law and the Digital*

Economy, Hart Nomos, 2019, pp. 27-63; cfr. BRÜGGEMEIER, G., *Tort Law of the European Union,* Wolters Kluwer, 2015, para 306, 314; OWEN, D. G., *Products Liability Law*, Thomson-West, 2015, pp. 315–334; WHITTAKER, S. D., *The EEC Directive on Product Liability,* Yearbook of European Law, 1985, pp. 234, 242–243;

[19] Si veda, *ex multis*, INFANTINO, M., ZERVOGIANNI, E., *The European Ways to Causation,* in *Causation in European Tort Law*, Cambridge University Press, 2017, pp. 84-128

[20] PALMIERI, A., PARDOLESI, R., *Difetti del prodotto e del diritto privato europeo*, in *Il Foro Italiano*, IV, 2002, c. 295.

[21] Si veda il Commission Staff Working Document su *Liability for emerging digital technologies* del 25/04/2018 (COM (2018) 237 final), consultabile al link http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51633.

[22] Si veda CALO, R., *Open Robotics*, Maryland Law Review, 70 no.3, 2011, p. 568.

Ai fini del presente lavoro, verrà preso in analisi solamente quest'ultimo livello di autonomia, in quanto è ritenuto essere il più dirompente per gli schemi di responsabilità extra-contrattuale a disposizione del giurista, oggi.

4.1 Prodotto

È dibattuto in dottrina se la componente software di un sistema avanzato di IA possa essere classificata come "prodotto", ai sensi dell'articolo 2 della Direttiva[23]. Dal momento che la Direttiva trova la sua applicazione nei confronti di tutte le cose mobili -unitamente all'elettricità, di cui espressa menzione al comma secondo, il software potrebbe essere escluso dall'ambito dello strumento comunitario per via della sua natura intangibile[24]. Da ritenersi minoritaria la dottrina che propenderebbe per la tangibilità nei casi in cui il software fosse incorporato in un bene mobile a tal punto da non poter essere più distinto da esso (ad esempio: un robot)[25]. A dimostrazione di ciò, non si è mai riconosciuta in capo ai produttori di software una responsabilità extra-contrattuale da prodotto difettoso per un difetto di codice[26].

---

[23] Imponente la letteratura sul punto. Tra i primi giuristi ad occuparsi dell'applicazione della Direttiva al software, si vedano: WHITTAKER, S., *European Product Liability and Intellectual Products*, Law

Quarterly Review, 1989, pp. 135-137; TRIAILLE, J., *The EEC Directive on Product Liability and its Application to Databases and Information,* Computer Law and Practice, 1991, pp. 218-224; STUURMAN, C., *Product Laibility for Software in EU* in VANDENBERGHE, G. P. V., (a cura di), *Advanced Topics of Law and Information Technology*, 1989, pp. 129-141

[24] Si veda ALHELT, K., *The Applicability of the EU Product Liability Directive to Software*, 34, Comparative & International Law Journal South Africa, 2001, p. 20

[25] K.-U. Link and T. Sambuc, *Federal Republic of Germany* in KELLY, P., ATTREE, R., (a cura di), *European Product Liability*, Butterworths, 1992, p. 157

[26] Si veda KIM, S., *Crashed Software: Assessing Product Liability for Software Defects in Automated Vehicles*, 12, Duke Law and Technology Review, 2018, p. 311; cfr. REUTIMAN, J. L., *Defective*

Information: Should Information be a "Product" Subject to Products Liability Claims?, 22, Cornell Journal of Law & Public Policy, 2012, p. 185: "those courts that have determined whether computer software is a 'good' under the Uniform Commercial Code have struggled to apply a tangible–intangible distinction and have reached conflicting conclusions. Such courts have tended to focus on the service- like aspects of a software sale as compared to the tangible aspects of the software medium."; cfr. inoltre con SPRAGUE, R. D., *Software Products Liability: Has Its Time Arrived?*, Western State University Law Review, 1991, pp. 137-141.

4.2 Difettosità

Adottare la nozione di difettosità, ai sensi della Direttiva[27], in un contesto algoritmico può essere sviante.
In primo luogo, è da determinarsi se le tecniche di *machine learning*, conducendo potenzialmente a risultati diversi da quelli che il consumatore può attendersi, possano rientrare nell'interpretazione di "prodotto difettoso".

Inoltre, un altro interrogativo è suscitato dalla qualità del *dataset*[28] utilizzato per l'addestramento del modello di IA, dal momento che la qualità del prodotto è direttamente influenzata dalla qualità del trattamento dei dati[29]: dei (*big*) dati *biased*, *unfair* o *imbalanced* possono minare la sicurezza legittimamente attesa nel test del consumatore ex art. 2 della Direttiva?

Si aggiunga, come ulteriore complicazione, l'inesistenza di una definizione precisa per l'errore di codice (*software fault*): qualcuno ha provato a qualificare l'eventualità del guasto come una imperfezione strutturale da ricercarsi nelle linee di codice[30].
Se, infatti, i problemi di *software design* vengono rilevati durante la fase del testing, è bene sottolineare come ci siano sostanziali differenze tra il test di un algoritmo,

---

[27] Articolo 6 della Direttiva 85/374/CEE: un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto di tutte le circostanze, tra cui: a) la presentazione del prodotto; b) l'uso al quale il prodotto può essere ragionevolmente destinato; c) il momento della messa in circolazione del prodotto.

[28] Si veda BACHMANN, A., BERNSTEIN, A., *Software process data quality and characteristics - a historical view on open and closed source projects*, in Proceedings of the joint international and annual ERCIM workshops on Principles of software evolution, 2009, pp. 119–128.

[29] Si veda BACHMANN, A., BERNSTEIN, A., *When process data quality affects the number of bugs: Correlations in software engineering datasets,* in 7th IEEE Working Conference on Mining Software Repositories, 2010, p. 9

[30] Si veda MUNSONA, J. C., NIKORAB, A. P., SHERIF, J. S., *Software faults: A quantifiable definition* in *Advances in Engineering Software*, 37, Elsevier, 2006, p. 327: "an overwhelming number of faults that

are recorded as code faults are actually design faults: the design implements the specification and the code implements the design".

ancorché “semplice”, e un prodotto tradizionale[31]. I test, invero, non possono dimostrare in modo assoluto che non ci siano errori a livello di scrittura del codice[32]. Pertanto, l’interrogativo principale è quale sia il test idoneo a determinare la “difettosità” del design di un algoritmo; più precisamente, è molto probabile che tale dimostrazione per la parte attrice, in mancanza di un quadro ben delineato di standards accettati dalla comunità[33], si risolva in una prova diabolica[34].

4.3 Causalità

Molti degli aspetti concernenti la causalità sono lasciati dalla Direttiva agli ordinamenti domestici. Se agli articoli 1 e 4 statuisce chiaramente che l’onere di provare il difetto, il danno e il nesso causale tra questi due elementi ricada interamente sulla parte attrice, condizione necessaria per la responsabilità del produttore, non specifica però quale sia lo standard della prova richiesto, o più generalmente, *come* il nesso di causa vada provato.

Come si è avuto modo di osservare, gli Stati Membri, pur adottando diverse interpretazioni degli elementi necessari a provare la causalità, possono essere accorpati in macro-modelli, senza alcuna pretesa di fondare una tassonomia generale[35].

---

[31] Cfr. con BROOKS, F. P., *No Silver Bullet*. *Essence and Accidents of Software Engineering*, Computer Magazine, 1987. L’autore sostiene come potrebbe non esserci soluzione semplice ai problemi

dell’ingegneria del software, considerati due diversi ordini di complessità: “essential complexity is inherent and nothing can remove it. In contrast, accidental complexity is created by programmers and can be dealt with. The accidental complexity of writing and optimizing machine code can be dealt with by programming in high-level languages that require fewer lines of code and have very strong checking routines that test the operation of module interfaces and help to minimize syntax and semantic errors”.

[32] Si veda LLOYD, I. J., *Information Technology Law,* Oxford University Press, 2008, p. 562; si veda inoltre ZOLLERS, F. E., MCMULLIN, A., HURD, S. N., SHEARS, P., *No More Soft Landings for Software:*

Liability for Defects in an Industry That Has Come of Age, Santa Clara Computer and High Technology Law Journal, 21, 2005, p. 750-753

[33] La violazione di standards di sicurezza è un altro modo per stabilire la difettosità, considerato che il

produttore non è responsabile, ai sensi dell’articolo 7(d) della Direttiva, ove il difetto sia “dovuto alla conformità del prodotto a regole imperative emanate da poteri pubblici”. Ebbene, in un campo di continua ed esponenziale evoluzione come quello dell’IA, potrebbe passare un significativo lasso di tempo prima che gli attori possano fare affidamento su standards idonei.

[34] Si veda BORGHETTI, J.-S., *How can Artificial Intelligence be defective?*, in LOHSSE, S., SCHULZE, R., STAUDENMAYER, D., (a cura di), *Liability for Artificial Intelligence and the Internet of Things - Münster Colloquia on EU Law and the Digital Economy IV*, Nomos/Hart publishing, 2019, p. 64

Analizzando il formante legislativo nazionale, pertanto, si nota come il nesso eziologico richiesto dalle varie ipotesi di responsabilità aquiliana previste all’interno del codice civile non sia sempre uguale a se stesso, a differenza di quanto avviene nella tutela penale, fondata sull’ineluttabile correlazione indagato/imputato-evento di reato[36].

[35] Cfr. con INFANTINO, M., ZERVOGIANNI, E., *The European Ways to Causation,* op. cit. Le autrici sostengono come la maggior parte degli ordinamenti legali dell’Unione possa essere catalogato entro tre macro-modelli: *overarching causation*, *bounded causation approach* e *pragmatic causation approach*.

Nella divisione tra causalità cd. materiale e giuridica, dove l'accertamento della prima è prodromico al secondo, è rilevante il dettato dell'articolo 1223 c.c.[37] che prevede la risarcibilità dei danni che sono "conseguenza immediata e diretta", risultato ottenibile secondo l'*id quod plerumque accidit*. La giurisprudenza, nel tempo, ha elaborato dei criteri per riconoscere, nel caso di specie, le conseguenze dannose immediate e dirette di un fatto illecito: i criteri maggiormente utilizzati sono quello della *normalità* e della *prevedibilità*[38]. Similmente, negli USA il *foreseeability-test* è essenziale nel determinare la causalità giuridica o *scope of liability*[39]. Tuttavia, "ciò che è prevedibile" è strettamente connesso al tessuto sociale, rendendo pertanto il concetto di prevedibile inscindibile dal fattore temporale e del progresso della tecnica e delle scienze[40].
Il campo dell'IA consiste di sistemi di differenti livelli di complessità e di diverse curve di apprendimento[41]: i moderni sistemi di IA, operanti su algoritmi di *machine- learning*, non hanno regole preimpostate per la risoluzione dei problemi, bensì regole per imparare ad apprendere dai dati a disposizione[42].

---

[36] Si veda GIANTI, D., *Il Nesso di Causalità come Elemento della Fattispecie di Responsabilità Aquiliana* in MONATERI, P. G., GIANTI, D., BALESTRIERI, M., (a cura di), *Causazione e Giusitificazione*

del Danno, Giappicchelli, 2016, p. 43: la giurisprudenza e le dottrine maggioritarie concordano nel riconnettere il settore della responsabilità aquiliana -per quanto concerne l'accertamento del nesso causale- alla disciplina penalistica, ancorché soggettiva, antropomorfizzata e dunque dissimile dalla responsabilità civile, di cui agli artt. 40-41 c.p. "ove sarebbero stati trasposti principi di carattere generale suscettibili di trovare applicazione in ogni ramo dell'ordinamento"

[37] L'articolo 2056 c.c. rimanda, per il settore della r.c., al dettato di alcuni articoli della disciplina delle obbligazioni, quali: 1223, 1226 e 1227 c.c.

[38] Si veda GIANTI, D., *Il Nesso di Causalità come Elemento della Fattispecie di Responsabilità Aquiliana*, op. cit., p. 51; cfr. con MARTIN-CASALS, M., *Causation and Scope of Liability in the Internet of Things (IoT)*, in LOHSSE, S., SCHULZE, R., STAUDENMAYER, D., (a cura di), *Liability for Robotics and in the Internet of Things: Munster Colloquia on Eu Law and the Digital Economy*, Hart Nomos, 2019, pp. 212-213.

[39] Cfr. *Case Wagon Mound* and *Overseas Tankship (U.K.) vs Morts Dock and Engineering Co*. e *Case Doughty vs Turner Manufacturing Co*. *Ltd* (1964)

[40] Si veda KARNOW, C. E. A., *Liability for Distributed Artificial Agents*, Berkeley Technology and Law Journal, 1996, p. 180

[41] BATHAEE, Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, Harvard Journal of Law and Technology, 31, 2018, p. 898: l'ampio spettro varia da IA aventi il compito di *processare* decisioni attraverso regole pre-programmate per il processo inferenziale, sino a moderni sistemi di IA basati su algoritmi di *machine-learning* in grado di "apprendere" dai dati.

Cfr. con GOODFELLOW, I., et al., *Deep Learning*, The MIT Press, p. 2: "Several artificial intelligence projects have sought to hard-code knowledge about the world in formal languages. A computer can reason automatically about statements in these formal languages using logical inference rules. This is known as the knowledge base approach to artificial intelligence". Since such approach was unsuccessful, AI researchers are now more focused on creating AIs able to solve problems as humans would do, "by using intuition — problems such as image recognition, identification of patterns in large amounts of data, or language and voice processing".

[42] Si veda ALPAYDIN, E., *Introduction to Machine Learning*, The MIT Press, 2010, p.xxxi: "we need learning in cases where we cannot directly write a computer program to solve a given problem but need example data or experience. One case where learning is necessary is when human expertise does not exist, or when humans are unable to explain their expertise".

Gli algoritmi di *machine- learning* vengono addestrati su dei set di dati, quindi, per convalidare i primi set, gli algoritmi vengono testati su nuovi set[43]. Il risultato del processo di convalida sarà un modello capace di generalizzazioni[44]: sottoposti nuovi set di dati, il modello sarà in grado di elaborare predizioni attraverso delle categorizzazioni[45].

Nel dominio della causalità, questi modelli di IA rappresentano uno scenario nuovo, potenzialmente problematico, in quanto la complessità delle strutture algoritmiche che *processano* le moli di dati da cui poi verranno elaborate le inferenze non è capita in ogni sua parte dai creatori stessi del sistema. Si pensi al caso delle reti neurali (*deep neural networks*)[46], consistenti in decine di migliaia di neuroni artificiali i quali, lavorando in modo diffuso, elaborano un *output*, a partire dall'*input*, problema, iniziale trovando degli schemi nei dati o tracciando delle connessioni logiche o relazionali[47].

Tale mancanza di trasparenza, dovuta alla complessità di queste ampie reti multilivello di neuroni artificiali, è denominata *black box problem*[48]. L'IA può infatti arrivare a soluzioni controintuitive per l'uomo, può trovare oscuri schemi nascosti in petabyte di dati, può lavorare come un essere umano mai potrebbe (per esempio, nella velocità computazionale) oppure ancora può basare le proprie decisioni su collegamenti pluridimensionali tra variabili inaccessibili, nella loro totalità, ad un essere umano[49]. Se nemmeno il creatore dell'IA può prevedere ex ante *come* il modello perviene ad un certo risultato, è ragionevole attendersi che nemmeno la persona diligente possa riuscire in questo compito.

---

[43] BATHAEE, Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, op. cit., p. 900.

[44] Si veda GOODFELLOW, I., et al., *Deep Learning*, op. cit., p. 20

[45] Si veda FLACH, P., *Machine Learning: the Art and Science of Algorithms that Make Sense of Data*, Poznan University of Technology, 2012, disponibile al link: http://www.cs.put.poznan.pl/tpawlak/files/ ZMIO/W02.pdf, p. 52

[46] Si veda GOODFELLOW, I., et al., *Deep Learning*, op. cit., pp. 13-14: "the modern term "deep learning" goes beyond the neuroscientific perspective on the current breed of machine learning models. It appeals to a more general principle of learning multiple levels of composition, which can be applied in machine learning frameworks that are not necessarily neurally inspired".

[47] Si veda nuovamente BATHAEE, Y., *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, op. cit., p. 901.

[48] Si veda, per un'analisi più approfondita, PASQUALE, F., *The Black Box Society: the Secret Algorithms that Control Money and Information*, Harvard University Press, 2015; cfr. con LEMLEY, M.

A., e CASEY, B., *Remedies for Robots*, University of Chicago Law Review, 2019, p. 64; si veda inoltre CASTELVECCHI, D., *Can We Open the Black Box of AI?*, Nature, Oct. 5, 2016: l'autore, per spiegare la difficoltà concettuale dietro la comprensione del funzionamento delle reti neurali, paragona tale impresa con la difficoltà neuroscientifica di capire i funzionamenti delle cellule nervose del cervello umano.

[49] Si veda DENG, L., e YU, D., *Deep Learning: Methods and Applications*, Foundations & Trends in Signal Processing, 2013, p. 205

Pertanto, i criteri della normalità e della prevedibilità sembrano destinati a fallire in quanto viene meno la prevedibilità in astratto, ossia quelle conseguenze dannose che normalmente discendono da una certa condotta, che connota il nesso eziologico "attraverso la predeterminazione di una serie di doveri di precauzione ai quali fare riferimento per valutare se sussista o meno l'imputabilità del fatto dannoso"[50].

5. Un'analisi multilivello di sistemi alternativi nell'attribuzione della responsabilità

In attesa del report finale del gruppo di lavoro presso la Commissione Europea sulla revisione della Direttiva 85/374/CEE, alla luce di quanto emerso sulla *prima facie* difficoltosa applicabilità del paradigma della responsabilità da prodotto alle cd. tecnologie emergenti, è opportuno esaminare altri schemi di responsabilità extra- contrattuale, considerando tali sistemi intelligenti autonomi come attori o agenti, a seconda del vario grado di autonomia di cui sono capaci, prescindendo dal dibattito sulla personalità giuridica[51].

Possibili fonti per la costruzione di una teoria di responsabilità aquiliana flessibile abbastanza da disciplinare gli agenti artificiali possono provenire dalle esistenti dottrine di responsabilità semi-oggettiva, relative al danno cagionato da soggetti diversi dal chiamato a risarcire (artt 2048-2052). O persino da antichi istituti come quello del *peculium*, di provenienza romanistica, collegato alla schiavitù.

Dette analogie sono provocatorie; ciò non di meno hanno il pregio di mostrare come le avanzate -e sorprendenti- capacità degli agenti artificiali, unitamente al vasto spettro di decisioni loro delegate, permettano una comparazione con altri agenti e altri attori fotografati dal diritto.

Questa sezione mira a definire un approccio multilivello alla questione della RC, anziché uno più marcatamente *sliding-scale*, come nel paper di Boscarato[52]: l'autrice, distinguendo tra le azioni robotiche che possono essere prevedute dal programmatore/ utilizzatore e quelle che non sono programmate/imprevedibili, costruisce un sistema di attribuzione della responsabilità per fatto altrui in considerazione delle sempre maggiori capacità dei robot presi in esame. Quindi, al penultimo stadio, in virtù della capacità locomotiva, avremo la responsabilità per il fatto dell'animale, per pervenire all'ultimo stadio evidenziato -l'apprendimento- in cui l'analogia è con i minori. Tuttavia, una metodologia *scalare*,che riconnette uno schema di responsabilità ad una specifica classe di agenti in virtù di una specifica capacità, corre il rischio di non trovare riscontro nella vastità e imprevedibilità del mercato: è ben possibile che il robot con capacità locomotorie venga in seguito dotato di capacità di apprendimento (che in origine erano appannaggio esclusivo dello schema di responsabilità genitoriale ex 2048 c.c.).

---

[50] Si veda nuovamente GIANTI, D., *Il Nesso di Causalità come Elemento della Fattispecie di Responsabilità Aquiliana*, op. cit., p. 59

[51] Si veda CHOPRA, S., e WHITE, L. F., *A Legal Theory for Autonomous Artificial Agents*, University Michigan Press, 2011, p. 122-123

[52] BOSCARATO, C., *Who is responsible for a robot's actions? An initial examination of Italian law within a European perspective* in VAN DEN BERG, B., e KLAMING, L., (a cura di), *Technologies on the*

stand: legal and ethical questions in *Neuroscience and robotics*, Wolf Legal Publishers, 2011, disponibile al link: https://www.academia.edu/4407305/Who_is_responsible_for_a_robot%CA%BCs_actions_An_initial_examination_of_Italian_law_within_a_European_perspective

5.1 ***La rappresentanza: analogie e differenze con la legge romanistica della schiavitù***

Diverse voci in dottrina sostengono che l'IA sia una nuova forma di rappresentanza[53]. Il salto concettuale che si richiede al lettore è di non considerare tali tecnologie, animate da IA, alla stregua di meri artefatti. È risalente agli anni '80 una corrente di studiosi di cibernetica che proponeva una distinzione opportuna dei sistemi di IA dalla materia inanimata, in considerazione delle categorie a quest'ultima applicabili quali l'individualità, l'intelligenza, la locomozione e la percezione[54]. Ancora, si consideri che Weizenbaum, teorico estremamente critico con tali posizioni ritenute troppo *futuristiche*, riconosceva a tali sistemi autonomi una dignità di organismi dotati di "auto-coscienza", in considerazione della loro abilità nel "socializzare"[55]. Considerare tali sistemi avanzati di IA come qualcosa di diverso e ulteriore dalla materia inanimata può condurre su una china pericolosa; ciò non di meno, i giuristi di duemila anni fa avrebbero considerato illogico categorizzare gli schiavi fuori dal paradigma della proprietà. Così come alla condizione di schiavo, gradualmente, sono stati riconnessi sempre più diritti e doveri, anche nel contesto delle tecnologie avanzate di IA è possibile ipotizzare un ampliamento della sfera giuridica, in virtù di un progressivo avvicinamento alle capacità cognitive umane in ogni loro forma[56]: creativa[57], morale[58] e logica[59].

Riprendendo un'intuizione di Pagallo[60], l'istituto del *peculium* può essere decisivo nel dirimere il dibattito circa la responsabilità all'interno di un rapporto di rappresentanza. Gli schiavi, non avendo la capacità giuridica, non potevano disporre di nulla; non potevano peggiorare la posizione patrimoniale del *dominus* e quindi nessun negozio da essi compiuto avrebbe potuto generare *obligatio* a carico dello stesso *dominus*[61].

---

[53] Si veda FLORIDI, L.,e SANDERS, J. W., *On the Morality of Artificial Agents*, Minds and Machines, 14(3), 2004, pp. 349–379; cfr. con CHOPRA, S., e WHITE, L. F., *A Legal Theory for Autonomous Artificial Agents*, op. cit., p. 119-152; cfr. con PAGALLO, U., *The Laws of Robots*, Springer, 2013, pp. 154-155; cfr. con SARTOR, G., *Cognitive Automata and the Law*, op. cit., p. 282; cfr. con WEITZENBOECK, E. M., *Electronic Agents and the Formation of Contracts*, in *International Journal of Law and Information Technology*, 2001, p. 204; cfr. con HILDEBRANDT, M., et al.. *Bridging the accountability gap: Rights for new entities in the information society?*, Minnesota Journal of Law, Science & Technology, 11(2), 2010, p. 550; cfr. con KARNOW, C. E. A., *Liability for Distributed Artificial Agents*, op. cit., p. 192

[54] Si veda KEMENY, J. G., *Man and the Computer*, Charles Scribner's Sons, 1972, p. 10: l'autore, alludendo ai sistemi di IA come *servo-mechanisms*, consente teoricamente un primo parallelismo comparativo con gli schiavi.

[55] Cfr. con WEIZENBAUM, J., *Computer Power and Human Reason*, W. H. Freeman and Co, 1976, p. 210.

[56] Si veda LEHMAN-WILZIG, L., *Frankenstein Unbound: towards a legal definition of Artificial Intelligence*, Futures, 1981,

[57] Cfr. con https://edition.cnn.com/style/article/artificial-intelligence-ai-art/index.html
[58] Si veda FLORIDI, L., SANDERS, J. W., *On the Morality of Artificial Agents* in *Minds and Machines*,

Springer, 2004, pp. 349-379
[59] Cfr. con https://www.theguardian.com/technology/2017/dec/07/alphazero-google-deepmind-ai-

beats-champion-program-teaching-itself-to-play-four-hours

[60] Si veda PAGALLO, U., *The Laws of the Robots*, op. cit., p. 82

[61] Si veda MARRONE, M., *Istituzioni di Diritto Romano*, Palumbo, 2006, p. 195. [62] Si veda PAGALLO, U., *The Laws of the Robots*, op. cit., p. 82

Tuttavia, già dall'età arcaica, era in uso conferire ai servi una somma di danaro, o altri beni, configurante il *peculium*, appunto, che essi guadagnavano attraverso il loro lavoro: proprietario

peculiare restava il *dominus* ma si ammise che i servi potessero trasferire il possesso delle *res peculiares* salva la facoltà del padrone di revocare il *peculium* in ogni momento.

In modo similare, Pagallo suggerisce che un simile "portafoglio robotico" possa fornire le basi per una forma di assicurazione per le obbligazioni assunte da questi sistemi[62]. La responsabilità del possessore o produttore di questi sistemi sarà pertanto limitata al valore del *peculium digitale*, garantendo però che i creditori delle obbligazioni contratte dai sistemi autonomi vedano soddisfatte le proprie pretese.

Per quanto concerne il versante della responsabilità extra-contrattuale, l'istituzione del *peculium*, in una prospettiva di responsabilità oggettiva a carico dell'utilizzatore o del produttore, può porre un limite al risarcimento, fissato nella somma del portafoglio concesso all'agente. Inoltre, tale peculio digitale, sarebbe una garanzia per tutti i terzi che verrebbero a contatto con l'agente artificiale autonomo, prescindendo da ogni valutazione sulla colpa nel caso in cui risultasse un danno da tale interazione.

5.2 ***Teorie di responsabilità vicaria: analogie e differenze con i minori, gli impiegati e gli animali.***
Possibili fonti per la costruzione di una teoria di responsabilità aquiliana flessibile abbastanza da disciplinare gli agenti artificiali possono provenire dalle esistenti dottrine di responsabilità oggettiva e semi-oggettiva rinvenibili nel codice civile, relative al danno cagionato da soggetti diversi dal chiamato a risarcire. È opportuno pertanto provare ad applicare alla classe di agenti artificiali autonomi le dottrine di responsabilità per il danno cagionato da minore (art. 2048 c.c.) e dagli impiegati (art. 2049 c.c.) e il danno commesso dagli animali (art. 2052 c.c.).

L'analogia con i minori
È possibile tracciare un parallelismo tra un sistema robotico integrato da intelligenza artificiale e minori vicini alla maggior età; presupposto logico per l'applicazione di tale responsabilità al sistema artificiale è la libertà di imparare, muoversi, agire e reagire. Come i minori, alcuni agenti artificiali potrebbero essere capaci di apprendere nuove reazioni e comportamenti dall'esperienza diretta[63]: come i genitori provvedono all'educazione del minore senza però poter controllare ogni singolo atto del loro comportamento, così alcune azioni del robot potrebbero sfuggire all'intenzione originaria del programmatore o dell'utilizzatore.

---

63 Si veda ALLEN, C., VARNER, G., ZINSER, J., *Journal of experimental and theoretical artificial intelligence*, Taylor & Francis Online, 2000, 12, pp. 251–261; cfr. con FLORIDI, L., SANDERS, J. W., *On the Morality of Artificial Agents* in *Minds and Machines*, op. cit., pp. 349-379

Parte della dottrina interpreta la responsabilità di cui all'art. 2048 come fondata su una presunzione di colpevolezza, bipartita tra la *culpa in educando* e *in vigilando*. Risulta pertanto un'inversione dell'onere probatorio favorevole al danneggiato: il tutore o genitore per andare esente da responsabilità dovrà provare di non aver potuto impedire che il fatto illecito venisse commesso[64]. Tuttavia, una più prudente dottrina[65] sottolinea come la responsabilità vicaria del genitore si avvicini al modello della responsabilità oggettiva, forte delle considerazioni giurisprudenziali circa il rapporto di coabitazione tra genitori e minore; i primi sono infatti i soggetti meglio posizionati per evitare il danno ingiusto.

L'analogia con gli impiegati
La dottrina *respondeat superior*, che disciplina il regime di responsabilità aquiliana

all'interno del rapporto lavorativo tra commesso e committente, implica una responsabilità oggettiva del datore quando l'agente commetta un fatto illecito: il datore, tuttavia, non dovrà assorbire tutti i costi degli incidenti inevitabilmente provocati dall'esercizio dell'attività, ma solo di quelli risultanti dall'aver fallito nell'imporre uno standard di diligenza sul lavoratore[66]. Una più recente corrente dottrinale e giurisprudenziale sembra invece porre maggiormente l'accento sullo scopo dell'agente durante l'esecuzione del compito assegnatogli da cui risulta il danno: il datore è responsabile se la condotta illecita è funzionalmente o strumentalmente connessa all'incarico ricevuto all'interno del rapporto[67]. L'articolo 2049 c.c. disegna quindi un regime di responsabilità oggettiva, la cui giustificazione è da rinvenirsi nel conferimento del compito da parte del datore: se la condotta dell'agente non è riferibile al *normale* e *prevedibile* ambito di svolgimento del lavoro, allora il datore non sarà responsabile per tale condotta[68].

---

[64] Si veda SCIONTI, R., *Sulla responsabilità dei genitori ex art. 2048 C.C.*, in Diritto di famiglia, 1978, p. 1434; cfr. con MAJELLO, U., *Responsabilità dei Genitori per il Fatto del Figlio Minore e Valutazione del Comportamento del danneggiato ai fini della Determinazione del Contenuto della Prova Liberatoria*, in Diritto e Giustizia, 1960, pp. 44-48.

[65] Si veda MONATERI, P. G., *Manuale della Responsabilità Civile*, op. cit., p. 303; *contra* cfr. con SALVI, C., *La Responsabilità Civile*, in IUDICA, G., ZATTI, P., (a cura di), Trattato di Diritto Privato, Giuffré, 1998, pp. 185-188.

[66] Si veda VISINTINI, G., *Trattato Breve della Responsabilità Civile*, Cedam, 1999, pp. 658-659; cfr. con GALOPPINI, A., *La Responsabilità dei Padroni e dei Committenti*, in *Rivista Trimestrale Diritto*

Processuale Civile, 1968, p. 1209; cfr. con GAUDINO, L., *La Responsabilità dei Padroni e dei Committenti nella Casistica Giurisprudenziale*, in *Contratto e Impresa*, 1987, pp. 915 ss.

[67] Cfr. con DAVOLA, A., *Responsabilità del datore di lavoro e nesso di occasionalità necessaria: la rilevanza delle finalità del preposto ai fini dell'imputazione dell'illecito*, in Il Foro Italiano, III, 2016,

p. 2775

[68] Così Cass., 4/11/2014, no. 23448, Giurisprudenza italiana, 2015, p. 554, con la nota di Scapellato: *La responsabilità dell'agenzia assicurativa per la condotta illecita del suo subagente*; cfr. con la nota di Crusco, *La Corte di legittimità fa un "passo indietro" sulla responsabilità solidale dell'assicuratore per il fatto illecito del subagente privo del potere di rappresentanza?*

Mutatis mutandis, tali considerazioni possono essere applicate anche ad agenti artificiali autonomi qualora deviino dal compito originariamente assegnato dal datore o supervisore: è probabile che in contesti di *machine learning*, o di *deep learning*, ciò

accada. Tale scenario sarebbe dirompente perché richiederebbe una riflessione ulteriore sulla responsabilità del sistema stesso, riaccendendo il dibattito sulla personalità giuridica delle tecnologie emergenti.

L'analogia con gli animali

Specialmente nel dominio della robotica, la complessità interpretativa e di interazione cresce quando i sistemi artificiali autonomi sono dotati dell'abilità locomotiva. Grazie alla capacità di agire, reagire[69], di essere situati[70] e muoversi, a diversi livelli di autonomia, è opportuno tracciare un'analogia con i modelli di responsabilità oggettiva[71] che inquadrano il danno cagionato dall'animale: non vi è la necessità di provare la colpa[72]. Si consideri inoltre che nell'Enciclopedia di Stanford di Filosofia, Bringsjord definisce l'IA come:

the field devoted to building artificial animals (or at least artificial creatures that – in suitable contexts – appear to be animals) and, for many, artificial persons (or at least artificial creatures that – in suitable contexts – appear to be persons)[73].

Seguendo questo paradigma, il punto focale del sistema risarcitorio investigherà *come* l'uomo ha trattato il sistema sotto indagine, piuttosto che indagare il design e la costruzione particolare della macchina[74]. È evidente, pertanto, come l'accoglimento di tale paradigma, come già visto in parte nella sezione sui minori, suggerisca uno scarto tra i soggetti responsabili: dai produttori, agli utilizzatori.

Il primo tratto peculiare di tale regime risiede nella relazione intercorrente tra il custode e l'animale: giurisprudenza e dottrina concordano nel considerare l'uso[75] e la custodia quali tratti configuranti il potere-dovere del custode sull'animale, incluse pertanto tutte quelle misure di sicurezza idonee a prevenire pregiudizio per i terzi[76].

---

[69] Si veda WOOLDRIDGE, M. J., JENNINGS, N. R., *Agent theories, architectures,and languages: A survey,* in *Intelligent agents*, Springer, 1995, pp. 1-22

[70] Si veda MATHEWS, N., et al., *Spatially Targeted Communication and Self-Assembly*, IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012, link disponibile a: http:// code.ulb.ac.be/dbfiles/MatChrOgrDor2012iros.pdf

[71] Si veda MONATERI, P. G., *Manuale della Responsabilità Civile,* op. cit., p. 405; cfr. con TRIMARCHI, P., *Rischio e responsabilità oggettiva*, op. cit., p. 169; cfr. con RODOTÀ, S., *Il Problema della Responsabilità Civile*, op. cit., p. 144

[72] Così Cass., 9/12/1979, no. 2615, *D'Erasmo c. Gismondo, MGI,* 1970; Cass., 3/08/1962, no. 2329, *Volpi c. Piscini, MGI,* 1962; Cass., 16/11/1955, no. 3745, *Bertelli c. Pareti, MGI,* 1955

[73] Si veda BRINGSJORD, S., et al., *Artificial Intelligence,* The Stanford Encyclopedia of Philosophy (edited by E. N. Zalta), 2018, link disponibile a: https://plato.stanford.edu/archives/fall2018/entries/ artificial-intelligence/

[74] Si veda PAGALLO, U., *The Laws of Robots,* op. cit., p. 72.

[75] Anche se l'utilizzo non è requisito necessario: la fruizione dell'animale può avvenire a meri fini

estetici. Si veda BELFIORE, A., *Appunti in materia di danni cagionati da animali*, in Giurisprudenza di merito, 1973, I, p. 14; cfr. con FRANZONI, M., *Dei Fatti Illeciti,* Zanichelli e Roma Società Editrice del Foro Italiano, 1993, pp. 609 ss.

[76] Si veda VISINTINI, G., *Trattato Breve della Responsabilità Civile,* op. cit., pp. 704-705

La parte attrice dovrà provare il nesso eziologico intercorrente tra il danno e l'azione dell'animale, parte attiva necessaria del fatto-evento e di conseguenza non un mero strumento dell'azione umana. Tale sottolineatura è ben applicabile anche nel contesto degli agenti artificiali autonomi, dal momento che i sistemi di nuova generazione, ove richiesta, garantiscono un'autonomia tale da rendere l'intervento umano non solo inutile[77], ma financo dannoso[78].

Si consideri, infine, che nel contesto di agenti artificiali avanzati, i funzionamenti interni, incidenti sulla condotta del sistema, non sono chiari e trasparenti agli occhi dei custodi; un *device* potrebbe eseguire un comportamento inaspettato ed imprevedibile perché frutto di un apprendimento nel corso del tempo, ancorché non desiderato dal custode, oppure come conseguenza di un malfunzionamento[79].

6. Profili conclusivi

Il panorama che emerge da un tentativo di analisi dello stato dell'arte circa il dibattito sulle regole di responsabilità extra-contrattuali nel contesto delle tecnologie autonome emergenti è di non chiara riunificazione.
Un contesto che sappia coniugare la necessità di sicurezza, incentivi per la ricerca e sviluppo e al tempo stesso promuova la diffusione di tali sistemi autonomi deve essere coordinato con un regime di responsabilità che protegga gli interessi dei consumatori danneggiati. In questo lavoro, la responsabilità da prodotto difettoso, il regime ordinario per i beni mobili di consumo e durata, è stata il punto di inizio della riflessione circa l'adeguatezza e applicabilità delle regole di responsabilità extra-contrattuale vigenti. Dal momento che tale schema sembra non essere, allo stato dell'arte, idoneo a regolamentare il dirompente settore tecnologico riferibile alla classe degli agenti autonomi, e dal momento che l'applicazione per via analogica di esistenti schemi di responsabilità aquiliana non offra soluzioni di sicura affidabilità, è opportuno tracciare una linea di demarcazione tra un generale standard di *negligence* e un modello di responsabilità oggettiva, pura, analizzandone vantaggi e svantaggi da una prospettiva di teoria economica del diritto.

Ricondurre la responsabilità del produttore all'alveo della *strict* liability, dunque, entro forme di responsabilità che escludono la rilevanza dell'elemento soggettivo proprio dell'illecito civile tradizionalmente inteso fondando l'onere risarcitorio in via prioritaria sull'elemento causale e sull'indesiderabilità sociale della condotta oggetto di responsabilità, pone l'accento sulla considerazione che chi risulta vittima di un illecito (dal suo punto di vista) inspiegabile o inevitabile non dovrebbe essere mai chiamato a sopportarne il costo.

---

[77] Si veda MATTHIAS, A., *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata,* Ethics and Information Technology, 2004, p. 177; cfr. con KARNOW, C.E.A., *The application of traditional tort theory to embodied machine intelligence*, op. cit., p. 5

[78] Si veda WAGNER, G., *Robot Liability*, op. cit., p. 34-35

[79] Si veda CHOPRA, S., WHITE, L. F., *A Legal Theory for Autonomous Artificial Agents,* op. cit., p. 131

In tale contesto, il produttore, dovendo fronteggiare il costo totale di ogni incidente che coinvolga il sistema da lui commercializzato, tenderà razionalmente a minimizzare tale costo: applicando un regime di *strict liability* il costo sociale relativo ai danni causati da sistemi intelligenti autonomi è uguale al costo privato del produttore degli stessi, che massimizzerà, aderente ad un approccio economico tradizionale, gli incentivi ad implementare ogni ricerca ed innovazione diretta alla

sicurezza, imponendo così il più elevato tasso di deterrenza in capo all'azienda[80]. Una seconda prospettiva che favorirebbe l'implementazione di tale modello si riferirebbe ad una efficienza maggiore dal punto di vista dell'allocazione dei costi del rischio: ne risulterebbe una selezione naturale dei produttori, ove solo i più virtuosi sopravviverebbero[81]. Ogni produttore, soprattutto in questo settore, ha costi diversi per soddisfare gli standard di sicurezza in relazione al proprio prodotto/ servizio; dal momento che il costo derivante dagli incidenti è inversamente proporzionale a quello di realizzazione di nuove interazioni tecnologiche, è altamente probabile che si verifichi un processo di auto-selezione tra gli attori nel mercato. I produttori in grado di realizzare un maggiore costo marginale di messa in sicurezza per unità di prodotto tenderanno ad investire in maniera minore in tale settore, rispetto a coloro che, raggiunto un livello di sofisticazione tecnologica comparativamente elevato, affrontano costi marginali minori[82].

Secondo una certa corrente dottrinale, una responsabilità fondata su uno standard di colpevolezza eviterebbe alcuni svantaggi che si concretizzerebbero in un regime di *strict liability*. Su tutti, il cd. *chilling effect*[83]. Un sistema fondato sulla colpa giustifica generalmente la responsabilità in virtù del mancato rispetto di taluni requisiti, come il rispetto di standard di sicurezza o diligenza. Dal punto di vista dei consumatori, il prezzo per unità sarebbe inferiore rispetto ad un sistema di *strict liability*; purtuttavia, ciò potrebbe scoraggiare gli eventuali compratori della nascente tecnologia a causa del maggiore onere probatorio richiesto da tale regime.

In conclusione, un regime di responsabilità oggettiva ha il considerevole vantaggio (tale da superare ad opinione di chi scrive il modesto beneficio di un costo per unità ridotto applicando delle teorie di *negligence*), rispetto ad un sistema fondato sulla colpa, di rassicurare il consumatore nella prospettiva risarcitoria: lo spostamento dei pesi che occorre nei diversi oneri probatori non è dovuto all'accoglimento di una prospettiva *pro victima* bensì si conforma al criterio processualistico della vicinanza dell'onere della prova. Il produttore, in un contesto di elevata sofisticazione, complessità tecnologica dovuta ai tanti attori e servizi in gioco, sarà il soggetto che potrà più agevolmente farsi carico di tale onere.

---

[80] Si veda DAVOLA, A., *Veicoli Autonomi, Sinistri Stradali e Nuovi Modelli di Responsabilità Civile*, in Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido - studi in onore di Roberto Pardolesi, La Tribuna, 2018

[81] Si veda COOTER, R., ULEN, T., *Law and Economics*, Pearson, 2004. Si veda inoltre BERTOLINI, A., *Insurance and Risk Management for Robotic Devices: Identifying the Problems*, in *Global Jurist*, 2016, 1 ss.

[82] Si veda nuovamente DAVOLA, A., *Veicoli Autonomi, Sinistri Stradali e Nuovi Modelli di Responsabilità Civile*, op. cit., p. 12.

[83] I produttori potrebbero infatti aspettare a commercializzare tali tecnologie fino ad essere ragionevolmente certi di poter calcolare i danni potenziali causati dai loro "prodotti", al fine di internalizzare il costo degli incidenti traslandolo sugli acquirenti. Si veda, sul punto, nel settore delle auto a guida autonoma, SCHELLEKENS, M., *Self-driving cars and the chilling effect of liability law*, 31 Computer Law & Security Review, 2015, pp. 506-517.

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA
NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

SPONSORED BY

intesa

4CLEGAL
www.4cLegal.com

Qi net

ASSOCIAZIONE GIOVANI AVVOCATI TORINO

LA NORMATIVA SUL CYBERBULLISMO: PER UN BILANCIO A DUE ANNI DALL'ENTRATA IN VIGORE DELLA L. 29 MAGGIO 2017, N. 71

DI RICCARDO MICHELE COLANGELO

Indice

Abstract

L'intervento avrà ad oggetto gli aspetti informatico-giuridici della l. 71/2017 in materia di cyberbullismo, in modo particolare quelli correlati alla procedura di oscuramento, rimozione o blocco, di cui all'articolo 2, e al procedimento di ammonimento, disciplinato dall'articolo 7.
La normativa italiana sul cyberbullismo – talvolta oggetto di fuorvianti semplificazioni interpretative – verrà analizzata tenendo conto dello stato di attuazione della medesima, nonché alla luce del GDPR e in una prospettiva *de jure condendo,* in relazione anche al d.d.l. approvato dalla Camera dei deputati il 3 aprile 2019 e trasmesso alla Presidenza del Senato, recante "Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere" (c.d. "Codice rosso"). Conclude l'analisi un'aggiornata rassegna comparatistica.

1. I principali aspetti informatico-giuridici

Sono trascorsi due anni esatti dal 18 giugno 2017, data dell'entrata in vigore della l. 29 maggio 2017, n. 71, pubblicata in Gazzetta Ufficiale il 3 giugno del medesimo anno[2]. Si tratta, notoriamente, della principale fonte di rango primario disciplinante il fenomeno del cyberbullismo[3].
Le considerazioni che tale ricorrenza permette di svolgere sono particolarmente numerose e di vario tipo: in questa sede, previa sintetica illustrazione dei principali aspetti informatico-giuridici della l. 71/2017, nei limiti di quanto rilevante in relazione alle questioni applicative emerse nel biennio, ci si soffermerà sulla esposizione di alcune considerazioni *de jure condendo* e comparatistiche[4].

Nonostante il clamore mediatico ingenerato in Italia non solo dai casi di cyberbullismo più gravi e tristemente noti[5], ma anche dall'entrata in vigore della legge Ferrara, è possibile osservare come quest'ultima, sin dal 2017, sia poco conosciuta e, talvolta, oggetto di fuorvianti semplificazioni interpretative.
Tra le letture forzate di quello che è stato correttamente tratteggiato in dottrina come il "diritto "mite" della legge Ferrara"[6], la più rilevante concerne la chiara scelta del legislatore di non introdurre nuove fattispecie delittuose e, nello specifico, alcun reato di cyberbullismo[7].

---

[2] G.U. n. 127 del 3 giugno 2017.

[3] In realtà, oltre alla legge 71, altre due leggi – una precedente e una posteriore – considerano espressamente il cyberbullismo, pur non disciplinandolo.
In argomento, il riferimento più risalente può essere rinvenuto nell'art. 1, comma 1250, lett. h), l. 27 dicembre 2006, n. 296 (la c.d. legge finanziaria 2007, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato") ove, riferendosi al fondo per le politiche della famiglia di cui all'ar. 19, comma 1, d.l. 4 luglio 2006, n. 223, convertito, con modificazioni, dalla l. 4 agosto 2006, n. 248 [...], si specifica che il medesimo viene utilizzato al fine di finanziare "interventi a tutela dell'infanzia e dell'adolescenza, con particolare riferimento alle situazioni di vulnerabilità socioeconomica e al disagio minorile, anche con riferimento al contrasto del fenomeno del cyberbullismo".

Il comma sopra richiamato è stato sostituito dall'art. 1, comma 482, l. 30 dicembre 2018, n. 145 ("Bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021"), che fa riferimento al medesimo fondo.
In particolare, la lett. h) risulta caratterizzata da un disposto perfettamente sovrapponibile a quello citato nella presente nota e, quindi, considera espressamente il fenomeno del cyberbullismo.

[4] Per approfondimenti maggiormente esaustivi è possibile fare riferimento a quanto ho pubblicato sulla rivista internazionale "Informatica e diritto" dell'ITTIG-CNR: RICCARDO M. COLANGELO (2017), *La legge sul cyberbullismo. Considerazioni informatico- giuridiche e comparatistiche*, in "Informatica e diritto", XLIII annata, vol. XXVI, 2017, n. 1-2, pp. 397-418.

[5] Primo fra tutti, il caso di Carolina Picchio, in merito al quale si rimanda a quanto specificato, *ex multis*, in: ELENA BUCCOLIERO, MARCO MAGGI (2017), *Contrastare il bullismo, il cyberbullismo e i pericoli della Rete*, Milano, Franco Angeli, in particolare pp. 235-236.
Gli stretti legami tra il suicidio di Carolina Picchio, vittima di cyberbullismo, e la legge 71 sono meglio approfonditi in GIUSEPPE CASSANO, CORRADO MARVASI (2018), *La responsabilità educativa dei genitori per minori cyberbulli*, in "Danno e Responsabilità", 6, 2018, pp. 763 ss.

[6] GIUSEPPE CASSANO, CORRADO MARVASI (2018), *La responsabilità educativa dei genitori per minori cyberbulli*, op. cit.

[7] "La formulazione di un'apposita figura di reato risulterebbe ardua e avrebbe scopi più che altro simbolici: da un lato, le molteplici modalità di offesa riconducibili al fenomeno in questione mal si prestano a essere catturate da una singola fattispecie; dall'altro lato, non paiono sussistere vuoti di tutela, vista la riconducibilità delle condotte in questione a norme incriminatrici già esistenti, delle quali si offre una panoramica ragionata": così CIRO GRANDI (2017), *Il "reato che non c'è": le finalità preventive della legge n. 71 del 2017 e la rilevanza penale del cyberbullismo*, in "Studium Iuris", 12, 2017, p. 1040.

Tale linea di politica legislativa, chiaramente desumibile dal dettato normativo della legge 71, sovente non è emersa, in tutto o in parte, soprattutto nei titoli degli articoli di testate giornalistiche e di opere dottrinali[8].

La dottrina giuridica, dopo una prima fioritura di monografie dedicate al fenomeno complesso del cyberbullismo, pubblicate a ridosso dell'entrata in vigore della legge Ferrara, ed eccezion fatta per alcuni paper, pare non aver continuato ad interrogarsi sul tema in maniera significativa[9].
Il riferimento alla legge 71, che ha determinato un salto di qualità circa la prevenzione del fenomeno in ambito giovanile e scolastico[10], è stato, in ottica particolarmente critica, al centro di alcuni articoli apparsi su varie testate giornalistiche nazionali nel mese di giugno 2019[11]. Di alcune di tali riscontri critici, non sempre adeguatamente fondati, si darà atto nel prosieguo.

1.1 La procedura di oscuramento, rimozione o blocco

L'art. 2 della legge Ferrara, rubricato "Tutela della dignità del minore", dispone quanto segue:

"1. Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro[12] dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo URL (Uniform resource locator[13]), non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici.

2. Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del citato decreto legislativo 30 giugno 2003, n. 196".

La procedura di cui all'art. 2, come sopra articolata, si fonda ancora attualmente sulle ordinarie procedure di segnalazione di contenuti illeciti, che i vari social network notoriamente mettono a disposizione degli utenti. Tale procedura, infatti, è saldamente legata all'operatività del tavolo tecnico interministeriale per la prevenzione e il contrasto del cyberbullismo, coordinato dal MIUR ed istituito presso la Presidenza del Consiglio dei Ministri *ex* art. 3, comma 1, legge Ferrara.

---

[8] A mero titolo esemplificativo, si rimanda a quanto indicato in RICCARDO M. COLANGELO (2017), *La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche*, op. cit., p. 400 ed in particolare le note 12, 13 e 14.

[9] Le monografie principali, infatti, datano quasi tutte 2017. Senza pretesa di esaustività, si fa riferimento a: GIUSEPPE CASSANO (a cura di) (2017), *Stalking, atti persecutori, cyberbullismo e tutela dell'oblio. Aggiornato con la legge 29 maggio 2017, n. 71*, Assago, WKI; MARIA SABINA LEMBO (2017), *Bullismo e cyberbullismo dopo la L. 29 maggio 2017, n. 71*, Santarcangelo di Romagna, Maggioli; MAURO ALOVISIO, GIOVANNI BATTISTA GALLUS, FRANCESCO PAOLO MICOZZI (a cura di) (2017), *Il cyberbullismo. Alla luce della legge 29 maggio 2017, n. 71*, Roma, Dike; VALENTINA SELLAROLI (2017), *Il nuovo reato di cyberbullismo (l. 29 maggio 2017, n. 71)*, Milano, Giuffrè; MAURO BERTI, SERENA VALORZI, MICHELE FACCI (2017), *Cyberbullismo. Guida completa per genitori, ragazzi e insegnanti*, Trento, Reverdito; MARCO OROFINO, FEDERICO GUSTAVO PIZZETTI (a cura di) (2018), *Privacy, minori e cyberbullismo*, Torino, Giappichelli; ANNA LIVIA PENNETTA, GIULIANA ZILIOTTO (2019), *Bullismo, cyberbullismo e nuove forme di devianza*, Torino, Giappichelli.

[10] Cfr., a titolo esemplificativo, LORENZO ISACCO (2019), *Social network ed imprese, la sfida quotidiana che nasce dai giovani*, in "Il diritto industriale", 2, 2019, pp. 161 ss.

[11] http://osservatorio-cyberbullismo.blogautore.repubblica.it/2019/06/08/senatrice-ferrara-legge-ancora-non-applicata-e-gia-la- vogliono-affossare/ (visionato l'ultima volta in data 18 giugno 2019)

A due anni dall'entrata in vigore della legge 71, tuttavia, l'operatività di tale tavolo tecnico non può di certo dirsi piena, a fronte non solo di un numero di convocazioni *de facto* inconsistente[14], ma soprattutto della mancata adozione di quanto previsto dai commi 2 e 3 dell'art. 3, legge Ferrara. Tali commi concernono rispettivamente il piano di azione integrato per il contrasto e la prevenzione del cyberbullismo[15], che avrebbe dovuto essere redatto dal tavolo tecnico "entro sessanta giorni dal suo insediamento", nonché il codice di coregolamentazione per la prevenzione e il contrasto del cyberbullismo[16], da adottarsi entro il medesimo termine.

La mancata predisposizione di quanto appena indicato, ed in modo particolare del codice di coregolamentazione, al quale, a norma dell'art. 3, comma 3, legge 71, "devono attenersi gli operatori che forniscono servizi di social networking e gli altri operatori della rete internet" ha tutt'ora una ricaduta negativa in ordine alla piena applicabilità dell'art. 2, legge Ferrara.

Ciò in quanto avrebbe dovuto già essere istituito un "comitato di monitoraggio", con il preciso compito di

"identificare procedure e formati standard per l'istanza di cui all'articolo 2, comma 1, nonché di aggiornare periodicamente, sulla base delle evoluzioni tecnologiche e dei dati raccolti dal tavolo tecnico [...], la tipologia dei soggetti ai quali è possibile inoltrare la medesima istanza secondo modalità disciplinate con il decreto di cui al medesimo comma 1".

[12] In merito all'aggettivo "altro" - che parte della dottrina, in maniera non comprensibile, espunge dalle citazioni del disposto del vigente art. 2 - si riporta quanto indicato dal Servizio Studi della Camera, nel Dossier n. 315/2 - Schede di lettura, in data 20 marzo 2017: "Si chiarisca, all'art. 2, comma 1, la portata del richiamo a qualsiasi "altro" dato personale del minore diffuso in rete, previa conservazione dei dati originali. Non risulta infatti evidente quali siano i dati del minore cui si va ad aggiungere qualsiasi "altro" dato diffuso in rete". Così all'URL https://documenti.camera.it/Leg17/Dossier/Pdf/GI0384B.Pdf (consultato in data 10 giugno 2019).

[13] Tale dato, tuttavia, non sempre è effettivamente conoscibile – e, quindi, indicabile – da parte dell'utente, soprattutto nel caso di applicazioni per smartphone.

[14] Il tavolo risulta insediato in occasione del *safer internet day* di febbraio 2018: cfr. https://www.miur.gov.it/web/guest/-/il-6-febbraio- e-il-safer-internet-day (consultato in data 10 giugno 2019). Tale insediamento risulta comunque parziale in quanto non sono presenti *ab origine* tutti i soggetti indicati dal vigente art. 3, comma 1: a fine maggio 2018, infatti, era prevista la scadenza per la presentazione delle candidature di associazioni, enti e operatori intenzionati a collaborare con il tavolo tecnico interministeriale.

[15] Tale piano dovrebbe essere corroborato da "un sistema di raccolta di dati finalizzato al monitoraggio dell'evoluzione dei fenomeni e, anche avvalendosi della collaborazione con la Polizia postale e delle comunicazioni e con altre Forze di polizia, al controllo dei contenuti per la tutela dei minori": così l'art. 3, comma 2.

[16] Tale codice di coregolamentazione non va confuso con il codice di autoregolamentazione in materia di cyberbullismo, che si tentò di approvare tra il 2013 ed il 2014, come è curiosamente riscontrabile in parte della dottrina: si vedano i riferimenti in materia indicati in RICCARDO M. COLANGELO (2017), *La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche*, op. cit., in particolare, pp. 408-409, nota 47. In argomento, è stato correttamente affermato: "pare definitivamente naufragata anche la proposta di Codice di Autoregolamentazione contro il Cyberbullismo avviata dal Comitato Media e minori e sottoposta a consultazione pubblica". Così ARIANNA THIENE (2017), *Riservatezza e autodeterminazione del minore nelle scelte esistenziali*, in "Famiglia e Diritto", 2, 2017, pp. 172 ss., in particolare la nota 20.

Nelle more, è stato predisposto, da parte dell'Autorità Garante per la protezione dei dati personali, un modulo per facilitare l'utenza nell'invio della segnalazione, disponibile on line dal 23 agosto 2017[17]. Tale modulo, che richiama sia le condotte costituenti cyberbullismo ai sensi dell'art. 1, comma 2, legge 71, sia quanto indicato *ex* art. 2, deve tuttavia essere applicato nello stato di fatto attuale. A titolo esemplificativo, in assenza di apposite procedure e formati standard, non è ordinariamente possibile ottenere, in esito all'istanza inoltrata ai sensi dell'art. 2, una ricevuta allegabile al modulo predisposto dall'Autorità Garante, per comprovare l'inadempimento del titolare del trattamento, presupposto necessario per l'intervento dell'Autorità medesima[18] .

Inoltre, il modulo non prevede espressamente un campo deputato alla firma (sia essa chirografa, digitale o elettronica), bensì semplicemente l'indicazione di "nome e cognome"; inoltre, a pagina 4, si trova l'informativa sul trattamento dei dati personali, resa ai sensi dell'art. 13, d.lgs. 196/2003, articolo abrogato – in periodo successivo rispetto alla pubblicazione del modulo – dal d.lgs. 101/2018.

In ordine alla scarsa consistenza numerica – circa un centinaio – delle segnalazioni *ex* art. 2 rivolte, nei due anni di vigenza della legge Ferrara, all'Autorità Garante per la protezione dei dati personali, recentemente lamentata dalla stampa[19], è opportuno tenere presente quanto indicato dal presidente dell'Autorità medesima, che ha di recente qualificato come "poco frequente" l'inerzia dei social in esito a segnalazioni di casi di cyberbullismo e quindi alle istanze di oscuramento, rimozione o blocco ai sensi dell'art. 2[20].

---

17 Disponibile all'URL: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6732688 (consultato in data 10 giugno 2019).

18 Il Garante richiede espressamente l'allegazione di "copia della richiesta inviata e altri documenti utili": così a pagina 3 del modello disponibile sul sito ufficiale dell'Autorità Garante per la protezione dei dati personali, all'URL https:// www.garanteprivacy.it/ documents/10160/0/Modello+per+la+segnalazione+reclamo++in+materia+di+cyberbullismo.docx/ bee0b13d-24c6-4889-af91- a17fae45c6cc?version=1.7 (consultato in data 10 giugno 2019).

19 Cfr. https://www.avvenire.it/attualita/pagine/cyberbullismo-ecco-perch-la-legge-non-salva-i-ragazzi (visionato in data 5 giugno 2019).

20 Cfr. ANTONELLO SORO, *Contro il revenge porn estendere l'ammonimento*, "Italia oggi", 17 giugno 2019, p. 5.

1.1.1 I rapporti con la disciplina di cui al GDPR ed al Codice privacy novellato

Tale ultimo riscontro mette in luce lo stretto legame tra la normativa sul cyberbullismo e quella sulla privacy, attualmente rinvenibile nel GDPR[21] e nel d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.
Tale riscontro non va sottaciuto, e in questa sede va messo in luce in particolare il riferimento al minore ultraquattordicenne, espressamente riportato nell'art. 2, comma 1, che inizialmente ha suscitato qualche perplessità in dottrina, considerato che, in base alla normativa applicabile *ratione temporis* in Italia, i soggetti minori di età non potevano manifestare alcun valido consenso al trattamento dei propri dati personali.

L'art. 8 GDPR, rubricato "Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione" ed applicabile dal 25 maggio 2018, al par. 1 dispone che, nei casi in cui rilevi la base giuridica del consenso,

"per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale".

Il medesimo paragrafo consente agli Stati membri di stabilire *ex lege* "un'età inferiore a tali fini purché non inferiore ai 13 anni": il legislatore italiano, in argomento, ha stabilito un'età minima di anni 14 – pienamente corrispondente a quanto previsto *ex* art. 2, comma 1, legge Ferrara – per quanto concerne il consenso dei minori[22] .

A tali norme fa riferimento anche una interessante ordinanza del Tribunale di Rieti del 7 marzo 2019, alla quale si rinvia circa i presupposti della tutela cautelare nei casi di diffusione, tramite social, di immagini e dati riguardanti soggetti minorenni[23].

1.2 Il procedimento di ammonimento

L'art. 7 della legge Ferrara, rubricato "Ammonimento", dispone quanto segue:

"1. Fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594, 595 e 612 del codice penale e all'articolo 167 del codice per la protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196[24], commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento di cui all'articolo 8, commi 1 e 2, del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, e successive modificazioni.
2. Ai fini dell'ammonimento, il questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale.

3. Gli effetti dell'ammonimento di cui al comma 1 cessano[25] al compimento della maggiore età".

---

[21] Si tratta notoriamente del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), il cui testo integrale è consultabile all'URL: https://eur- lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679 (visionato in data 10 giugno 2019).

[22] "Il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione": così l'art. 2 quinqies, comma 1, d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.

[23] Tale ordinanza risulta pubblicata in "Famiglia e Diritto", 6, 2019, pp. 591 ss., con nota di ROSA FORCINITI, *Tutela cautelare e d'urgenza e diffusione di immagini di soggetti minori sui social networks.*

Si noti come l’assenza di espresso richiamo dei commi 3 e 4 dell'art. 8, d.l. 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla l. 23 aprile 2009, n. 38, sia stata motivata da precise scelte di politica legislativa.
Tra i rilievi critici recentemente operati dalla stampa in relazione alla legge Ferrara, emerge lo scarso numero di ammonimenti (in un articolo, quantificati in tre)[26].

In realtà, una puntuale analisi degli articoli di cronaca ancora oggi liberamente disponibili on line e le chiare e recenti precisazioni della stessa prima firmataria del d.d.l. smentiscono oggettivamente tale conteggio, che va pertanto considerato al ribasso[27].
In ogni caso, è lo stesso presidente dell’Autorità Garante per la protezione dei dati personali ad aver recentemente affermato come sia attestata la scarsa conoscenza degli strumenti introdotti dalla legge Ferrara a beneficio dei minori[28]. Il medesimo, inoltre, concorda circa la necessità di ampliare il novero delle fattispecie delittuose, costituenti anche atti di cyberbullismo, nell’ambito della procedura di ammonimento di cui all’art. 7, legge 71[29].

---

[24] L’art. 594 c.p. risulta abrogato dal 2016, mentre l’art. 167, d.lgs. 196/2003 è stato sostituito ad opera del d.lgs. 101/2018, ma non è stato abrogato.
Anche alla luce di tali rilievi, potrebbe essere utile sfruttare al meglio il procedimento di ammonimento, rendendolo applicabile anche in relazione ad altre fattispecie delittuose costituenti anche atti di cyberbullismo e di conseguenza anche incluse nella definizione di cui all’art. 1, comma 2, legge Ferrara.

[25] La prima firmataria del d.d.l. ha recentemente specificato che “in assenza di recidiva entro il diciottesimo anno il provvedimento amministrativo del Questore decade senza conseguenze”: https://leparoleascuola.it/2019/06/13/un-primo-bilancio-sulla-legge-contro- il-cyberbullismo-intervista-allon-elena-ferrara/ (visionato in data 20 giugno 2019).

[26] Così, ad esempio, nell’articolo pubblicato sul sito del quotidiano Avvenire in data 5 giugno 2019, ove si specifica che nel meridione (“da Napoli a Palermo”) non è stato possibile acquisire i dati riguardo agli ammonimenti destinati ai cyberbulli ai sensi della legge Ferrara: https://www.avvenire.it/attualita/pagine/cyberbullismo-ecco-perch-la-legge-non-salva-i-ragazzi (visionato in data 5 giugno 2019).

[27] Cfr. http://osservatorio-cyberbullismo.blogautore.repubblica.it/2019/06/08/senatrice-ferrara-legge-ancora-non-applicata-e-gia-la- vogliono-affossare/ (visionato in data 10 giugno 2019).

[28] Cfr. ANTONELLO SORO, *Contro il revenge porn estendere l’ammonimento*, “Italia oggi”, 17 giugno 2019, p. 5.

[29] Cfr. ANTONELLO SORO, *Contro il revenge porn estendere l’ammonimento*, “Italia oggi”, 17 giugno 2019, p. 5, ove si auspica l’estensione dell’ammonimento anche a condotte rientranti nel c.d. *revenge porn*, in merito al quale si veda quanto argomentato *infra.*

2. Alcune considerazioni *de jure condendo*

Già nel 2016, la Camera aveva modificato il testo della proposta di legge C. 3139, trasmessa dal Senato il 21 maggio 2015, non solo introducendo anche la disciplina del bullismo ed esulando dall'ambito giovanile e scolastico (caratteristiche comuni ad alcune recenti proposte di legge), ma anche con l'intenzione di novellare l'art. 612 bis c.p., che notoriamente prevede e punisce il delitto di atti persecutori[30].

Nello specifico, si intendeva introdurre nuovi commi all'interno dell'art. 612 bis c.p.: ciò emerge chiaramente dal disegno di legge S. 1261-B, trasmesso dalla Camera il 22 settembre 2016[31].

In particolare, l'art. 8 – in seguito stralciato dal testo definitivamente approvato – rubricato "Modifica all'articolo 612-bis del codice penale, concernente il delitto di atti persecutori", disponeva la soppressione delle parole "ovvero se il fatto è commesso attraverso strumenti informatici o telematici" dall'art. 612 bis c.p., comma 2 e, contestualmente, l'inserimento, dopo il secondo comma, del seguente:

> "La pena è della reclusione da uno a sei anni se il fatto di cui al primo comma è commesso attraverso strumenti informatici o telematici. La stessa pena si applica se il fatto di cui al primo comma è commesso utilizzando tali strumenti mediante la sostituzione della propria all'altrui persona e l'invio di messaggi o la divulgazione di testi o immagini, ovvero mediante la diffusione di dati sensibili, immagini o informazioni private, carpiti attraverso artifici, raggiri o minacce o comunque detenuti, o ancora mediante la realizzazione o divulgazione di documenti contenenti la registrazione di fatti di violenza e di minaccia".

L'art. 8, comma 2, prevedeva inoltre una modifica dell'art. 240, comma 2, n. 1-bis) c.p., introducendo una nuova ipotesi di confisca obbligatoria degli strumenti informatici o telematici utilizzati, in tutto o in parte, per la commissione anche del reato di cui all'art. 612 bis c.p.

Sulla base di tali premesse, risulta ora possibile indicare, nell'ambito dell'attuale legislatura, i più rilevanti progetti di legge che meritano in questa sede un sintetico commento, sempre in una prospettiva *de jure condendo*.

---

[30] Cfr. RICCARDO M. COLANGELO (2017), *Cyberbullismo e responsabilità: Internet è veramente un mondo virtuale?*, in P. PASSAGLIA, D. POLETTI (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa, Pisa University Press, pp. 189-202.

[31] http://leg17.senato.it/service/PDF/PDFServer/BGT/00990787.pdf (visionato in data 20 giugno 2019).

Anzitutto occorre menzionare la proposta di legge C 643, presentata il 18 maggio 2018 d'iniziativa dei deputati Zanella e altri, e che risulta più genericamente rivolta ai fenomeni complessi del bullismo e del cyberbullismo. Muovendo dalla presa d'atto della vigente normativa italiana sul cyberbullismo[32], infatti, tale proposta mira chiaramente ed esclusivamente all'istituzione di una Commissione parlamentare di inchiesta sui fenomeni del bullismo e del cyberbullismo, i cui compiti risultano delineati *ex* art. 1, comma 2[33].

Decisamente più interessante risulta essere il disegno di legge S 1180 ("Modifiche alla legge 29 maggio 2017, n. 71, recante disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo")[34] .
In questa sede, il d.d.l. 1180 merita particolare attenzione in quanto, mediante lo stesso, si intenderebbe novellare la legge Ferrara, come risulta chiaramente dalla relazione e dall'articolato.

Nello specifico, tale d.d.l. è stato presentato in data 28 marzo 2019 ed annunciato nella seduta n. 105 del 2 aprile successivo. Più di recente, l'11 giugno, risulta essere stato assegnato alla 1a Commissione permanente (Affari Costituzionali) in sede redigente.
I tratti fondamentali concernono un maggiore coinvolgimento delle famiglie, ma soprattutto l'estensione della disciplina anche agli atti di bullismo[35], definito *ex* art. 1, comma 1 bis.

---

32 "Un testo che, seppur con alcune debolezze, ha consentito di mettere al centro una serie di misure di carattere preventivo ed educativo nei confronti dei minori (vittime e autori del bullismo sul *web*), da attuare anche in ambito scolastico. È inoltre prevista la possibilità – nel caso di bullismo informatico – di ottenere provvedimenti inibitori e prescrittivi a tutela dei minorenni (oscuramento, rimozione, blocco di qualsiasi altro dato personale del minore diffuso su i*nternet*, con conservazione dei dati originali eccetera)": così nell'introduzione all'articolato della proposta di legge, come riportata all'URL: http://documenti.camera.it/leg18/pdl/pdf/ leg.18.pdl.camera.643.18PDL0013170.pdf (visionato in data 20 giugno 2019).

33 "*a)* svolgere indagini sulle reali dimensioni, condizioni, caratteristiche e cause dei fenomeni del bullismo e del cyberbullismo, con particolare riguardo ai minori;
b) monitorare l'attuazione e gli effetti della normativa nazionale e regionale vigente in materia, e in particolare della legge 29 maggio 2017, n. 71, anche per individuare possibili carenze della normativa stessa rispetto al fine di tutelare la vittima della violenza e gli eventuali minori coinvolti;

c) accertare il livello di attenzione, controllo, capacità d'intervento e prevenzione da parte delle istituzioni e delle pubbliche amministrazioni, centrali e periferiche, competenti a svolgere attività di controllo, prevenzione e assistenza, nonché da parte delle associazioni interessate operanti sul territorio e il ruolo svolto dai soggetti che svolgono attività in qualità di gestori o di *provider* dei siti *internet*;

d) individuare e proporre soluzioni anche di carattere normativo e amministrativo al fine di realizzare la più adeguata prevenzione e il più efficace contrasto del fenomeno e per la tutela della reputazione digitale;
e) effettuare una ricognizione e valutare le diverse iniziative portate avanti da istituzioni, associazioni e altri soggetti che operano nel contrasto dei fenomeni del bullismo e del cyberbullismo, anche al fine di organizzare e diffondere le migliori pratiche dai medesimi elaborate, prevedendo il coinvolgimento di tali soggetti nella raccolta di dati statistici e nella produzione di rapporti periodici, in particolare con la collaborazione delle istituzioni scolastiche al fine di acquisire elementi di conoscenza sulle manifestazioni di tali fenomeni nelle classi scolastiche, dell'autorità giudiziaria e della polizia postale attraverso la raccolta e la trasmissione dei dati riguardanti i casi di denuncia e le conseguenti sanzioni che sono state applicate, nonché del Garante per la protezione dei dati personali con riferimento alle richieste di rimozione delle fattispecie lesive della reputazione *on line* e di deindicizzazione dai motori di ricerca" : http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.643.18PDL0013170.pdf (visionato in data 20 giugno 2019).

34 http://www.senato.it/service/PDF/PDFServer/BGT/01110904.pdf (visionato in data 20 giugno 2019).

35 Ai sensi dell'art. 1, comma 7, lett. f) del d.d.l., il titolo verrebbe così sostituito: "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del bullismo e del *cyberbullismo*".

"l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, a danno di una o più vittime, idonee a provocare in esse sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni per ragioni di lingua, etnia, religione, orientamento sessuale, aspetto fisico, disabilità o altre condizioni personali e sociali della vittima".

Ciò in quanto, come si afferma nella relazione, "occorre [...] rendere completo l'intervento legislativo, attraverso la previsione normativa di strumenti che agiscano in contrasto, anche al bullismo, così come inizialmente previsto nella proposta di legge esaminata nella XVII legislatura"[36] .
In prima analisi, tale definizione di bullismo, anche in quanto priva di ogni riferimento all'età[37] ed agli ambiti scolastici e di gruppo, pare destare qualche significativa perplessità, così come la soppressione del riferimento al minore ultraquattordicenne quale soggetto legittimato nell'ambito della procedura di oscuramento, rimozione o blocco[38]; inoltre, non si riscontra alcun intervento integrativo circa la definizione del cyberbullismo e la disciplina dell'ammonimento.

Particolarmente rilevanti, inoltre, risultano le proposte di legge C 1453[39], C1524[40], C 1537[41] e C 1543[42], che in questa sede verranno sinteticamente analizzate in ordine di presentazione.
La prima, presentata il 17 dicembre 2018 e recante "Modifiche al codice penale e alla legge 29 maggio 2017, n. 71, e altre disposizioni per l'uso responsabile della rete *internet*", risulta essere stata assegnata lo scorso 7 giugno alle Commissioni riunite Giustizia e Trasporti in sede referente.

Nella relazione, oltre alla illustrazione di alcune modifiche al codice penale, per quanto maggiormente interessa in questa sede, si specifica che

"l'articolo 2 stabilisce nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyberbullismo*, novellando la legge 29 maggio 2017, n. 71, sotto tre aspetti che, alla luce dell'esperienza applicativa, hanno sollevato alcune perplessità.
In primo luogo, si prevede che ogni istituto scolastico, nell'ambito della propria autonomia e in conformità alle linee di orientamento stabilite a livello nazionale, da un lato, debba adottare il proprio codice interno per la prevenzione e il contrasto del fenomeno del *cyberbullismo*; da un altro lato, sia tenuto a istituire un tavolo permanente di monitoraggio con la partecipazione dei rappresentanti degli studenti, degli insegnanti, delle famiglie e degli esperti di settore. La *ratio* è quella di completare, con un organo locale a livello del singolo istituto, prossimo alla realtà concreta e quotidiana, la strategia di orientamento, regolamentazione e monitoraggio che ad oggi è confinata solo a livelli «di governo» superiore, fisiologicamente più lontani dalle dinamiche della specifica realtà della singola scuola.

In secondo luogo, si prevede il rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48, pari a 500.000 euro per ciascuno degli anni 2020, 2021 e 2022. [...].
In terzo luogo, si modifica la misura dell'ammonimento, in modo da assicurarne il finalismo rieducativo. Si prevede, infatti, che il questore convochi il minore, unitamente ad almeno un genitore o a un'altra persona esercente la responsabilità genitoriale, al dirigente scolastico e a un tecnico designato dai servizi territoriali, per definire uno specifico progetto personalizzato volto alla rieducazione dell'autore della condotta, anche attraverso l'esercizio di attività riparatorie o di utilità sociale".

---

36 Si fa riferimento al testo del d.d.l. Ferrara, come modificato dalla Camera: v. *infra.*
37 Va dato atto che il nuovo titolo mantiene comunque il riferimento alla tutela dei minori: v. *supra.*

38 L'art. 1, comma 1, lett. b) del d.d.l. dispone che "all'articolo 2, comma 1, [della legge Ferrara] la parola: «ultraquattordicenne» è soppressa".

39 http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.1453.18PDL0041530.pdf (visionato in data 20 giugno 2019). 40 http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.1524.18PDL0044650.pdf (visionato in data 20 giugno 2019). 41 http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.1537.18PDL0044690.pdf (visionato in data 20 giugno 2019).

42 I dettagli relativi a tale proposta di legge ("Introduzione degli articoli 612-ter e 612-quater del codice penale e altre disposizioni per il contrasto del bullismo e del bullismo informatico (cyberbullismo)") sono reperibili all'URL: http://www.camera.it/leg18/126?tab=1&leg=18&idDocumento=1543&sede=&tipo= (visionato in data 20 giugno 2019). Il testo completo, alla data di ultima consultazione, non risulta ancora disponibile, per cui non è attualmente possibile una più adeguata analisi del medesimo.

Come anticipato nella relazione, l'art. 2 della proposta di legge, rubricato "Nuove disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", dispone le modifiche sopra indicate agli artt. 4, 6, e 7 della legge Ferrara.
In merito alla proposta di adozione, da parte di ogni istituzione scolastica, di un "codice interno per la prevenzione e per il contrasto del fenomeno del *cyberbullismo*", sia sufficiente in questa sede ricordare che è già previsto ai sensi dell'art. 5, comma 2, legge 71, che i regolamenti delle istituzioni scolastiche, nonché il patto educativo di corresponsabilità debbano essere "integrati con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti". Parrebbe pertanto sufficiente che le scuole osservino quanto già previsto ex art. 5, comma 2, legge Ferrara, nonché nelle più recenti linee di orientamento ministeriali in materia[43], anche sulla base del riscontro che tale articolo non sarebbe in alcun modo oggetto di novellazione da parte della proposta di legge *de qua.*

L'istituzione di un "tavolo permanente di monitoraggio con la partecipazione dei rappresentanti degli studenti, degli insegnanti, delle famiglie e degli esperti di settore", di fatto insediato con una strutturazione simile presso gli Uffici scolastici regionali e territoriali, probabilmente non si presta operativamente ad essere attivo presso ciascuna istituzione scolastica, che è già dotata di un referente nominato, con compiti di coordinamento; può essere comunque condiviso lo spirito di maggiore ed effettiva corresponsabilità che emerge dalla previsione *de jure condendo.*

In merito alla sostituzione dell'art. 7, comma 2, legge 71, essa si traduce nella previsione della contemporanea convocazione non solo del minore e di almeno un genitore o altra persona esercente la responsabilità genitoriale (come nel testo vigente), ma anche del dirigente scolastico e di un "tecnico designato dai servizi territoriali" – figura i cui contorni paiono alquanto vaghi – al fine di "definire uno specifico progetto personalizzato volto alla rieducazione dell'autore della condotta, anche attraverso l'esercizio di attività riparatorie o di utilità sociale".

Si noti come la proposta di legge, in merito all'ammonimento, non preveda alcuna integrazione delle fattispecie indicate nell'art. 7, comma 1, né l'espunzione del riferimento all'art. 594 c.p., ormai abrogato da oltre tre anni.

---

[43] Si veda quanto affermato *infra* in proposito.

[44] L'art. 1 della proposta di legge *de qua* dispone l'aggiunta alle già previste condotte di molestia e minaccia, quelle di percosse, ingiuria – ma si ricordi che l'ingiuria, depenalizzata, costituisce oggi un illecito civile sottoposto a sanzione pecuniaria – diffamazione, umiliazione, emarginazione. Soprattutto le ultime due condotte andrebbero precisate e definite, a maggior ragione trattandosi di una norma penale.

Si prevede inoltre una diminuzione di pena fino alla metà *"*se i fatti [...] sono commessi da un minorenne, ove questi si sia adoperato spontaneamente ed efficacemente per elidere o attenuare le conseguenze dannose o pericolose del reato".

La seconda proposta di legge, intitolata "Modifiche al codice penale, alla legge 29 maggio 2017, n. 71, e al regio decreto-legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835, in materia di prevenzione e contrasto del fenomeno del bullismo e di misure rieducative dei minori" e presentata il 23 gennaio 2019, risulta assegnata alla Commissione Giustizia in sede referente a far data dal 29 aprile scorso. È significativo notare come l'esame in Commissione di tale proposta di legge sia iniziato il 30 maggio 2019: tale riscontro invita l'interprete a prestare maggiore attenzione all'articolato, che attualmente prevede anzitutto delle modifiche all'art. 612 bis[44] ed all'art. 731 c.p.[45].

Per quanto maggiormente interessa in questa sede, l'art. 3 della proposta di legge reca modifiche alla legge 71.
Nello specifico, si intende novellare l'art. 5, comma 1, ed abrogare l'art. 7, legge Ferrara.
In merito all'art. 5, si intende anzitutto sostituire la rubrica attuale ("Informativa alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero") con la seguente: "Informativa alle famiglie, segnalazione all'autorità giudiziaria minorile, iniziative di carattere educativo e sanzioni disciplinari in ambito scolastico". Più rilevante risulta essere la sostituzione del comma 1 dell'art. 5[46], che considera atti sia di bullismo – dei quali non si riporta alcuna definizione, non essendo novellato l'art. 1 legge Ferrara – sia di cyberbullismo e mira ad introdurre una sistematica segnalazione ("in ogni caso") di tali atti alla Procura della Repubblica presso il tribunale per i minorenni, da parte del dirigente scolastico. Tale incombenza potrebbe essere eccessiva, soprattutto nei casi meno gravi di bullismo e di cyberbullismo, soprattutto se ed in quanto non costituenti reato e commessi da minori infraquattordicenni.

In ordine all'abrogazione dell'art. 7, sia sufficiente richiamare quanto più diffusamente argomentato *supra*, in relazione alla necessità, sostanzialmente condivisa, di ottimizzare l'istituto dell'ammonimento, migliorando il disposto dell'art. 7, ma non di certo privando vittime e famiglie della possibilità di richiedere al Questore l'ammonimento medesimo.

Si prevede inoltre l'adeguamento del d.p.r. 249/1998 ("Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondari"), prevedendo l'impegno per la scuola "a porre progressivamente in essere le condizioni per assicurare l'emersione di episodi riconducibili ai fenomeni del bullismo e del cyberbullismo, di situazioni di uso o abuso di alcool o di sostanze stupefacenti e di forme di dipendenza" e, per gli studenti, "a rispettare il dirigente scolastico, i docenti, il personale della scuola e i loro compagni" – previsione comunque inferibile dalla normativa.

---

45 Il disposto verrebbe interamente sostituito dal seguente: "Il genitore o l'esercente la responsabilità genitoriale, che ometta di impartire o di far impartire l'istruzione obbligatoria, è punito con l'ammenda da euro 500 a euro 5.000". Si noti l'esponenziale espansione della cornice edittale, in quanto la norma attualmente prevede un'ammenda massima di euro 30.

46 "Il dirigente scolastico che venga a conoscenza, in qualsiasi modo, di atti di cui all'articolo 1, realizzati anche in forma non telematica, che coinvolgono a qualsiasi titolo studenti iscritti all'istituto scolastico che dirige, in applicazione della normativa vigente e delle disposizioni del comma 2 del presente articolo e salvo che il fatto costituisca reato, ne informa tempestivamente i genitori dei minori coinvolti o i soggetti esercenti la responsabilità genitoriale su di essi e promuove adeguate iniziative di carattere educativo nei riguardi dei minori medesimi. In ogni caso, il dirigente scolastico trasmette tempestivamente la segnalazione di tali atti alla procura della Repubblica presso il tribunale per i minorenni, anche ai fini dell'adozione delle misure previste dall'articolo 25 del regio decreto- legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835». Tale articolo, rubricato "Misure applicabili ai minori irregolari per condotta o per carattere", prevede per i minori che danno "manifeste prove di irregolarità della condotta o del carattere", che il Tribunale per i minorenni possa disporre con decreto motivato l'affidamento del minore al servizio sociale minorile o il "collocamento in una casa di rieducazione od in un istituto medico-psico-pedagogico".

Si intende inoltre modificare la disciplina relativa al Patto educativo di corresponsabilità, introducendo

"l'impegno da parte delle famiglie a partecipare ad attività di formazione organizzate dalla scuola, con particolare riferimento all'uso della rete *internet* e delle comunità virtuali[47], e a collaborare con la scuola per consentire l'emersione di episodi riconducibili ai fenomeni del bullismo e del cyberbullismo, di situazioni di uso o abuso di alcool o di sostanze stupefacenti e di forme di dipendenza".

In argomento, non si dimentichi che le linee di orientamento ministeriali di ottobre 2017[48], ancorandosi al disposto normativo dell'art. 5 legge Ferrara, prevedono espressamente che

"Le misure di intervento immediato che i dirigenti scolastici sono chiamati a effettuare, qualora vengano a conoscenza di episodi di cyberbullismo, dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione".

L'art. 6 della proposta di legge *de qua* mira all'attivazione di un numero telefonico gratuito nazionale ed allo sviluppo di una applicazione informatica per dispositivi mobili, "dotata di una funzione di geolocalizzazione attivabile previo consenso dell'utilizzatore", caratteristica tecnica probabilmente considerata maggiormente utile per i casi di bullismo tradizionale particolarmente gravi.

La terza, recante "Norme per la tutela dei minori che accedono alla rete *internet* e istituzione del registro dei *provider* aderenti al codice di autoregolamentazione «*Internet* e minori»", risulta presentata in data 24 gennaio 2019 ed assegnata alla Commissione Trasporti in sede referente lo scorso 17 maggio.

Pur prestandosi a varie osservazioni informatico-giuridiche, si sottolinea in questa sede in particolare l'art. 2, rubricato "Servizi di navigazione differenziata", ove si fa riferimento al cyberbullismo:

"1. Allo scopo di contrastare la pedopornografia, la pedofilia, l'adescamento dei minori attraverso la rete *internet* e il cyberbullismo, il *provider* deve offrire all'utenza, secondo le tecnologie disponibili, servizi di navigazione differenziata per i minori, che rispettino le forme di tutela previste dal codice *internet* e minori, ovvero indirizzare l'utenza verso altri fornitori di tali servizi. Nel rispetto del principio di non discriminazione, i citati servizi non possono comunque impedire l'accesso ai contenuti sicuri.

2. Qualora l'utente non usufruisca del servizio di navigazione differenziata offerto ai sensi del comma 1, il *provider* è esentato da qualsiasi responsabilità connessa alla navigazione sulla rete *internet* e, in particolare, all'eventuale accesso a contenuti non sicuri per il minore".

---

[47] In ordine all'utilizzo del termine 'virtuale' in relazione alla Rete, si rimanda a quanto affermato in RICCARDO M. COLANGELO (2017), *Cyberbullismo e responsabilità: Internet è veramente un mondo virtuale?*, op. cit.

[48] Tali linee di orientamento sono consultabili all'URL: http://www.miur.gov.it/documents/20182/0/ Linee+Guida+Bullismo+-+2017.pdf/ 4df7c320-e98f-4417-9c31-9100fd63e2be?version=1.0 (visionato in data 10 giugno 2019). Disponibili dal mese di ottobre 2017, avrebbero dovuto essere adottate entro 60 giorni dall'entrata in vigore della legge Ferrara.

In merito a quanto direttamente concerne il cyberbullismo, si ritiene prioritario non solo rispettare *ex ante* l'età minima di iscrizione ai singoli social, ma anche osservare sempre più strettamente quanto disposto dal vigente art. 4, comma 5, legge Ferrara, che attribuisce alle istituzioni scolastiche di ogni ordine e grado il compito di promuovere "l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche".

Pur non essendo direttamente incidente sulla legge Ferrara, risulta di particolare interesse anche il disegno di legge S 1264[49]. All'art. 5, significativamente rubricato "Educazione alla cittadinanza digitale", prevede che nell'ambito dell'insegnamento trasversale dell'educazione civica, l'offerta formativa contempli "almeno le seguenti abilità e conoscenze digitali essenziali, da sviluppare con gradualità tenendo conto dell'età degli alunni e degli studenti":

"*f)* conoscere le politiche sulla tutela della riservatezza applicate dai servizi digitali relativamente all'uso dei dati personali; *g)* essere in grado di evitare, usando tecnologie digitali, rischi per la salute e minacce al proprio benessere fisico e psicologico; essere in grado di proteggere sé e gli altri da eventuali pericoli in ambienti digitali; essere consapevoli di come le tecnologie digitali possono influire sul benessere psicofisico e sull'inclusione sociale, con particolare attenzione ai comportamenti riconducibili al bullismo e al cyberbullismo"[50] .

In merito all'indagine conoscitiva su bullismo e cyberbullismo, essendo notoriamente ancora in corso presso la competente commissione parlamentare per l'infanzia e l'adolescenza[51], non è allo stato possibile effettuare un commento completo anche se, per quanto è possibile riscontrare, i riferimenti alla legge 71, siano essi positivi o negativi, non risultano significativamente presenti.

---

[49] Si tratta della proposta di legge C 682, recante "Istituzione dell'insegnamento dell'educazione civica nella scuola primaria e secondaria e del premio annuale per l'educazione civica" ed approvata in testo unificato con il nuovo titolo "Introduzione dell'insegnamento scolastico dell'educazione civica". I testi completi risultano attualmente disponibili ai seguenti URL: http:// documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.682.18PDL0014080.pdf e http://www.senato.it/service/PDF/ PDFServer/BGT/ 01108181.pdf (visionati in data 20 giugno 2019).

[50] Così l'art. 5, commi 1 e 2, del d.d.l.

[51] http://www.senato.it/leg/18/BGT/Schede/ProcANL/ProcANLscheda41201.htm (visionato in data 20 giugno 2019).

[52] Il rilievo dato all'aggettivo '*happy*' – le ragioni del cui utilizzo mantengono margini di opacità anche nell'ambito della letteratura psicologica: cfr. ELISA DONGHI, VERA PAGANI, FRANCESCA APPIANI, SIMONA CARAVITA (2018), *Bullismo online. Conoscere e contrastare il cyberbullismo,* Santarcangelo di Romagna, Apogeo Education - Maggioli, p. 136 – rischia di sfumare, in maniera indebita ed eccessiva, ogni significativo profilo di responsabilità, anche e soprattutto dal punto di vista giuridico. L'originaria – e più corretta – accezione di tale espressione è riportata anche in GIULIANA GUADAGNINI (2014), *Cyberbullismo e cyberstalking. Dinamiche comportamentali e stalkers*, in ANNA MARIA CASALE, PAOLO DE PASQUALI, MARIA SABINA LEMBO (a cura di), *Profili criminali e psicopatologici del reo,* Santarcangelo di Romagna, Maggioli, p. 223.

Attualmente, soprattutto nelle elencazioni sintetiche delle tipologie di cyberbullismo, risultano molto più sfumati i confini tra il *sexting* e il c.d. "*happy slapping*": nell'ambito di quest'ultimo, infatti, non emerge più il riferimento allo schiaffo e vengono sovente incluse anche condotte potenzialmente riconducibili, *de jure condendo*, all'art. 615 ter c.p.
A titolo esemplificativo, ELISA DONGHI, VERA PAGANI, FRANCESCA APPIANI, SIMONA CARAVITA (2018), *Bullismo online. Conoscere e contrastare il cyberbullismo*, op. cit., p. 115, lo (ri)definiscono come "pubblicazione o diffusione di immagini o video di una vittima tramite cellulare o smartphone".

Particolarmente interessante è il riferimento *de jure condendo* all'art. 612 ter c.p., considerato anche che "*sexting*" e "*happy*[52] *slapping*" costituiscono due delle principali forme di cyberbullismo indicate – seppur con alcune significative imprecisioni definitorie[53] e di natura operativa – dalla letteratura psicologica più accreditata[54].
Tale articolo può essere sinteticamente analizzato richiamando il disegno di legge di iniziativa governativa[55] n. S 1200, recante "Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere"[56] e denominato nella prassi comunicativa più recente come "Codice rosso"[57].

Tale disegno di legge, nel testo approvato in prima lettura dalla Camera mercoledì 3 aprile 2019 e trasmesso al Senato il successivo 8 aprile, è al momento in corso di esame al Senato, presso la seconda Commissione permanente (Giustizia) in sede redigente.
In questa sede è opportuno soffermarsi, in particolare, sull'art. 10, rubricato "Introduzione dell'articolo 612-ter del codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti".

L'art. 612 ter c.p., rubricato "Diffusione illecita di immagini o video sessualmente espliciti", dispone:

"salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000".

È opportuno sottolineare come, nel secondo comma, si specifichi che la medesima cornice edittale trovi applicazione anche nei confronti di coloro i quali hanno "ricevuto o comunque acquisito" gli stessi contenuti e, successivamente, li inviano, consegnano, cedono, pubblicano o diffondono "senza il consenso delle persone rappresentate al fine di recare loro nocumento".

Nel comma successivo sono previste ipotesi aggravate, che si configurano nei casi in cui i fatti siano commessi "dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa", così come – ipotesi tutt'altro che rara nell'ambito del c.d. *revenge porn* – "se i fatti sono commessi attraverso strumenti informatici o telematici".

Il comma 4 prevede aumenti di pena da un terzo alla metà qualora le immagini o i video sessualmente espliciti ed illecitamente diffusi riguardino persone "in condizione di inferiorità fisica o psichica" o gestanti.
Il delitto è punito a querela di parte – la quale, si noti, può essere proposta entro un termine di sei mesi – con remissione solo processuale.

---

53 Si veda *infra* quanto argomentato in merito al c.d. *revenge porn*.

54 Cfr. NANCY E. WILLARD (2007), *Cyberbullying and cyberthreats: responding to the challenge of online social cruelty, threats and distress*, Champaign, Research Press. L'"*happy slapping*" è stato aggiunto in seguito nel novero delle azioni comuni di cyberbullismo: cfr. ELISA DONGHI, VERA PAGANI, FRANCESCA APPIANI, SIMONA CARAVITA (2018), *Bullismo online. Conoscere e contrastare il cyberbullismo,* op. cit., pp. 114-115.

Si ritiene, tuttavia, che non tutte le fasi proprie delle due categorie di condotte alle quali si fa riferimento in questa nota debbano essere necessariamente considerate, *sic et simpliciter*, degli atti di cyberbullismo.

55 Ministro della giustizia, di concerto con Ministro dell'interno, Ministro della difesa, Ministro per la pubblica amministrazione, Ministro dell'economia e delle finanze: cfr. http://www.senato.it/service/PDF/PDFServer/BGT/01107220.pdf (visionato in data 10 giugno 2019).

56 Cfr. GIAN MARCO CALETTI (2019), *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie "esemplare", ma davvero efficace?,* in "Diritto Penale Contemporaneo", all'URL: https://www.penalecontemporaneo.it/d/6648-revenge-porn-prime-considerazioni-in-vista-dell-introduzione-dell-art-612-ter-cp-una-fattispecie-es (visionato in data 10 giugno 2019).

57 Cfr., *ex multis*: https://www.huffingtonpost.it/2019/04/03/via-libera-della-camera-al-codice-rosso-contro-la-violenza-sulle-donne-passa-al-senato-cosa-prevede-il-testo_a_23705778/ (visionato in data 10 giugno 2019).

Si prevede inoltre la procedibilità d'ufficio non solo nei casi di cui al comma quarto, bensì anche quando il fatto risulta essere connesso con un altro delitto procedibile d'ufficio.

Si tenga presente, sempre *de jure condendo*, che un caso simile alle condotte appena indicate[58], ed al contempo – fatte salve le responsabilità penali e civili – costituente un atto di cyberbullismo, risulta al centro della sentenza del Tribunale di Sulmona del 09 aprile 2018[59], che approfondisce in particolare i profili del danno non patrimoniale.

3. Per una lettura in ottica comparatistica

Già due anni fa, in occasione dell'entrata in vigore della legge Ferrara, ho ritenuto opportuno approfondire, in ottica comparatistica, se ordinamenti giuridici differenti da quello italiano avessero adottato una disciplina positiva del fenomeno complesso del cyberbullismo.
In tale occasione, ho avuto modo di riscontrare come tentativi di disciplinare il cyberbullismo fossero stati posti in essere da legislatori di altri ordinamenti, sia di common law sia di civil law, soffermandomi in particolare sulle discipline positive del fenomeno del cyberbullismo adottate in Colombia, Argentina, USA[60] (Connecticut, California, Florida, New Jersey, Texas, Arkansas, Missouri), Canada (British Columbia, Alberta, Ontario e Nova Scotia), Australia[61].

Da tale analisi iniziale – relativa ad alcune leggi in materia, tutte antecedenti alla normativa italiana del 2017 – è emerso come talora siano anche significativamente differenti le accezioni di cyberbullismo rinvenibili nelle differenti normative nazionali.
A mero titolo esemplificativo, la legge argentina 15 dicembre 2016, n. 5775 – ley para la prevención del ciberacoso sexual a menores (grooming) – contempla non solo il cyberbullismo tra minorenni, ma anche condotte che, esulando del tutto dalla definizione di cui all'art. 1, comma 2, l. 71/2017, ricordano molto da vicino la fattispecie delittuosa di cui all'art. 609-undecies del Codice penale italiano.

Si pensi, inoltre, agli ordinamenti che considerano espressamente il cyberbullismo come fenomeno fisiologicamente riscontrabile anche tra adulti[62].

---

[58] Una ragazza, che ha incautamente ceduto a conoscenti, tra cui un maggiorenne, proprie immagini osé (condotta tipica del c.d. *sexting*), ha ritrovato la medesima immagine diffusa on line, in un profilo fake: sia sufficiente notare, in questa sede, le affinità con il c.d. *revenge porn* e, *de jure condendo,* soprattutto, con l'art. 612 ter, comma 2, c.p., in quanto uno tra i destinatari, dopo aver "ricevuto" tali immagini, le ha evidentemente pubblicate e diffuse in assenza del consenso della persona rappresentata, arrecando un nocumento che il Tribunale ha ritenuto ascrivibile alla categoria dei danni non patrimoniali e ha riconosciuto come sussistente in capo non solo alla minore, ma anche ai di lei genitori: cfr. nota seguente.

[59] Con nota di GIUSEPPE CASSANO, CORRADO MARVASI (2018), *La responsabilità educativa dei genitori per minori cyberbulli*, in "Danno e Responsabilità", 6, 2018, pp. 763 ss.

[60] È interessante consigliare in questa sede la lettura del seguente paper: JEFF KOSSEFF (2019), *Cybersecurity of the Person*, in "First Amendment Law Review", 17, 2019, in particolare pp. 350-351, ove si illustra un caso di applicazione a livello giurisprudenziale della normativa vigente in North Carolina sul cyberbullismo.

[61] RICCARDO M. COLANGELO (2017), *La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche*, op. cit. in particolare pp. 414-417.
Per cenni in merito alla disciplina del cyberbullismo in Australia, Nuova Zelanda, Filippine e Singapore si veda anche RAJNESH SINGH (2018), *Mapping Online Child Safety in Asia and the Pacific*, in "Asia & the Pacific Policy Studies", 3, vol. 5, p. 660.

[62] A mero titolo esemplificativo si veda COLETTE LANGOS, MARK GIANCASPRO (2017), *Empowering Workers: Avenues of Legal Redress for Victims of Workplace Cyberbullying*, in "Australian Business Law Review", vol. 45, n. 6, pp. 448-466.

In questa sede, considerato il lasso di tempo intercorso dall'entrata in vigore della legge Ferrara, ho ritenuto opportuno impostare una rinnovata analisi comparatistica, indirizzata in particolare alle normative straniere sul cyberbullismo cronologicamente successive a quella italiana.

Utili spunti in tal senso, senza pretesa di esaustività, emergono in modo particolare dalla normativa texana nota come "David's Law"[63], entrata in vigore il 1° settembre 2017 ed espressamente dedicata a David Molak, un sedicenne vittima di cyberbullismo[64].
Mediante tale legge, che si riferisce al bullismo ed al cyberbullismo in ambito scolastico, risulta novellato l'*Education Code*. Più nello specifico, con una tecnica normativa differente rispetto a quella della legge 71, il legislatore texano ha stabilito che debba intendersi per cyberbullismo:

"*bullying that is done through the use of any electronic communication device, including through the use of a cellular or other type of telephone, a computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an Internet website, or any other Internet-based communication tool*"[65].

Particolarmente interessante, in tale normativa pensata – come quella italiana – per l'ambito scolastico, è l'esplicita precisazione in base alla quale essa trova applicazione anche in relazione agli atti di cyberbullismo commessi al di fuori degli edifici scolastici e delle relative pertinenze. Si tratta di un punto molto rilevante anche nell'ambito scolastico italiano, che non può non essere preso adeguatamente in considerazione, soprattutto da quanti operano nel mondo della scuola.

In argomento, la normativa texana specifica che la sezione "a-1" trova applicazione anche in relazione a:

"*cyberbullying that occurs off school property or outside of a school-sponsored or school-related activity if the cyberbullying: (A) interferes with a student's educational opportunities; or*
(B) substantially disrupts the orderly operation of a classroom, school, or school-sponsored or school-related activity"[66].

È possibile affermare che sostanzialmente, nell'ambito degli USA, ogni Stato ha ormai adottato una espressa disciplina del fenomeno del cyberbullismo. È questo il caso, tra i più recenti, del Texas, dell'Indiana[67]

---

[63] Il testo integrale è disponibile al seguente URL: https://locker.txssc.txstate.edu/3942be0c6bbe569ed1417377e6c1d2a9/SB-179.pdf (consultato in data 20 giugno 2019)

[64] Cfr. https://www.davidslegacy.org/davids-story/ (consultato in data 20 giugno 2019). Si noti come, similmente a quanto *de facto* avvenuto per la legge 71, anche la normativa texana trae ispirazione da un caso di cyberbullismo tristemente sfociato in suicidio.

[65] https://locker.txssc.txstate.edu/3942be0c6bbe569ed1417377e6c1d2a9/SB-179.pdf (consultato in data 20 giugno 2019)

[66] https://locker.txssc.txstate.edu/3942be0c6bbe569ed1417377e6c1d2a9/SB-179.pdf (consultato in data 20 giugno 2019). *Simili modo*, viene riconosciuta la rilevanza del cyberbullismo "off campus" in JOSHUA RIEGER (2018), *Digitizing the Schoolhouse Gate: Protecting Students' Off-Campus Cyberspeech by Switching the Safety on Tinker's Trigger*, in "Florida Law Review", 70, 2018, pp. 695-737. Più nello specifico, a p. 695 si afferma che "*states should enact laws prohibiting school officials from punishing students for off-campus cyberspeech, except when that speech constitutes a true threat to the school community or is adjudicated as unlawful, as in cases of cyberbullying, harassment, or defamation*".
L'autore tratteggia altresì alcune interessanti questioni a livello federale e giurisprudenziale.

[67] House Bill 1356/2018.

ove il legislatore ha inteso novellare l'*Indiana Code concerning education*[68] – e del Michigan. In tale ultimo Stato, il legislatore ha scelto di prediligere il ricorso alle sanzioni penalistiche, svincolando al contempo il cyberbullismo dall'ambito giovanile e scolastico[69].

Fatto salvo quanto sopra illustrato in merito alle differenti accezioni di cyberbullismo fatte proprie dai vari legislatori nazionali, l'approccio chiaramente educativo al fenomeno del cyberbullismo, fatto proprio dal legislatore italiano nell'ambito della normativa in materia, si contrappone a quello spiccatamente sanzionatorio, che annovera già da tempo sostenitori anche oltreoceano[70].

Sul punto, anche nella dottrina americana più recente è possibile riscontrare osservazioni critiche relativamente alla generalizzazione di un approccio sanzionatorio particolarmente severo. È questo il caso, ad esempio, della normativa vigente in Texas, in ordine alla quale la dottrina, riconoscendo il valore di un approccio maggiormente (ri)educativo, ha affermato che "*while criminalization may be appropriate in some instances, it is certainly not the answer for every student"*[71].

Nell'ambito degli Stati Uniti, inoltre, rimane vivo il dibattito dottrinale in merito a possibili limitazioni al primo emendamento, correlate alle normative sul cyberbullismo[72]; in argomento, non si dimentichi che anche durante l'iter di approvazione della legge Ferrara, a partire da quando la Camera stravolse il testo base, includendo anche la disciplina del bullismo e contemplando la configurabilità di atti di bullismo o cyberbullismo tra soggetti adulti, la dottrina italiana più attenta ebbe a criticare potenziali derive censorie[73].

In molti tra gli stati che ancora sono privi di una espressa disciplina in materia, come ad esempio la Nigeria, la dottrina auspica l'interesse del legislatore[74].

---

68 Tale Codice non disciplina espressamente il fenomeno del cyberbullismo, tuttavia, tra le condotte costituenti bullismo, il legislatore dell'Indiana considera anche "*verbal or written communications or images transmitted in any manner (including digitally or electronically*)": cfr. Chapter 8. ("Student Discipline"), Section 0.2.

69 Cfr. Enrolled House Bill No. 5017/2018, entrata in vigore il 27 marzo 2019, che introduce nel Codice penale del Michigan la Sezione 411x., ove le nuove fattispecie sono introdotte dalla seguente precisazione: "*A person shall not cyberbully another person*".

70 A mero titolo esemplificativo, si veda: S.W. BRENNER, M. REHBERG (2009), *Kiddie Crime – The Utility of Criminal Law in Controlling Cyberbullying*, in "First Amendment Law Review", 8, 2009, pp. 1-85.

71 Così KATHERINE MALLON (2019), *The Bully Left Behind: Why David's Law Perpetuates the School-To-Prison Pipeline and is Inadequate to Serve the Needs of Texas Schools*, p. 2. Testo disponibile all'URL http://dx.doi.org/10.2139/ssrn.3327534 (consultato in data 20 giugno 2019).

72 A titolo esemplificativo, in relazione ad un campione di soggetti adulti e senza espressi riferimenti al cyberbullismo in ambito scolastico, si veda: JONATHON W. PENNEY (2017), *Can Cyber Harassment Laws Encourage Online Speech?*, in AA.VV., *Perspectives on Harmful Speech Online*, the Berkman Klein Center for Internet & Society at Harvard University, pp. 10-12, disponibile on line all'URL: http://dx.doi.org/10.2139/ssrn.3147336 (consultato in data 20 giugno 2019).

73 Cfr. GIOVANNI ZICCARDI, *La soluzione c'è: si chiama censura*, in "Il Mulino", 2, 2017, pp. 226-234.
Faccio riferimento al testo approvato dalla Camera, con modificazioni, in data 20 settembre 2016, in ordine al quale rinvio alle osservazioni critiche che ho già avuto modo di esporre nell'ambito dell'Internet Festival di Pisa dell'ottobre 2016, successivamente pubblicate in RICCARDO M. COLANGELO (2017), *Cyberbullismo e responsabilità: Internet è veramente un mondo virtuale?*, op. cit., pp. 189-202.

74 Riscontrando la diffusione di atti di cyberbullismo in ambito scolastico e comunque tra i più giovani, nonché riconoscendo la necessità di precise politiche educative, preventive e di sensibilizzazione, KINGSLEY CHINAZA NWOSU , CHRISTIANA NGOZI EMENTA, PERPETUAL EBERECHI EJIKEME (2018), *Cyberbullying among undergraduate students in a Nigerian University: awareness and incidence*, in "Romanian Journal Of Psychological Studies", p. 55, affermano espressamente: "government should enforce laws/ edicts on cyberbullying".

4. Conclusioni

Lo sguardo comparatistico – che in questa sede è stato possibile solamente accennare, ma che meriterebbe ulteriori e più ampi approfondimenti – mette in luce non solo i punti di contatto, ma anche – e forse soprattutto – le fisiologiche differenze intercorrenti tra gli ordinamenti giuridici[75].
Questo – come si è visto – è chiaro in materia di cyberbullismo, laddove le varie normative nazionali risultano discordanti addirittura in merito alla definizione ed ai confini di questo fenomeno complesso.

Occorre non sottovalutare, tuttavia, profili di incertezza e di incoerenza in ordine al (bullismo ed al) cyberbullismo, riscontrabili non solo – *de jure condendo* – internamente all'ordinamento giuridico italiano, ma anche nell'ambito del contesto sociale.
Ciò, in prima approssimazione, può attualmente ritenersi correlato ad una scarsa conoscenza della normativa sul cyberbullismo ma, più in generale ed anche prima dell'entrata in vigore della medesima, anche a competenze talora approssimative in ordine alle caratteristiche fondamentali del fenomeno complesso. Quest'ultimo, inoltre, non può essere adeguatamente considerato prescindendo dalle plurime ed articolate implicazioni di natura informatico-giuridica.

---

[75] Cfr., *ex multis*, GIANMARIA AJANI, DOMENICO FRANCAVILLA, BARBARA PASA (2018), *Diritto comparato. Lezioni e materiali*, Torino, Giappichelli, in particolare p. 8.

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

SPONSORED BY

ASSOCIAZIONE AVVOCATI TORINO GIOVANI

POLIEDRICITÀ NORMATIVA DEL BITCOIN

DI ALESSANDRA GIULIA NASTRI

1.Nozioni introduttive-2. Breve analisi condotta alla luce del GDPR-3. Cenni riguardanti la Normativa antiriciclaggio-4. La questione tributaria-5. Conclusioni.

1.Nozioni introduttive

E' necessario partire da una considerazione basilare, che spesso causa confusione nel pubblico: non bisogna assimilare il concetto di *Bitcoin* a quello di *Blockchain*. Infatti, cercando di semplificare il più possibile le due nozioni, è possibile considerare che il *Bitcoin* sia la valuta virtuale che si serve ed è introdotta in un panorama più ampio: quello della tecnologia della *Blockchain*.

Il decreto legislativo 90/2017 fornisce una definizione di valuta virtuale che può essere considerata un ottimo punto di partenza, al fine di delineare una disciplina giuridica applicabile al celebre *Bitcoin*.

Si considera valuta virtuale una rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata ad una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente. Il *Bitcoin* è la cripto valuta comunemente più nota al grande pubblico e le sue caratteristiche principali ed il funzionamento sono comuni a quelle meno conosciute quali, ad esempio, *Ethereum, Monero* e *Ripple*.

Analizzando le caratteristiche che accomunano le cripto valute, quella più importante è senz'altro l'incorporeità data dalla rappresentazione digitale e dall'assenza del carattere monetario. Sicuramente questa prerogativa trova la sua origine principalmente nel fatto che le cripto valute non vengano emesse da una banca centrale o da un'autorità pubblica e proprio il *Bitcoin* introduce la possibilità di trasferire un'unità economica *peer to peer,* non richiedendo l'intervento di terze parti.[12] E' proprio il fatto che sia uno scambio *peer to peer* , a rendere le parti equivalenti.

L'elemento più innovativo del fenomeno è proprio lo scambio di valute senza l'intermediazione di altri soggetti.

L'inventore del *Bitcoin*, Satyoshi Nakamoto, nel suo paper *Bitcoin: un sistema di moneta elettronica peer-to-peer* , annovera tra i vantaggi dell'utilizzo di questa cripto valuta proprio l'eliminazione dei costi di transazione derivanti dall'intervento di un mediatore garante del pagamento. Secondo Nakamoto infatti, è proprio il costo della transazione a scoraggiare l'utilizzo dei pagamenti elettronici per piccoli importi. Il *Bitcoin* ovvia a questo problema utilizzando la tecnologia della *blockchain* e rendendo la valuta elettronica una vera e propria catena di firme digitali[3] tramite una combinazione di crittografia e informatica.

---

1 Vincenzo DE STASIO, *Verso un conce*o europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento,* in *Banca Borsa Titoli di Credito*, 1 dicembre 2018, pag. 747.

2 Massimo GIULIANO, *La Blockchain e gli smart contracts nell'innovazione del diri*o nel terzo millennio,* in *Diri*o dell'Informazione e dell'InformaAca (II), 1 dicembre 2018,* pag.989.

Tuttavia, la mancanza di un'autorità garante dell'autenticità pagamenti, creerebbe un modello di scambio basato meramente sulla fiducia e di conseguenza una tutela certamente insufficiente per gli utilizzatori e la soluzione al problema, su cui si basa il circuito del *Bitcoin*, è la tracciatura indelebile di ogni transazione avvenuta.

E' chiaro che in un sistema del genere, apparentemente autonomo, dotato di un enorme potenziale economico, dato anche dal fatto che il *Bitcoin* è la criptovaluta più scambiata al mondo[4], si rende comunque necessario l'intervento del legislatore al fine di tutelare gli utenti e di evitare l'impiego di questo strumento per fini illeciti. Gli approcci diffidenti al fenomeno sono dati proprio dal fatto che il *Bitcoin*, è stata la cripto valuta più utilizzata dal dark web per il contrabbando. Una delle principali questioni, rimaste ancora ad oggi irrisolte, è il fatto che non sia possibile conoscere con certezza assoluta l'identità della persona che compie la transazione. Infatti, nonostante le transazioni siano note alle parti e gli utenti siano identificabili da una chiave, quest'ultima informazione non consente di avere la certezza della riferibilità ad uno specifico soggetto.[5]

Ad oggi, si può dire che vi sia ancora una parvenza di incertezza normativa per quanto riguarda il *Bitcoin* e le cripto valute in generale ma, è interessante analizzare l'interazione del fenomeno con tre ambiti giuridici quali il GDPR, la normativa antiriciclaggio e il diritto tributario.

2. Breve analisi condotta alla luce del GDPR

Molti sono stati i dubbi sollevati in dottrina circa la compatibilità della tecnologia *blockchain* ed il nuovo regolamento sulla Privacy.[6]

Il punto di partenza fattuale, su cui ormai non vi sono più dubbi, è che i dati inseriti dagli utenti relativi alle transazioni sono considerati dai personali di cui all'art.4 del GDPR.

Proprio al fine di condurre un'analisi alla luce del regolamento UE 2016/679 è necessario fare una distinzione tra due tipologie di *blockchain* possibili, quella *permissioned* e quella *permissionless*.

---

[3] Satoshi NAKAMOTO*, Bitcoin:un sistema di moneta ele*ronica peer-to-peer*, disponibile su www.bitcoin.org.

[4] Fulvio SARANZANA DI S. IPPOLITO, Massimiliano NICOTRA, *Diri*o della blockchain, intelligenza arAficiale e IoT*, IPSOA, Vicenza, 2018.

[5] Massimo GIULIANO, *La Blockchain e gli smart contracts nell'innovazione del diri*o nel terzo millennio,* in *Diri*o dell'Informazione e dell'InformaAca (II),* 1 dicembre 2018, pag.989.

[6] Sul punto, tra altri, Michèle FINCK, *Blockchains and Data ProtecAon in the European Union*, disponibile su hSps://edpl.lexxion.eu/arWcle/edpl/2018/1/6, 2018: "*We will observe that at least at first sight blockchains (especially those that are public and un-permissioned) and the GDPR are profoundly incompaAble at a conceptual level as the data protecAon mechanisms developed for centralized data silos cannot be easily reconciled with a decentralized method of data storage and protecAon. Even where data is encrypted or hashed it qualifies as personal data under EU law."*

Nel caso in cui si sia in presenza di una *blockchain* chiusa o *permissioned,* ed è una singola persona fisica o giuridica a voler prenderne parte, è il partecipante stesso ad esprimere il consenso al trattamento dei dati che saranno pubblici alle altre parti della transazione. E' in questo caso che si configurerebbe l'ipotesi prevista dall'art.26 del GDPR ossia la contitolarità del trattamento.[7] Ai sensi dell'articolo 26, i contitolari del trattamento determinano congiuntamente la responsabilità derivante dall'osservanza degli obblighi del regolamento e, con il medesimo accordo, ne definiscono i rispettivi ruoli per l'adempimento degli obblighi derivanti dal GDPR. Anche nel caso in cui sia un consorzio ad offrire agli utenti finali il servizio e registri i dati sulla *blockchain* chiusa, i contitolari del trattamento si individuano nei partecipanti al consorzio.[8]

E' chiaro che i responsabili per l'adempimento degli obblighi previsti dal regolamento dovranno occuparsi sia di un'analisi preventiva sulla qualità dei dati personali raccolti, sulla tipologia di *blockchain* utilizzata, sul trattamento e su tutto ciò che verte le modalità di acquisizione dei dati.

Quando invece si è in presenza di una *blockchain permissionless*, se è il singolo ad effettuare delle transazioni, risulta difficile individuare un unico titolare del trattamento, trasferendo la responsabilità direttamente in capo all'utente. Se invece l'utente interagisce con un'applicazione che utilizza la *blockchain permissionless*, allora saranno i gestori dell'applicazione stessa i titolari del trattamento. [9] Chiaro è che la *blockchain* aperta costituisce un contesto fortemente decentralizzato, dove risulta difficile individuare con precisione i soggetti responsabili del trattamento dei dati.

Un'incompatibilità significativa tra la tecnologia *blockchain* e il GDPR è l'indelebilità dei dati inseriti. Infatti, ai sensi dell'art.5 del regolamento sui principi applicabili al trattamento dei dati personali, "devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati".[10]

Inoltre il fatto che i dati inseriti non possano essere cancellati contrasta anche con il diritto all'oblio. Infatti, una delle caratteristiche della *blockchain,* è che i dati immessi diventano automaticamente pubblici a tutti i partecipanti alla transazione e vengono conservati illimitatamente.[11]

---

7 Fulvio SARANZANA DI S. IPPOLITO, Massimiliano NICOTRA, *Diri*o della blockchain, intelligenza arAficiale e IoT*, IPSOA, Vicenza, 2018, pag.76.

8 Sul punto, è uWle precisare che la tesi che individua i Wtolari del traSamento nei partecipanW al consorzio non è da tuZ condivisa. Tra gli altri, Michèle FINCK, *Blockchains and Data ProtecAon in the European Union*, hSps:// edpl.lexxion.eu/ arWcle/edpl/2018/1/6, 2018: "*Nodes do not, in principle, qualify as joint controllers under ArAcle 26(I) GDPR as the do 'jointly determine the purposes and means of processing'. This requires a clear and transparent allocaAon of responsibiliAes."*

9 Fulvio SARANZANA DI S. IPPOLITO, Massimiliano NICOTRA, *Diri*o della blockchain, intelligenza arAficiale e IoT*, IPSOA, Vicenza, 2018,pag.79-80.

10 Art.5 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.
11 NicoleSa BOLDRINI, *Blockchain e GDPR: le sfide (e le opportunità) per la protezione* dei daW, disponibile su

hSps://www.blockchain4innovaWon.it/sicurezza/blockchain-gdpr/, 9 luglio 2018.

Circa l’anonimato dei dati inseriti, è intervenuto il Gruppo di Lavoro per la tutela dei dati istituito in virtù dell'articolo 29 della direttiva 95/46/CE. Nonostante i dati degli utenti siano espressi in cifre, non possono essere considerati anonimi poiché sono collegabili ad un’identità determinata. E’ proprio riguardo alla questione dell’identità che risulta necessario fare almeno accennare ad un’altra problematica, che si presenta nelle operazioni in rete. Infatti, ad oggi, la tecnologia di internet non ci permette ancora di conoscere con certezza l’individuo che effettivamente utilizza una certa firma digitale o una certa chiave nel caso del *Bitcoin*.[12]

3. Cenni riguardanti la Normativa antiriciclaggio

La presa di coscienza dei rischi derivanti dall’utilizzo dell’anonimato (o pseudo anonimato) nel campo delle valute virtuali è ben esplicitata dal nono considerando della direttiva UE 2018/843.[13]

Dal punto di vista normativo, per la disciplina del fenomeno, è molto attinente e rilevante anche il decreto legislativo n.90/2017. Tale decreto infatti, ha approfondito ed introdotto nuove disposizioni riguardanti proprio la disciplina delle cripto valute oltre ad introdurre la predetta definizione di valuta virtuale[14]. Chiaro è la maggior parte dei rischi di uso illecito della cripto valuta è causata dall’anonimato virtuale con cui vengono effettuate le transazioni. [15] Infatti, anche se la tecnologia *blockchain* è uno strumento più che valido per la tracciabilità delle transazioni, spesso risulta difficile, a causa della complessità dell’algoritmo, risalire ad una persona fisica o giuridica determinata, senza tener conto degli *escamotage* che permettono di oscurare l’origine della transazione.[16]

---

[12] “*On the Internet, nobody knows you’re dog*”: è una frase molto rappresentativa del problema, tratta da una vignetta pubblicata sulla rivista *The New Yorker,* 5 luglio 1993, disegnata da Peter Steiner.

[13] “L’anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L’inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell’anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell’ambiente delle valute virtuali rimarrà caratterizzato dall’anonimato. Per contrastare i rischi legati all’anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all’identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un’autodichiarazione alle autorità designate.”

[14] v.par.1.

[15] Seppur non così considerato dal parere del Gruppo di Lavoro per la tutela dei dati istituito in virtù dell'articolo 29 della direttiva 95/46/CE.

[16] Ludovica STURZO, *BITCOIN E RICICLAGGIO 2.0*, disponibile su https://www.penalecontemporaneo.it/upload/6225-sturzo2018a.pdf, maggio 2018.

[17] Roberto BOCCHINI, *LO SVILUPPO DELLA MONETA VIRTUALE: PRIMI TENTATIVI DI INQUADRAMENTO E DISCIPLINA TRA PROSPETTIVE ECONOMICHE E GIURIDICHE*, in *Diritto dell’informazione e dell’Informatica*, 1 febbraio 2017, pag.27.

L’ampia categoria di soggetti a cui si rivolgono gli obblighi previsti dal decreto legislativo 231/2007 è costituita dai prestatori di servizi relativi all’utilizzo di valuta virtuale. Tali soggetti sono identificati dal dall’art.1 comma 2, f), del decreto come “ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all’utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale”. Infatti, l’art.17-bis del decreto legislativo 141/2010, relativo ai contratti di credito ai consumatori, subordina l'esercizio professionale nei confronti del pubblico dell’attività di cambiavalute, anche su base stagionale, consistente nella negoziazione a pronti di mezzi di pagamento in valuta, all’iscrizione in un apposito registro, introducendo quindi un nuovo strumento di controllo.[18]

Circa la professionalità dell’attività degli *exchangers* si è espresso anche il Tribunale di Verona, con sentenza n.195/2017, statuendo che l’operazione di cambio valuta tradizionale contro unità della valuta virtuale *Bitcoin* e viceversa, effettuate a fronte del pagamento di un corrispettivo, è qualificabile come attività professionale di prestazioni di servizi a titolo oneroso svolta in favore di consumatori.

L’iscrizione al registro presuppone il requisito della liceità dell’attività e lo stesso art.17-bis, al quinto comma, statuisce che l'esercizio abusivo dell’attività di cui al comma 1 è punita con una sanzione amministrativa da 2.065 euro a 10.329 euro emanata dal Ministero dell'economia e delle finanze. I medesimi soggetti saranno inoltre assoggettati agli obblighi di adeguata verifica, conservazione dei dati e comunicazione di operazioni sospette già previsti dal d.lgs.231/2007. E’ rilevante sottolineare che a livello sostanziale i prestatori di servizi relativi all’utilizzo di valuta virtuale siano gli unici soggetti aventi la possibilità di venire a conoscenza della vera identità dell’utente Bitcoin prima che questi diventi una chiave numerica difficilmente individuabile.

Tuttavia, sotto questo aspetto, il decreto legislativo 90/2017 non ha creato efficacemente un vero e proprio dovere di controllo in capo agli *exchangers*.[19]

La seconda categoria di soggetti a cui si rivolge la V normativa antiriciclaggio[20] sono i *wallet providers* cioè coloro che forniscono “*servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*” che si sostanzia in un servizio di deposito, dietro corrispettivo, delle cripto valute. Tuttavia, anche in questo caso la normativa antiriciclaggio rivela avere un’efficacia relativa poiché la fruizione del servizio di deposito è meramente a discrezione dell’utente.

---

[18] Giovanni Paolo ACCINI, *Regole anAriciclaggio e risvolA penalisAci dell’operaAvità in valute virtuali,* in *Rivista delle Società*, 1 dicembre 2018, pag.1516.

[19] Ludovica STURZO, *BITCOIN E RICICLAGGIO 2.0*, disponibile su hSps://www.penalecontemporaneo.it/upload/6225-sturzo2018a.pdf, maggio 2018.

[20] Inizialmente la V normaWva anWriciclaggio era rivolta solo agli *exchangers*, ma con l’approvazione del quinto emendamento da parte del Parlamento europeo, gli obblighi sono staW estesi anche ai *wallet providers*.

4. La questione tributaria

Il 22 ottobre 2015, con sentenza numero 264, la Corte di giustizia dell'Unione Europea, pronunciandosi su una controversia svedese ed interpretando la direttiva 2006/112, ha statuito che le operazioni di cambio di valuta tradizionale in *Bitcoin* e viceversa sono esenti dall'imposta sul valore aggiunto. La decisione della Corte è condivisibile poiché essendo il *bitcoin* qualificato come una moneta vera e propria, risulta opportuno continuare a scindere l'imposta sul reddito da quella sui consumi.

E' comunque rilevante sottolineare che il quadro normativo circa gli obblighi fiscali sulle cripto valute è ancora molto incerto.

5. Conclusioni

L'importanza del fenomeno, sia per i risvolti giuridici che per quelli economici, è innegabile e gli interventi normativi, forse per una generale sottovalutazione, risultano ad oggi insufficienti.

Anche circa la qualificazione del *Bitcoin* come moneta vi sono orientamenti contrastanti. Infatti, se da un lato a fini fiscali è considerato come un reddito, ed in alcuni casi come a Zugo, cantone svizzero, è assimilato ad una moneta vera e propria tanto da poterlo acquistare tramite comuni ATM e pagare le tasse in *Bitcoin*[21], dall'altro non sembra condividere lo stesso orientamento il Tribunale di Brescia che ha escluso, con la sentenza n.7556/2018 riconfermata in seguito dalla Corte d'Appello, la possibilità apportare conferimenti in società in cripto valute poiché considerate inidonee ad essere oggetto di valutazione in un dato momento storico e ad essere aggredibili dai creditori sociali.[22] Certo è che una tale valutazione è in netta contrapposizione con la prassi che invece considera, sempre di più, la cripto moneta come una vera e propria valuta.

Inoltre, circa l'aggredibilità da parte dei creditori sociali, rimane comunque la possibilità per gli amministratori di convertire, in ogni momento, gli eventuali conferimenti dalla cripto valuta all'euro. In realtà, la Corte di Appello di Brescia ammette la qualificazione monetaria della cripto valuta considerandola tuttavia inidonea a costituire oggetto di conferimento.

Sull'insufficiente intervento del legislatore c'è da dire che la mobilità e l'immediatezza della tecnologia *blockchain* rende difficoltoso cristallizzarne una disciplina.

In un panorama così nebuloso, le reazioni degli stati sono state diverse.

La Cina ha adottato delle misure discutibili circa il rispetto della privacy. Infatti, dal 15 febbraio 2019 è entrato in vigore il Cyberspace Administration of China che impone l'accesso delle autorità statali ai dati conservati su *blockchain*, la registrazione delle attività degli utenti e il mantenimento di *backup* per almeno sei mesi. [23]

---

[21] Mario PASSARETTA, *Bitcoin: il leading case italiano*, in *Banca Borsa Titoli di Credito*, 2017, pag.471. [22] Massimo RUBINO DE RITIS, *ApporA di criptomonete in società, GiusAziaCivile.com*, 19 marzo 2019.

[23] Massimiliano NICOTRA, *Le norme su Bitcoin e cri*ovalute nei diversi Paesi: il quadro*, disponibile su hSps://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-criSovalute-nei-diversi-paesi-quadro/2 marzo 2018.

Certo è che in uno scenario europeo, misure simili non potrebbero mai essere adottate tuttavia, ci si aspetta una maggior ingerenza del legislatore per tutelare gli utenti.

Il Giappone invece, dal 2017, ha dichiarato le cripto valute forme legali di pagamento.

Un'ulteriore riflessione deve essere fatta anche riguardo alla persona fisica, non informata, che decide di investire sul *Bitcoin*. Non sono ancora previsti infatti degli obblighi di informazione verso il consumatore in questo campo, nonostante la compravendita di valute virtuali possa essere considerata un'operazione ad alto rischio per il risparmiatore. [24] A tal proposito, anche la Banca Centrale Europea, tramite un comunicato del 13 febbraio del 2018, ha tentato di mettere in guardia l'investitore sulla pericolosità del *Bitcoin*, pur tuttavia sostenendo che non rientrasse nella sua competenza la regolamentazione della materia.[25]

Inoltre, anche l'attività dei *wallet providers*, dovrebbe essere regolamentata non solo sotto il profilo dell'antiriciclaggio ma anche circa la funzione di deposito.

Molte sono ancora le incertezze normative e di difficile risoluzione. Si auspica quindi una futura regolamentazione efficace ma che non comprometta, a causa di un'ingerenza eccessiva, l'anima liberale alla base del funzionamento delle cripto valute e di internet in generale.

---

[24] Conforme Trib. Verona n.195/2017: "La compravendita di valute virtuali (ad es. di *Bitcoin*), qualificabili alla stregua degli strumenW finanziari, è un'operazione definibile ad alto rischio per il risparmiatore, il che obbliga colui il quale ne pubblicizzi la vendita, in proprio o per conto terzi, ad informare preliminarmente l'utente interessato all'acquisto sui rischi connessi all'invesWmento (c.d. informaWva precontraSuale), così come stabilito dagli arS. 67 e ss. del codice del consumo in tema di commercializzazione a distanza di servizi finanziari ai consumatori; in parWcolar modo, il promotore dell'operazione di vendita è tenuto all'applicazione delle disposizioni più rigorose previste dalla normaWva di seSore che disciplina l'offerta del servizio o del prodoSo interessato", massima traSa da www.dejure.it. Il caso specifico si riferisce all'ipotesi in cui vi sia un soggeSo che pubblicizzi le operazioni. TuSavia, una prerogaWva del *Bitcoin* è proprio il faSo che il consumatore possa effeSuare transazioni senza l'intervento di un intermediario.

[25] *What is a Bitcoin?*, disponibile su hSps://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html, 18 febbraio 2018.

BIBLIOGRAFIA

ACCINI Giovanni Paolo, *Regole antiriciclaggio e risvolti penalistici dell'operatività in valute virtuali*, in *Rivista delle Società*, 1 dicembre 2018.

BOCCHINI Roberto, *LO SVILUPPO DELLA MONETA VIRTUALE: PRIMI TENTATIVI DI INQUADRAMENTO E DISCIPLINA TRA PROSPETTIVE ECONOMICHE E GIURIDICHE*, in *Diritto dell'informazione e dell'Informatica*, 1 febbraio 2017.

BOLDRINI Nicoletta, *Blockchain e GDPR: le sfide (e le opportunità) per la protezione* dei dati, disponibile su https://www.blockchain4innovation.it/sicurezza/blockchain-gdpr/, 9 luglio 2018.

DE STASIO Vincenzo, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca Borsa Titoli di Credito*, 1 dicembre 2018.

FINCK Michèle, *Blockchains and Data Protection in the European Union*, disponibile su https://edpl.lexxion.eu/article/edpl/2018/1/6, 2018.

GIULIANO Massimo, *La Blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Diritto dell'Informazione e dell'Informatica (II),* 1 dicembre 2018.

NAKAMOTO Satoshi, *Bitcoin: un sistema di moneta elettronica peer-to-peer*, disponibile su www.bitcoin.org.

NICOTRA Massimiliano e SARANZANA DI S. IPPOLITO Fulvio, *Diritto della blockchain, intelligenza artificiale e IoT*, IPSOA, Vicenza, 2018.

NICOTRA Massimiliano, *Le norme su Bitcoin e crittovalute nei diversi Paesi: il quadro*, , disponibile su https://www.agendadigitale.eu/sicurezza/le-norme-bitcoin-crittovalute-nei-diversi- paesi-quadro/, 2 marzo 2018.

PASSARETTA Mario, *Bitcoin: il leading case italiano*, in *Banca Borsa Titoli di Credito*, 2017.

RUBINO DE RITIS Massimo, *Apporti di criptomonete in società*, *GiustiziaCivile.com*, 19 marzo 2019.

STURZO Ludovica, *BITCOIN E RICICLAGGIO 2.0*, disponibile su https://www.penalecontemporaneo.it/upload/6225-sturzo2018a.pdf, maggio 2018.

CALL FOR PAPERS

INNOVAZIONE TECNOLOGICA NUOVE PROSPETTIVE PER L'INDAGINE GIURIDICA E PER LA PROFESSIONE FORENSE

RISOLUZIONI
QUESTIONI
GIURIDICHE
IMPATTO
VITA
FRODI
INFORMATICHE
INTELLIGENZA ARTIFICIALE
AGAT
CRIPTOVALUTE
BIOTECNOLOGIE
BLOCKCHAIN
STRUMENTI TECNOLOGICI
ETICA E DIRITTO
DUE DILIGENCE
ROBOTICA
BIG DATA
PROCEDURA CIVILE
FRODI INFORMATICHE
NUOVE TECNOLOGIE
ETICA E DIRITTO
LEGAL DESIGN
FURTO DI IMMAGINI
INTERNET DELLE COSE
SOCIAL MEDIA
PROVE DIGITALI
IMPATTO VITA
OPERE MULTIMEDIALI
COPYRIGHT
INTERNET DELLE COSE
PROCEDURA PENALE
CYBERSECURITY
INTELLIGENZA ARTIFICIALE
SMART CONTRACT
ROBOTICA DUE DILIGENCE
PROCEDURA CIVILE
ROBOTICA
PHISHING
E-PRIVACY
IP
PROVA
RICERCA
SERVICE PROVIDER
CRIPTOVALUTE
FURTO DI IMMAGINI
IMPATTO VITA
INTERNET DELLE COSE
GDPR
FRODI INFORMATICHE
BIG DATA
NUOVE TECNOLOGIE
ETICA E DIRITTO
PROCEDURA CIVILE
PHISHING

SPONSORED BY

intesa

4CLEGAL
www.4cLegal.com

Qi net

ASSOCIAZIONE GIOVANI AVVOCATI TORINO
AGA

CLOUD COMPUTING E PROTEZIONE DEI DATI PERSONALI NEGLI STUDI LEGALI

DI LUDOVICA PASERI

1. Introduzione

Sempre più frequentemente gli studi legali si affidano a *Internet Service Provider* per ottenere servizi di *cloud computing*, utili ai fini dello svolgimento dell'attività forense. Non sempre questo avviene, ed è avvenuto negli anni precedenti, in totale consapevolezza. Molti sono i rischi che le tecnologie di *cloud computing* portano con sé in relazione alla protezione dei dati in esso allocati e, con l'introduzione di una nuova disciplina europea in materia di tutela dei dati personali, risulta utile ricomporre la questione e analizzare vantaggi e rischi.

Il presente elaborato intende analizzare i profili problematici in materia di protezione dei dati personali, che caratterizzano il *cloud computing*, alla luce di un cambiamento di paradigma nella materia, introdotto con il nuovo Regolamento Europeo, con specifico riferimento agli studi legali. A questo proposito la trattazione indaga le linee generali del cambiamento di paradigma nella tutela dei dati personali e le conseguenze dello stesso, in particolare, nel mondo della professione forense, nel par. 2. Nel successivo par. 3, invece, si passa all'analisi della tecnologia di *cloud computing* con specifico riferimento all'applicazione della stessa negli studi legali. Infine, dopo l'analisi di vantaggi e rischi correlati al *cloud*, l'attenzione è posta sull'attuale tutela dei dati personali in *cloud* negli studi legali, facendo emergere le *best practicies* tese ad ottenere il massimo dallo sfruttamento del potenziale delle tecnologie di *cloud computing* nell'attività forense.

2. Un cambiamento di paradigma nella tutela dei dati personali

Il 25 maggio 2018 è divenuto effettivamente applicabile il Reg. 2016/679/UE, il cd. *General Data Protection Regulation* (in seguito, GDPR), introducendo una nuova disciplina in materia di dati personali a livello europeo, sostituendo la risalente Dir. 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il cambio di paradigma in merito alla tutela dei dati personali, reso possibile da questa nuova normativa, è ravvisabile da più punti di vista.

Innanzitutto, vi è un cambiamento di contenitore: la disciplina della protezione dei dati personali non è più contenuta in una Direttiva[1], come avveniva fino a quel momento, ma, bensì, assume la formale veste del Regolamento, fonte del diritto europeo di portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri senza che sia necessario alcun tipo di recepimento, come previsto dall'art. 288 TFUE.

---

1 Sul punto si veda: R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy): scritti in memoria di Stefano Rodotà*, Giuffrè editore, Milano, 2019, pp. 7-11.

In secondo luogo, vi è un cambiamento di approccio: l'attenzione passa dal dato in sé e per sé, ai processi realizzati sui dati, vale a dire i differenti trattamenti. A questo proposito, infatti, vi è il tentativo del legislatore europeo, di superare il modello del cd. *notice and consent*, vale a dire dell'informativa e consenso, considerando quest'ultimo una sola delle sei basi legali che rendono lecito il trattamento, rappresentate dall'analitica e tassativa elencazione contenuta nel par. 1 dell'art. 6 del Reg. 2016/679/UE[2].

Inoltre, gli attori coinvolti nel trattamento dei dati personali devono attenersi ai due pilastri della normativa: approccio al rischio e responsabilizzazione.

La responsabilizzazione, espressa con il termine inglese *accountability*, è uno degli obbiettivi che il GDPR intende far perseguire a coloro che trattano dati personali: per permettere una tutela dinamica di tali dati, infatti, è necessario che i soggetti coinvolti mantengano memoria storica di quanto realizzato nei propri trattamenti e si assumano la responsabilità di una corretta gestione dei medesimi.

Con l'espressione "approccio al rischio" si intende la capacità di valutare quale possa essere il rischio che riguarda i dati dell'interessato, il cd. *data subject*, vale a dire colui a cui i dati personali si riferiscono. Tale valutazione, la cd. *data protection impact assessment* deve essere realizzata allorquando un determinato tipo di trattamento, nell'ipotesi in cui preveda un particolare uso di nuove tecnologie, "*considerati la natura, l'oggetto, il contesto e le finalità del trattamento*"[3], possa presentare un elevato rischio per i diritti e le libertà delle persone fisiche. La stessa prevede una descrizione del trattamento e delle finalità dello stesso; una valutazione in ordine a necessità e proporzionalità dei trattamenti rapportati alle finalità; una valutazione dei rischi che possono essere arrecati a diritti e libertà dei *data subjects*; nonché le misure previste per affrontare tali rischi[4].

Al di là dei materiali adempimenti resi necessari per essere conformi alla normativa, si può, quindi, affermare che si sia voluto introdurre un cambio di paradigma della *data protection*, teso a favorire una presa di consapevolezza da parte dei vari soggetti coinvolti nel trattamento dei dati personali.

---

[2] Le basi legali che garantiscono liceità al trattamento di dati personali, ai sensi del citato art. 6 Reg. 2016/679/UE, sono: a) il consenso al trattamento reso dall'interessato; b) l'esecuzione di un contratto di cui l'interessato è parte o l'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) l'adempimento di un obbligo legale a cui è soggetto il titolare del trattamento; d) la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il perseguimento del legittimo interesse del titolare o di terzi.

[3] Art. 35, par. 1, Reg. 2016/679/UE;
disponibile a: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679.

[4] Sul punto l'ex Garante Privacy, Franco Pizzetti, in un suo recente contributo, afferma che «La valutazione del rischio e la conseguente adozione di misure adeguate a ridurlo il più possibile, diventano dunque il nucleo centrale della tutela, con la conseguenza che devono essere costantemente rinnovati», in F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018, p. 47.

2.1 La professione forense e i dati personali

Il cambio di paradigma che ha interessato la protezione dei dati personali, con il GDPR, travolge anche la professione forense. Gli avvocati sono, infatti, chiamati a prendere consapevolezza del fatto che, a causa dell'intrinseca natura della loro professione, trattano un gran numero e una grande varietà di dati personali[5]. Questo implica, innanzitutto, abbandonare la visione per la quale tutto ciò che riguarda la privacy dei clienti si limiti ad essere una lista di anonimi adempimenti che si possa risolvere con qualche firma.

Come detto poco sopra, infatti, ciò che deve cambiare prima di tutto è l'approccio alla protezione dei dati: l'avvocato deve prendere consapevolezza di quali e quanti dati tratta nel suo fisiologico operare, come gli stessi sono conservati, per quanto tempo, con quali modalità e, soprattutto, adottare un approccio dinamico nei confronti della materia, che implichi il miglioramento continuo della gestione dei dati.

Una robusta, consapevole e soprattutto proporzionata protezione dei dati personali da parte degli studi legali rappresenta sia un dovere che un vantaggio per gli stessi. Da un lato, deontologicamente, garantire ai clienti che i loro dati siano trattati sapientemente è parte del dovere sancito all'art. 14 del codice deontologico, secondo cui «*L'avvocato è tenuto, nell'interesse del cliente e della* parte assistita, alla rigorosa osservanza del segreto professionale e al massimo riserbo su fatti e circostanze in qualsiasi modo apprese nell'attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell'attività di consulenza legale e di assistenza [6] stragiudiziale e comunque per ragioni professionali» . D'altro canto, un'effettiva tutela dei dati personali dei clienti si concretizza in un vantaggio nella creazione di un clima di trasparenza e fiducia, che si pone alla base di un sano e proficuo rapporto tra cliente e professionista.

Nel parlare di proporzionata ed effettiva tutela dei dati personali si fa, però, riferimento ad un ulteriore aspetto che l'avvocato non deve dimenticare, vale a dire che la protezione dei dati personali non significa segretezza: un pilastro della disciplina, infatti, è l'art. 1 Reg. 2016/679/UE in cui si sancisce che «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*». Proprio per questo motivo, si fa necessario che l'avvocato, nel trattare dati personali, rifugga da un'ottica integralista di tutela, per operare un meditato bilanciamento dei contrapposti interessi in gioco, in nome dell'*accountability* di cui sopra.

---

[5] Il pratico operare dell'avvocato coinvolge necessariamente una nutrita gamma di dati considerati "ex sensibili": necessariamente la professione forense implica il trattamento di particolari categorie di dati, ai sensi dell'art. 9 Reg. 2016/679/UE, vale a dire l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, nonché i dati personali relativi a condanne penali e reati il cui trattamento, ai sensi dell'art. 10 Reg. 2016/679/UE, « [...]*deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati*».

[6] Art. 14 Codice deontologico forense, approvato dal Consiglio Nazionale Forense nella seduta del 31 gennaio 2014, e pubblicato nel GU, SG, n. 241, del 16 ottobre 2014.

3. Il *cloud computing* negli studi legali

Il *cloud computing*, «l'evoluzione di una serie di tecnologie che, una volta utilizzate congiuntamente, sono in grado di rivoluzionare le modalità con cui le organizzazioni costruiscono le proprie infrastrutture informatiche»[7], per la sua specifica natura, può apportare un gran numero di vantaggi all'effettivo operare di coloro che svolgono la professione forense. Per poterli comprendere appieno, è, però, opportuno analizzare cosa si intenda per *cloud computing*[8]. Con questa espressione, infatti, si fa riferimento (1) all'utilizzo di applicazioni informatiche, (2) all'acquisto di servizi, oppure, (3) al trasferimento di parte delle proprie attività informatiche in infrastrutture detenute di terzi, sulle quali si vada direttamente ad operare.

(1) Per quanto riguarda il primo aspetto, si fa riferimento all'acquisizione di spazio in *cloud*, in cui allocare i propri dati. Le applicazioni informatiche di cui ci si avvale possono riguardare, tra le altre cose, la gestione di documenti, lo sviluppo di *software*, l'amministrazione di banche dati e la gestione di posta elettronica[9]. Questo modello è definito *Software as a Service* (SaaS)[10] e gli esempi tipici sono i servizi forniti da Sakeforce (CRM) e Google Apps con Google Docs o i servizi e-mail[11].

---

[7] G. REESE, *Cloud computing. Architettura, infrastrutture, applicazioni*, Tecniche nuove, Milano, 2010, p. 1

[8] Una definizione tecnica e comunemente accettata di *cloud computing* è fornita dal *US National Institute for Standards and Technology* (NIST), secondo cui: «Il *cloud computing* è un modello che permette l'accesso facile, su richiesta e in rete ad un insieme condiviso di risorse informatiche configurabili [...] che può essere fornito rapidamente o con l'interazione di fornitori di servizi» in P. MELL, T. GRANCE, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, Special Publication, 800-145, 2011, p. 2. Disponibile in: <http:// nvlpubs.nist.gov/ nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. La classificazione esposta ai fini della presente trattazione è quella basata sulla tipologia di servizi erogati.

[9] J. BARR, *Il cloud computing per applicazioni web*, Apogeo, Milano, 2010, p. 4.

[10] SUN MICROSYSTEMS, INC, *Introduction to Cloud Computing Architecture, White paper*, ed. I, 2009, p. 9. Disponibile in

<http://staff.polito.it/alessandro.mantelero/cloud_computing.html>.

[11] S. A. AHSON E M. ILYAS, *Cloud computing and software services. Theory and techniques*, CRC press, New York, 2011, p. 3.

(2) L'acquisto di servizi di *cloud computing*, invece, rappresentato dal modello *Infrastructure as a Service* (IaaS)[12], implica l'ottenimento, da parte del fruitore finale, di un computer virtuale di cui si avvarrà per le proprie attività, dove collocherà dati e *software* di cui necessita. Questo computer virtuale che si acquista è generato dalle varie componenti informatiche del *cloud*.

(3) Infine, il trasferimento delle proprie attività informatiche in *cloud,* rappresentato dal modello *Platform as a Service* (PaaS) significa evitare di dover realizzare un proprio apparato informatico per avvalersi di quello offerto direttamente dal *provider*[13] per lo sviluppo e l'*hosting* evoluto di applicazioni[14].

3.1 I vantaggi per la professione forense

La tipologia di servizi *cloud* che può maggiormente interessare uno studio legale è generalmente quella ricollegabile al primo modello, SaaS, e, nello specifico, il riferimento va ai servizi di *cloud storage*, vale a dire all'immagazzinamento e all'archiviazione su server remoti di dati, facilmente recuperabili in ogni momento.

I vantaggi sono molteplici. In primo luogo, è prevista la gestione diretta e su richiesta[15] di tali servizi: la possibilità per l'avvocato in quanto consumatore finale di attivare autonomamente nuove risorse (nuovi server o nuovo spazio di *storage*), in maniera indipendente rispetto al *cloud provider*[16]. Dal punto di vista economico, questa possibilità è decisamente vantaggiosa: dal momento che il servizio è basato sull'effettivo bisogno, risulta non essere necessario un cospicuo investimento iniziale, antecedente la reale richiesta di utilizzo delle risorse[17]. Per rendere la fruibilità dei servizi il più ampia possibile, realizzabile attraverso qualsiasi dispositivo, mediante meccanismi standardizzati, è comunque imprescindibile ampio accesso alla rete.

---

[12] Questo modello è volto a concedere un'infrastruttura «con capacità elaborativa, di memorizzazione, di rete e altre risorse IT, sulla quale l'utente può installare ed eseguire il software a lui necessario, a partire dal sistema operativo e arrivare alle applicazioni», si veda F. PIROZZI, *Il cloud computing. Lex mercatoria e tutela dei dati*, Giuffrè, Milano, 2016, p. 16.

[13] Con il termine *provider*, vale a dire il fornitore dei servizi di *cloud*, ci si riferisce alla società privata ed esterna rispetto al fruitore, specializzata nella fornitura di servizi informatici.

[14] G. SARTOR*, L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli editore, Torino, 2012, pp. 63 -64.

[15] Si traduce così il peculiare carattere definito dal NIST "*On-demand self-service*" in P. MELL, T. GRANCE, *The NIST Definition, op. cit.,* p. 2.

[16] R. ROSSI, *Cloud computing per la piccola e media impresa*, Tecniche nuove, Milano, 2015, p. 4.

[17] J. BARR, *op. cit*., p. 8.

In secondo luogo, un enorme vantaggio è il *resource pooling*, vale a dire la messa in comune delle risorse, a favore di una moltitudine di utenti, attraverso[18] il cd. modello *multi-tenant* , cioè mediate un'applicazione che conceda i servizi ad una pluralità di utenti, in parallelo, preservandone la separazione, dando così la percezione di unicità del rapporto, benché sia *database* che architettura sottostante siano, di fatto, condivise. All'interno di uno studio legale di medie o grandi dimensioni, questo vantaggio è decisamente considerevole se si pensa alla possibilità di accedere a dati condivisi da più utenti in differenti luoghi geografici.

Inoltre, i servizi di *cloud* sono caratterizzati da una grande flessibilità ed elasticità. Essi, infatti, sono forniti in maniera considerevolmente rapida (nell'ordine di secondi o minuti), aumentando e riducendo le prestazioni a seconda della moltitudine di consumatori, senza che le stesse subiscano dei degradi. Questo vantaggio è dovuto alla scalabilità dei sistemi di *cloud computing*, in grado di espandere o limitare l'infrastruttura con grandissima flessibilità, sulla base del bisogno di maggiori o minori risorse[19].

Infine, i servizi sono misurati, basati sulla formula del "*pay-as-you-go*", prevedendo che si paghi solo ciò che effettivamente venga utilizzato: in questo modo il *provider* fornisce un'automatica attività di controllo su andamenti e consumi, permettendo di adottare la risposta sulla base dell'effettiva domanda del cliente, a cui, successivamente, dovrà poi rendere conto[20].

3.2 I rischi tecnologici: il rapporto tra il giurista e il tecnico

Come ogni tecnologia, anche il *cloud computing* comporta una serie di rischi. Gli aspetti maggiormente problematici derivanti dall'adozione di soluzioni in *cloud* sono rappresentabili in termini di rischi relativi alla protezione dei dati, alla sicurezza e alla fiducia.

3.2.1 Protezione dei dati personali

La tutela del trattamento dei dati personali è una tematica trasversale che, in qualche modo, tocca ogni altro aspetto problematico del fenomeno *cloud*, dalla determinazione delle clausole contrattuali, alla *cybersecurity*, passando per la fiducia.

---

[18] Sull'architettura dati *multi-tenant* si veda: <https://msdn.microsoft.com/itit/library/aa479086.aspx> dove si precisa il rapporto tra separazione e condivisione dei dati in questo modello: «Ogni *database* è associato al relativo *tenant* tramite metadati, mentre le funzionalità di protezione del *database* impediscono ai *tenant* di accedere accidentalmente o intenzionalmente ai dati degli altri *tenant*».

[19] R. BRUNETTI, *Windows Azure. Il sistema operativo e la piattaforma per il cloud computing*, Mondadori informatica, Milano, 2009, p. 40.

[20] E. ACQUATI, S. MACELLARI E A. OSNAGHI (a cura di), *Pubblica Amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, Passigli Editori, Bagno a Ripoli, 2011, p. 35.

In relazione ai sistemi di *cloud*, si ha generalmente la percezione di avere a che fare con «un sistema "per sua natura insicuro e aperto", con conseguenti rischi di perdita e furto di informazioni e manovre non autorizzate»[21]. Tale percezione trova le sue radici nella natura stessa dell'infrastruttura *cloud*: per ragioni tecniche, legate all'esigenza di evitare il sovraccarico dei server, nonché per evitare le perdite delle informazioni, i dati vengano spostati frequentemente da un server all'altro, nonché immagazzinati in più d'uno nello stesso momento[22]. Tale fenomeno di delocalizzazione dei *data center* è ampiamente riconosciuto, anche in giurisprudenza[23]: in questo modo risulta difficile per il titolare del trattamento dei dati personali sapere con certezza dove gli stessi siano materialmente collocati, e quindi averne il pieno controllo.

Inoltre, se la delocalizzazione dei dati in *cloud* fra i vari server permette che le risorse allocate in queste infrastrutture siano meglio conservabili e prontamente reperibili, dall'altro lato rappresenta una problematica in materia di diritto alla cancellazione, ai sensi dell'art. 17 Reg. 2016/679/UE, secondo cui «*il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali*», qualora gli venga richiesto dal cliente-*data subject*[24].

3.2.2 Sicurezza informatica

Sempre più spesso si verificano casi in cui la minaccia nei confronti dei dati personali derivi dall'esterno, attraverso trattamenti illegittimi che minano la sicurezza dei dati degli utenti e inevitabilmente vanno ad abbassarne la fiducia. Con l'espressione sicurezza informatica, in generale, intendiamo «la capacità di una rete, o di un sistema di informazione, di resistere, ad eventi o atti dolosi che ne possono compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi, nonché dei servizi forniti, o [25] accessibili, tramite la suddetta rete (o sistema)» . L'architettura *cloud*, tenuto conto della sua struttura ed essendo un sistema multi-agente, può risultare una preda molto attraente per un attacco: può permettere l'accesso ai dati di tutti i clienti del fornitore di servizi.

---

[21] G. NOTO LA DIEGA, *Il cloud computing. Alla ricerca del diritto perduto nel web 3.0*, in "Europa e diritto privato", vol. 17, n. 2, 2014, p. 578, nota 3.

[22] N. FOGGETTI, *Privacy protection, applicable law and jurisdiction issues in cloud computing: an international and EU prospective*, in "Cyberspazio e diritto", vol. 15, n. 51, 2/3, 2014, p. 226.

[23] Il riferimento va a Cass. Penale, Sez. Un., 26/03/2015, n. 17325, in materia di accesso abusivo ai dati: «[...] la dimensione aterittoriale si è incrementata da ultimo con la diffusione dei dispositivi mobili (*tablet*, *smartphone*, sistemi portatili) e del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate dalle quali è possibile accedere da qualunque parte del globo». A questo proposito, la problematica della *data protection* in *cloud* si lega al tema del trasferimento transfrontaliero dei dati personali.

[24] In dottrina vi è chi sostiene che, limitatamente ai cloud di modello IaaS, laddove il servizio fornito si limiti ad un'attività di storage, il rapporto possa inquadrarsi nella tradizionale figura del deposito: si veda E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, in G. CASSANO, G. SCORZA e G. VACIAGO (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione, giurisprudenza*, Padova, Cedam, 2013, p. 683.

[25] F. BOSCO, *Cyberterrorismo e cyberwarfare: profili giuridici e analisi della casistica internazionale*, in G. CASSANO, G. SCORZA e G. VACIAGO (a cura di), *Diritto dell'Internet. op. cit.*, p. 658.

3.2.3. Fiducia

La fiducia è un elemento imprescindibile nella relazione fra cliente e difensore e, allo stesso modo, è fulcro della relazione fra utente e *provider* che fornisce servizi di *cloud*. Nel caso in cui uno studio legale decida di usufruire di servizi di *cloud computing,* quindi, la situazione risulta doppiamente delicata. Il livello di fiducia richiesto è maggiore, perché si basa su un doppio grado di asimmetria informativa: un primo grado, tra cliente e avvocato, e un secondo grado tra avvocato come utente di servizi e il *cloud provider*, vale a dire colui che fornisce tali servizi.

La tematica della cd. *trust* assume maggiore complessità quando si è nell'ambito dell'online: in tale situazione non si ha a che fare con una prestazione fiduciaria che vede due soggetti determinati ma, più ampiamente, l'oggetto è il funzionamento di una piattaforma[26].

L'avvocato deve, quindi, agire in due direzioni: da un lato deve pretendere fiducia dal proprio *provider* e dall'altro ha un dovere etico[27] nei confronti del proprio cliente e, pertanto, deve impegnarsi a garantire a quest'ultimo un elevato livello di sicurezza, tale per cui non venga meno la sua fiducia.

4. Come sono tutelati i dati personali in *cloud* negli studi legali?

Nella migrazione verso l'immateriale *cloud*, uno studio legale deve, ai fini della tutela dei dati personali, avere innanzitutto chiaro i ruoli rivestiti dai vari attori in gioco: in questo modo, infatti, è possibile identificare le specifiche responsabilità di coloro che sono «detentori del nuovo potere informatico, consistente nel controllo sui singoli, reso possibile dall'acquisizione e [27] dall'elaborazione di informazioni, spesso anche apparentemente neutre» .

Lo studio legale è il titolare del trattamento e, in quanto tale, è tenuto all'adempimento degli obblighi ad esso riconnessi, ai sensi dell'art. 24 Reg. 2016/679/UE. Il *data sujbect*, vale a dire l'interessato, il soggetto a cui i dati personali si riferiscono è rappresentato dal cliente dello studio legale. In questa dinamica, il *provider* che fornisce i servizi di *cloud* deve essere nominato responsabile del trattamento ai sensi dell'art. 28 Reg. 2016/679/UE.

Tale specifica individuazione dei differenti ruoli assume considerevole importanza in materia di sicurezza informatica. Gli art. 33 e 34 Reg. 2016/679/ UE, infatti, sanciscono l'obbligo, per il titolare del trattamento, di dare comunicazione all'autorità di controllo e allo stesso interessato dei dati, ogniqualvolta sia avvenuta una violazione dei dati personali o più in generale una perdita di informazioni. A sua volta, il responsabile-*provider* è chiamato a informare il titolare-avvocato senza ingiustificato ritardo, nel momento in cui venga a conoscenza di un'eventuale violazione. L'obbligo di comunicazione è sempre vincolante per quanto riguarda la notificazione all'autorità di controllo, mentre è eventuale nei confronti del diretto interessato, solamente laddove presenti «*un rischio elevato per i diritti e le libertà delle persone fisiche*».

---

[26] Sul tema della fiducia online si veda: M. DURANTE, *The online construction of personal identity through trust and privacy*, in "Information", v. 2, n. 4, 2011, p. 597; M. TADDEO, Fiducia on-line: rischi e vantaggi in M. DURANTE e U. PAGALLO (a cura di), Manuale di informatica giuridica e diritto delle nuove tecnologie, Torino, Utet, 2014, p. 420.

[27] D. L. ELM, S. BRODERICK, *Cloud Computing, Storing, and Sharing: Guidance for the Solo and Small Firm Lawyer*, in "Criminal Justice", vol. 30, n. 4, 2015, p. 5.

[28] A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, in "Diritto dell'informatica", vol. 24, Milano, Giuffrè, 2007, p. 52.

3.1 *Best practices*

Nel percorso teso a rendere conformi al GDPR i trattamenti dei dati personali realizzati nel pratico operare richiesto dalla professione forense[29], gli studi legali devo prestare particolare attenzione alle tecnologie di *cloud*, qualora siano utilizzate.

I servizi di *cloud computing* forniti dai *provider*, come finora analizzato, permettono di ottenere una serie notevole di vantaggi che inducono sempre più a migrare verso l'immateriale, ma, d'altro canto, richiedono specifiche cautele tese alla minimizzazione dei rischi.

In primo luogo, è richiesta profonda consapevolezza da parte dello studio legale nella scelta del *provider* a cui affidarsi[30], tenendo in considerazione l'affidabilità e la reputazione dello stesso, nonché la tipologia di *disaster recovery plan* di cui si è dotato.

In secondo luogo, inoltre, è essenziale garantirsi la possibilità di cambiare [31] fornitore e, pertanto, è fondamentale prestare attenzione alla portabilità : con sistemi di *vendor lock-in* si indicano meccanismi in base ai quale lo studio legale resta vincolato dal formato di standard proprietario scelto dal *provider* a cui si è rivolto, rendendo materialmente difficoltosa la portabilità dei dati, perlomeno in termini di costi che si trova costretto a dover sopportare l'utente-avvocato.

Viene, inoltre, raccomandato, anche di recente dall'*European Data Protection Supervisor*[32], una particolare attenzione da parte del titolare del trattamento nei confronti degli accessi ai dati allocati in *cloud*: è opportuno che gli stessi pretendano che i propri fornitori forniscano, sul punto, dei report periodici.

---

[29] A questo proposito si evidenzia che il Consiglio Nazionale Forense ha prodotto delle linee guida: CNF, Il GDPR e l'avvocato, 10 agosto 2018, disponibili a: https://www.consiglionazionaleforense.it/gdpr-e-privacy.

[30] F. GILBERT, *The use of cloud computing in a law office*, in "The Practical Lawyer", v. 60, n. 2, 2014, p. 3.

[31] *Ibid*.

[32] EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines on the use of cloud computing services*, 16 marzo 2018, disponibile a: http://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud- computing-services-european_en.

Un ulteriore aspetto fondamentale è, poi, quello relativo ai contratti di *cloud*: è fondamentale che lo studio legale presti attenzione sia alla specifica contrattazione che lo riguarda, sia ai *Service Level Agreement* (SLA)[33], vale a dire gli accordi per determinare il tipo di servizi erogati dai *cloud provider* agli utenti, identificando soluzioni comuni per risolvere il problema delle terminologie differenti utilizzate dai diversi fornitori. L'importanza dei SLA è stata anche ribadita dall'*European Data protection Supervisor*[34], perché gli stessi «non sono da considerarsi "clausole", bensì veri e propri accordi a sé stanti, con il cliente/ utente e il fornitore del servizio, che vanno a completare il contratto base di *cloud computing* con previsioni particolarmente analitiche volte a regolamentare l'accesso, l'uso e i vari livelli di sicurezza e di autorizzazione oltre alla sospensione degli account o dei servizi in caso di emergenza»[35].

Una peculiarità che caratterizza gli studi legali è, poi, il trattamento di particolari categorie di dati personali ai sensi dell'art. 9 Reg. 2016/679/UE e il trattamento dei dati giudiziari ex art. 10 Reg. 2016/679/UE. In merito a questi dati, è dovere del titolare del trattamento, vale a dire dello studio legale, garantire una tutela maggiore e più robusta, adottando specifiche misure di sicurezza come per esempio la crittografia.

Infine, nel garantire una trasparente comunicazione con il cliente, base per lo sviluppo del legame fiduciario, è specifico dovere dell'avvocato dare atto dell'archiviazione in *cloud*, nel rispetto degli obblighi di comunicazione previsti agli artt. 13 e 14 Reg. 2016/679/UE.

---

[33] D. L. ELM, S. BRODERICK, *Cloud Computing, op. cit.,* p. 6.
[34] EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines, op. cit.,* p. 28.
[35] M. C. DE VIVO, *Il contratto ed il cloud computing*, in "Disciplina del commercio e dei servizi", n. 3, 2015, p. 1020.

5. Conclusioni

In quest'epoca di rivoluzione digitale anche la professione forense deve necessariamente impegnarsi per comprendere i profondi cambiamenti che stanno investendo ogni ambito delle nostre vite. Attraverso tale comprensione è possibile, infatti, sfruttarne il potenziale ed evitare di doversi adattare o affidare in maniera inconsapevole.

L'analisi dell'utilizzo delle tecnologie di *cloud* da parte degli studi legali che è stata argomento della presente trattazione ha voluto, più in generale, rappresentare unicamente un approccio: l'avvocato deve, infatti, necessariamente adottare un metodo per interagire con le nuove tecnologie che in ogni caso influiscono, e influiranno sempre di più, sul proprio tradizionale operato.

Questo approccio pro-attivo si fa fondamentale per evitare che il professionista si debba affidare al tecnico ciecamente e inconsapevolmente. Nell'utilizzo delle infrastrutture di *cloud computing*, più che in altre circostanze, è emblematico che l'avvocato abbia il dovere di comprendere e in qualche modo anche vigilare sull'operato del tecnico, il provider fornitore dei servizi *cloud*, in linea con il cambiamento di paradigma nella tutela dei dati personali, introdotto con il GDPR, che, come abbiamo visto, mira ad aumentare la consapevolezza e la responsabilizzazione.

Così come l'umanità senza futuro non è quella priva di prospettive per l'avvenire né quella sottoposta a rigide regole meccanicistiche, ma è quella che non sa più interpretare, in modo critico, la propria storia, anche la professione forense deve adottare una visione di critico interesse nei confronti delle potenzialità delle nuove tecnologie, e sfidare la propria capacità di evolvere, con solide radici nel passato.

6. Bibliografia

MONOGRAFIE E ARTICOLI

ACQUATI E., S. MACELLARI, A. OSNAGHI (a cura di), *Pubblica Amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, Passigli Editori, Bagno a Ripoli, 2011.

AHSON S. A., M. ILYAS, *Cloud computing and software services. Theory and techniques*, CRC press, New York, 2011.

BARR J., *Il cloud computing per applicazioni web*, Apogeo, Milano, 2010. CASSANO G., G. SCORZA e G. VACIAGO (a cura di), *Diritto dell'Internet.*

Manuale operativo: casi, legislazione, giurisprudenza, Padova, Cedam, 2013.
DE VIVO M. C. , *Il contratto ed il cloud computing*, in "Disciplina del *commercio e dei servizi", n. 3, 2015.*

DURANTE M., *The online construction of personal identity through trust and privacy*, in "Information", v. 2, n. 4, 2011.

DURANTE M., U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, Utet, 2014.

ELM D. L., S. BRODERICK, *Cloud Computing, Storing, and Sharing: Guidance for the Solo and Small Firm Lawyer*, in "Criminal Justice", vol. 30, n. 4, 2015.

FOGGETTI N., *Privacy protection, applicable law and jurisdiction issues in cloud computing: an international and EU prospective*, in "Cyberspazio e diritto", vol. 15, n. 51, 2/3, 2014.

MANTELERO A., *Il costo della privacy tra valore della persona e ragione d'impresa*, in "Diritto dell'informatica", vol. 24, Milano, Giuffrè, 2007.

MELL P., T. GRANCE, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, Special Publication, 800-145, 2011.

NOTO LA DIEGA G., *Il cloud computing. Alla ricerca del diritto perduto nel web 3.0*, in "Europa e diritto privato", vol. 17, n. 2, 2014.

PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy): scritti in memoria di Stefano Rodotà*, Giuffrè editore, Milano, 2019.

PIROZZI F., *Il cloud computing. Lex mercatoria e tutela dei dati*, Giuffrè, Milano, 2016.

PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018.

REESE G., *Cloud computing. Architettura, infrastrutture, applicazioni*, Tecniche nuove, Milano, 2010.

ROSSI R., *Cloud computing per la piccola e media impresa*, Tecniche nuove, Milano, 2015.

SARTOR G.*, L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli editore, Torino, 2012.

SUN MICROSYSTEMS, INC, *Introduction to Cloud Computing Architecture, White paper*, ed. I, 2009.

NORMATIVA E GIURISPRUDENZA

Cass. Penale, Sez. Un., 26/03/2015, n. 17325

Codice deontologico forense, approvato dal Consiglio Nazionale Forense nella seduta del 31 gennaio 2014, e pubblicato nel GU, SG, n. 241, del 16 ottobre 2014.

EUROPEAN DATA PROTECTION SUPERVISOR, *Guidelines on the use of cloud computing services*, 16 marzo 2018.

Regolamento UE. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).

SPONSORED BY

ASSOCIAZIONE GIOVANI AVVOCATI TORINO

REG. (UE) N. 2016/679: RIMEDI DI NATURA PRIVATISTICA E COMPETENZA INTERNAZIONALE IN AMBIENTE ONLINE

DI ENNIO PIOVESANI

1. Introduzione[1]

Esaminati i rimedi di natura privatistica previsti nel Reg. (UE) n. 2016/679[2] (in prosieguo: RGPD o Regolamento) ed affrontate le principali questioni interpretative poste dall'art. 79, par. 2[3], l'attenzione si concentra sul problema della ripartizione della competenza internazionale, tra i giudici degli Stati membri dell'Unione, in ipotesi di azioni esercitate contro il titolare o il responsabile del trattamento (in prosieguo, ber brevità: titolare), per ottenere il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*[4].

[1] di Ennio Piovesani

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), G.U.U.E. L 119/1, 4.5.2016 (ELI: http:// data.europa.eu/ eli/reg/2016/679/oj).

[3] Salvo diversa indicazione, gli artt. ed i consid. indicati in seguito sono quelli del RGPD.

[4] I seguenti aa. si occupano degli aspetti di diritto processuale internazionale (e talora anche di diritto internazionale privato) connessi al RGPD: *Brkan, Maja*, Data protection and European private international law: observing a bull in a China shop, IDPL 2015, Vol., 5 No. 4, 257; *de Miguel Asensio, Pedro Alberto*, Competencia y Derecho Aplicable en el Regolamento General Sobre Protección de Datos de la Unión Europea, REDI 2017, Vol. 69, No. 1, 75; *Franzina, Pietro*, Jurisdiction regarding Claims for the Infringement of Privacy Rights under the General Data Protection Regulation, in: De Franceschi, Alberto (ed.), European Contract Law and the Digital Single Market, 2016, pp. 81 e segg.; *Hess, Burkhard,* Die EU-Datenschutzgrundverordnung und das europäische Prozessrecht, in: Schütze, Rolf A. (Hrsg.), Fairness Justice Equity, Festschrift für Reinhold Geimer zum 80. Geburstag, 2017, pp. 255 e segg.; *Kohler, Christian*, Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union, Riv. dir. int. priv. proc. 2016, vol. 52, fasc. 3, 653; *Lundstedt, Lydia*, International jurisdiction over cross-border private enforcement actions under the GDPR, Stokholm Faculty of Law Research Paper 2018, No. 57, pp. 212 e segg.; *Marongiu Buonaiuti*, *Fabrizio*, La disciplina della giurisdizione nel regolamento (UE) n. 2016/679 concernenti il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento "Bruxelles I-bis", CDT 2017, Vol. 9, No. 2, 448; *Pato, Alexia*, The Collective Private Enforcement of Data Protection Rights in the EU, AA.VV., MPI-IAPL Summer School, 3rd ed., in pubblicazione; *Piovesani, Ennio,* The interface between the jurisdictional rules of Reg. (EU) No 2016/679 and those of Reg. (EU) No 1215/2012, in: Università degli Studi di Milano (pub.), Big data and Public Law: new challenges beyond data protection, 2019, pp. 64 e segg.; *Requejo Isidro, Marta*, Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection, Max Planck Institute Luxembourg for Procedural Law, Research Paper Series 2019, No. 3; *Revolidis*, *Ioannis*, Judicial Jurisdiction over Internet Privacy Violations and the GDPR: a Case of "Privacy Tourism", MUJLT 2017, Vol. 7, Iss. 11, 7; *van Calster, Gert*, Sur des bases fragiles. Le RGPD et les règles de compétence concernant les infractions au droit respect de la vie privée, Obs. Bxl. Julliet 2018, No. 113, 28.

2. Rimedi di natura privatistica

«Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile», l'art. 79, par. 1, prevede il diritto «di ogni interessato ad un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento». In particolare, il RGPD prevede due rimedi di natura privatistica: il diritto di agire per il risarcimento del danno ai sensi dell'art. 82, par. 1, nonché di dare mandato ad un Ente ai sensi dell'art. 80, par. 1.

2.1. Ricorso giurisdizionale

Il ricorso, o meglio i ricorsi evocati all'art. 79, par. 1[5], sono quelli previsti nell'ordinamento dello Stato membro del giudice adito.

In Italia ed in Germania, le misure (interne) di adeguamento al RGDP – rispettivamente, il D.Lgs. 10.8.2018 n. 101[6] e la DSAnpUG-EU[7] –, introducono accorgimenti processuali relativi ai ricorsi, nonché ai rimedi di natura privatistica previsti nel Regolamento[8].

---

[5] La norma è associata ai consid. nn. 4, 108, 141 e 147 ed all'art. 45, par. 2, lett. a), RGPD; al consid. n. 55 ed all'art. 22 dell'abrogata Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (G.U.U.E. L 281/31, 23.11.1995 – ELI: http://data.europa.eu/eli/dir/1995/46/oj); all'art. 47 della Carta dei diritti fondamentali dell'Unione europea (G.U.U.E. C 303/1, 14.12.2007 http:// data.europa.eu/eli/treaty/char_2007/oj); all'art. 13 della Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali (S.T.E. n. 005); nonché, all'art. 15 del Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (S.T.C.E. n. 223).

[6] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), G.U. 4.9.2018, n. 205 (ELI: www.gazzettaufficiale.it/eli/ id/2018/09/04/18G00129/sg).

[7] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 30.6.2017, BGBl. 2017 I S. 2097.

[8] Chiari esempi di "europeizzazione" (*„EU-iesierung"*) del diritto processuale degli Stati membri. Cf. *Frenzel*, in Paal/ Pauly (Hrsg.), DS-GVO, BDSG, 2. Aufl. 2018, § 44 BDSG Rn. 8.

Per quanto concerne l'ordinamento italiano, ai sensi degli artt. 152, D.Lgs. 30.6.2003, n. 196[9] e 10, D.Lgs. 1.9.2011, n. 150[10] – così come modificati, rispettivamente, dall'art. 13, co. 1, lett. h) e dall'art. 17, D.Lgs. 101/2018 – i ricorsi di cui all'art. 79, par. 1, incluse le azioni per il risarcimento del danno di cui all'art. 82, sono:

- soggetti al rito del lavoro (art. 10, co. 1, D.Lgs. 150/2011);

- di competenza del Tribunale del luogo in cui il titolare abbia residenza o sede, oppure, in via alternativa, del Tribunale del luogo
  [11] in cui l'interessato abbia residenza (art. 10, co. 2, D.Lgs 150/2011) ; e,

- definiti con sentenza inappellabile (art. 10, co. 10, D.Lgs. 150/2011).

In Germania, la DSAnpUG-EU modifica la Bundesdatenschutzgesetz[12] (legge federale sulla protezione dei dati personali; in prosieguo: BDSG). Ai sensi del § 44 BDSG:

- il titolare può essere convenuto davanti al giudice del luogo in cui il titolare abbia uno stabilimento, oppure, in via alternativa, davanti al giudice del luogo in cui l'interessato abbia residenza abituale (§ 44, Abs. 1);
- la regola sulla competenza (interna) non si applica nell'ipotesi in cui il titolare sia un'autorità pubblica nell'esercizio dei suoi pubblici poteri (§ 44, Abs. 2); e,
- le notifiche di atti diretti al titolare che non abbia stabilimenti all'interno dell'Unione europea[13] possono compiersi anche presso il rappresentante designato a norma dell'art. 27, par. 1, RGPD (§ 44, Abs. 3).

---

[9] Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, G.U. 29.7.2003, n. 174, S.O. (ELI: www.gazzettaufficiale.it/eli/id/ 2003/07/29/003G0218/sg).

[10] Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione, ai sensi dell'articolo 54 della legge 18 giugno 2009, n. 69, G.U. 21.9.2011, n. 220 (ELI: https://www.gazzettaufficiale.it/eli/gu/ 2011/09/21/220/sg).

[11] I ricorsi di cui si tratta non sono attribuiti alla competenza del Tribunale in funzione di giudice del lavoro, ma, semplicemente, sono soggetti al rito del lavoro. Infatti, a.e. presso il Tribunale di Torino, i ricorsi non sono affidati alla Sez. V[a] (Lavoro), ma alla Sez. I[a] (Tribunale delle Imprese).

[12] Bundesdatenschutzgesetz v. 30.6.2017, BGBl. 2017 I S. 2097.

[13] V. *Mundil*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 27. Ed. Stand: 1.5.2018, § 44 BDSG Rn. 5.

Tra i ricorsi di cui all'art. 79, par. 1, in concreto ipotizzabili, figurano quelli esperiti per ottenere una misura cautelare, anche di natura inibitoria[14] – in Italia, ad esempio, un'ordinanza *ex* art. 700 c.p.c., che ordini la rimozione ed [15] inibisca la diffusione di dati personali sulle reti sociali ; e, in Germania, un provvedimento analogo ai sensi dei §§ 823 e 1004 BGB e 935 ZPO[16].

2.2. Risarcimento del danno

[17]
Il rimedio del risarcimento del danno è previsto nel già citato art. 82 . Il primo paragrafo dell'articolo infatti recita: «[c]hiunque subisca un danno materiale o immateriale causato da una violazione del [...] regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento»[18].

L'art. 82 introduce una norma uniforme a cui va data un'interpretazione [19] autonoma . Diventano così superflui i precedenti rinvii, in materia di protezione dei dati personali, alle disposizioni interne sulla responsabilità civile – in Italia agli artt. 2050 e 2059 c.c.[20] ed in Germania ai §§ 823 e 253 BGB[21] – salvo per gli aspetti (dell'obbligazione risarcitoria) non contemplati dalla norma eurounitaria, ad esempio, su tutti, i criteri di liquidazione del danno [22]

In ipotesi connotate dall'elemento d'estraneità, eventuali lacune devono essere colmate dalla legge applicabile in virtù del diritto internazionale privato autonomo dello Stato membro del giudice adito[23] – e cioè: in Italia, dalla legge applicabile ai sensi degli artt. 13, co. 2, lett. c) e 62 L. 31.5.1995, n. 219[24]; e, in Germania, da quella applicabile ai sensi degli artt. 40 e ss. EGBGB.

---

[14] V. *inter alios*, *Kohler*, Riv. dir. int. priv. proc. 2016, 653, 667. [15] Cf., a.e., Trib. Rieti, ord. 7.3.2019, Leggi d'Italia.

[16] Seppur non concesso per ragioni di merito, cf. OLG Dresden, Beschl. v. 7.1.2019 – 4 W 1149/18, BeckRS 2019, 327.

[17] L'art. è associato ai consid. nn. 75, 85, 108, 145 e 146 RDPG, nonché al consid. n. 55 ed agli artt. 47, par. 2, lett. e) e 23, par. 1, Dir. n. 95/46/CE.

[18] Per esempi di danni di cui all'art. 82, v. consid. nn. 83 e 85. [19] Cf. consid. n. 146.
[20] V. l'abrogato art. 15, D.Lgs. 196/2003.
[21] V. il § 83 BDSG.

[22] L'ideale sarebbe stato se il legislatore europeo avesse introdotto delle tabelle uniformi per la liquidazione del danno. *Dickmann, Roman*, Nach dem Datenabfluss: Schadenersatz nach Art. EWG_DSGVO Artikel 82 der Datenschutz-Grundverordnung und die Rechte des Betroffenen an seinen personenbezogenen Daten, r+s 2018, 345, 354.

[23] Il Reg. (CE) n. 864/2007 non trova applicazione, conformemente al suo art. 1, par. 2, lett. g). Regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II), G.U.U.E. L 199/40, 31.7.2007 (ELI: http://data.europa.eu/eli/reg/2007/864/oj).

[24] Riforma del sistema italiano di diritto internazionale privato, G.U. 3.6.1995, n. 128, S.O. (ELI: www.gazzettaufficiale.it/eli/id/1995/06/03/095G0256/sg).

Il generico riferimento a «chiunque» nell'art. 82, par. 1, suggerisce che, oltre agli interessati ed agli Enti di cui all'art. 80 (§ 2.3.), anche soggetti terzi possono promuovere azioni per ottenere il risarcimento del danno derivante dalla violazione del Regolamento[25].

Ad esempio, l'impresa che subisca un danno derivante dalla violazione delle norme del RGPD da parte dell'impresa concorrente, può agire contro quest'ultima, ai sensi dell'art. 82, per il ristoro del pregiudizio sofferto[26]. Nell'ordinamento italiano, in effetti, la violazione delle norme del RGPD potrebbe rilevare anche ai sensi delle norme civilistiche sulla concorrenza sleale [27]. In particolare, può integrare illecito concorrenziale ai sensi dell'art. 2598, n. 3, c.c., la condotta dell'impresa che tragga vantaggio competitivo[28] dalla violazione di norme di diritto pubblico , incluse le norme sulla protezione dei dati personali
In Germania, al contrario, è stato sinora escluso che la violazione del Regolamento possa far sorgere, in capo all'impresa concorrente- danneggiata, il diritto al risarcimento del danno. La dottrina tedesca più autorevole infatti sostiene che il RGPD introduca un regime sanzionatorio chiuso, insuscettibile di essere integrato dai rimedi contenuti nella Gesetz [29] gegen den unlauteren Wettbewerb[30] (legge contro la concorrenza sleale; in prosieguo: UWG); segnatamente dal § 3a UWG[31, 32]. Certi giudici di merito tedeschi hanno avallato la tesi[33], altri però l'hanno respinta.

---

[25] Cf., *inter alios*, *Moos/Schefzig/Arning*, Die neue Datenschutz-Grundverordnung, 1. Aufl. 2018, S. 617 Rn. 134 ed ivi nn. 160-161.

[26] Cf. *Däubler*, in: Däubler/Wedde/Weichert/Sommer, Datenschutz-Grundverordnung und BDSG-neu, Kompaktkommentar, 1. Aufl. 2018, Art. 82 DSGVO Rn. 4.

[27] V. *Fedi, Andrea*, Diritto dell'impresa e protezione dei dati personali, Società 2018, n. 10, 1087, 1091 ed ivi n. 40.

[28] V. Cass. 27.4.2004, n. 8012, Dir. ind. 2005, 203.

[29] V. Trib. Roma, 28.12.2006, Annali it. dir. autore 2008, 587.

[30] Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung v. 3.3.2010 (BGBl. 2010 I S. 254), das zuletzt durch Artikel 5 des Gesetzes v. 18.4.2019 (BGBl. 2019 I S. 466) geändert worden ist.

[31] Il § 3a UWG così recita: «Commette un atto di concorrenza sleale chiunque violi una disposizione di legge destinata, tra l'altro, a regolamentare il comportamento sul mercato nell'interesse dei suoi operatori, quando la violazione sia di natura tale da ledere in modo sensibile gli interessi dei consumatori, degli altri operatori del mercato o dei concorrenti». Trad. in C.G.U.E., sent. 15.7.2018 – C-339/17, *Verein fur lauteren Wettbewerb eV c. Princesport GmbH*, Racc., ECLI:EU:C:2018:539, punto 13.

[32] Cf. *Köhler*, in: Köhler/Bornkamm/Feddersen, UWG, Kommentar, 37. Aufl. 2019, § 3a UWG Rn. 1.40a-i.

[33] V. da ultimo, LG Stuttgart, Urt. v. 20.5.2019 – 35 0 68/18 KfH, reperibile in: https:// dejure.org.

Tra [34] quest'ultimi rientra l'Oberlandesgericht Hamburg . Con sentenza

d'appello del 25.10.2018, l'OLG si è pronunciato nell'ambito di una controversia sorta tra due imprese farmaceutiche tedesche tra loro concorrenti[35]. In primo grado, l'impresa attrice aveva lamentato come la convenuta avesse raccolto ordini su moduli contenenti dati personali dei pazienti, senza che per il trattamento di tali dati fosse stato ottenuto il [36] necessario consenso . Ciò avrebbe agevolato la convenuta nella raccolta [37] degli ordini . Così la convenuta avrebbe violato l'(ormai abrogato) art. 28, par. 7, BDSG, in materia di trattamento di dati personali in ambito sanitario. Tale violazione avrebbe integrato un illecito concorrenziale ai sensi del § 3a UWG. L'impresa attrice risultava vittoriosa in primo grado[38]. Successivamente interveniva il RGPD[39] e l'impresa soccombente ricorreva in appello. Davanti l'OLG, l'appellante si rifaceva all'orientamento dottrinale del RGPD come sistema sanzionatorio chiuso. L'OLG respingeva la tesi[40], anche alla luce dell'uso del pronome «[c]hiunque» nell'art. 82, par.

1, che consentirebbe a soggetti terzi di agire per il risarcimento del danno [41]Il Giudice però riteneva, nel merito, che l'art. 28, par. 7, BDSG fosse diretto a proteggere interessi diversi dalla leale concorrenza e, come tale, insuscettibile di rilevare ai fini del § 3a UWG.

---

[34] V. OLG Hamburg, Urt. v. 25.10.2018 – 3 U 66/17, ZD 2019, 33. [35] *Ibid.*, punti 1-2.
[36] *Ibid.*, punti 1 e 4.
[37] *Ibid.*, punti 7 e 56.

[38] *Ibid.*, punto 14.
[39] *Ibid.*, punto 26.
[40] *Ibid.*, punti 34-35.
[41] *Ibid.*, punti 36 e segg.

2.3. Rappresentanza degli interessati

[43] Ulteriore rimedio di natura privatistica è quello previsto all'art. 80 ,

rubricato «Rappresentanza degli interessati». Il primo paragrafo dell'articolo riconosce il diritto dell'interessato di dare mandato ad «un organismo, un'organizzazione o un'associazione senza scopo di lucro» (Ente) di esperire, per suo conto, i rimedi di cui agli artt. 79, par. 1, e 82[44]. All'interno dell'art. 80, par. 1, deve ritenersi inclusa anche l'ipotesi in cui più interessati diano mandato allo stesso Ente[45]. L'art. 80, par. 1, quindi contempla sia l'azione rappresentativa promossa per conto del singolo interessato sia l'azione collettiva promossa per conto di più interessati
Il secondo paragrafo dell'art. 80, prevede inoltre la possibilità per l'Ente di ricorrere ai sensi dell'art. 79, par. 1[47], indipendentemente dall'esistenza di un mandato conferito dall'interessato (o dagli interessati), ma senza far menzione della possibilità di agire per ottenere il risarcimento del danno ai sensi dell'art. 82.
I parr. 1 e 2 dell'art. 80 precisano che le possibilità ivi contemplate sussistono a condizione che le stesse siano riconosciute dall'ordinamento dello Stato membro del giudice adito.
L'ordinamento italiano riconosce entrambe le possibilità previste all'art. 80. In particolare, l'art. 10, co. 5, D.Lgs. 150/2011 – così come modificato dall'art. 17, D.Lgs. 101/2018 – prevede espressamente la possibilità per l'interessato di «dare mandato a un ente del terzo settore [...] che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione [...]». Per quanto concerne l'azione di classe, l'istituto è stato di recente riformato con L. 12.4.2019, n. 31[48] ed è ragionevole ritenere che i nuovi artt. 840-*bis* e 840-*sexdecies* c.p.c. permetteranno[49] all'Ente di esercitare l'azione collettiva inibitoria e risarcitoria ai sensi dell'art. 80, par. 1, per conto degli interessati, nonché di promuovere l'azione indipendentemente dall'esistenza di un mandato conferito dagli stessi interessati ai sensi dell'art. 80, par. 2, anche per il risarcimento del danno di cui all'art. 82.

---

[42] *Ibid.*, punto 56.

[43] L'art. è associato al consid. n. 142 e non trova precedenti nell'abrogata Dir. n. 95/46/CE.

[44] Oltre ai rimedi di natura amministrativa di cui agli artt. 77 e 78.

[45] Così suggerisce il consid. n. 142, nonché la stessa rubrica dell'art. 80.

[46] V., *inter alios*, *Agenzia dell'Unione europea per i diritti fondamentali*, Manuale sul diritto europeo in materia di protezione dei dati, ed. 2018, p. 271.

[47] Oltre ai rimedi di cui agli artt. 77 e 78.
[48] Disposizioni in materia di azioni di classe, G.U. 18.4.2019, n. 92 (ELI: https:// www.gazzettaufficiale.it/eli/gu/2019/04/18/92/sg/pdf).

[49] La riforma entrerà in vigore il 19.4.2020. Cf. art. 7, L. 31/2019. 7

Diversamente, in Germania, la UKlaG[50] si limita a consentire ad associazioni per la tutela dei consumatori di promuovere azioni inibitorie contro la violazione delle norme in materia di protezione dei dati personali[51].

3. Competenza internazionale

A fianco dei rimedi di natura privatistica, il RGDP introduce, all'art. 79, par. 2[52], una norma speciale sulla competenza internazionale in materia civile[53] che così recita: «Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.».

L'art. 79, par. 2, riflette, sul piano giurisdizionale, l'obiettivo di protezione [53] perseguito dal Regolamento . La norma infatti favorisce l'interessato, consentendogli di agire presso il "proprio" foro; davanti al giudice dello Stato membro in cui risiede abitualmente.

3.1. *«azioni»*

L'ambito d'applicazione oggettivo dell'art. 79, par. 2, è circoscritto alle [55] azioni esercitate contro le violazioni del RGPD : i ricorsi di cui all'art. 79, par. 1, incluse le azioni per il risarcimento del danno di cui all'art. 82[56]. Per quanto concerne quest'ultime, l'art. 82, par. 6, così recita: «Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2».

---

[50] Unterlassungsklagengesetz in der Fassung der Bekanntmachung v. 27.8.2002 (BGBl. 2002 I S. 3422, 4346), das zuletzt durch Artikel 4 des Gesetzes v. 17.6.2017 (BGBl. 2017 I S. 2446) geändert worden ist.

[51] V. § 2 Abs. 2 Nu. 11 UKlaG; trad. in: Conclusioni dell'Avvocato Generale Michal Bobek, presentate il 19.12.2018 – C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW e.V. con l'intervento di: Facebook Ireland Limited, Landesbeauftrage fur Datenschutz Informationsfreiheit Nordrhein-Westfalen*, punto 11.

[52] La norma è associata ai consid. nn. 145 e 147 e non trova precedenti nell'abrogata Dir. n. 95/46/CE.

[53] *Hess*, in: Schütze (n. 4), p. 258.
[54] V., *inter alios*, *Franzina*, in: De Franceschi (n. 4), pp. 97-98.

[55] V., *inter alios*, *Kreße*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 79 DSGVO Rn. 35.

[56] V. art. 82, par. 6.

L’art. 79, par. 2, non precisa quale sia l’elemento d’estraneità richiesto affinché possa trovare applicazione. L’elemento pare sussistere nel caso in cui l’interessato risieda abitualmente in uno Stato (non necessariamente uno Stato membro[57]) diverso da quello in cui il titolare abbia uno stabilimento; nonché nel caso in cui, pur trovandosi nello stesso Stato membro residenza abituale e stabilimento, il fatto generatore del danno o le sue conseguenze dannose abbiano luogo in un diverso Stato membro[58].

L’ambito d’applicazione soggettivo è determinato con riferimento all’identità del resistente: il titolare (o il responsabile del trattamento). Non è necessario che il titolare abbia uno stabilimento in uno Stato membro: il titolare dello Stato terzo può essere convenuto, in ogni caso, davanti al [59] giudice dello Stato membro in cui l’interessato abbia residenza abituale .

Piuttosto, ai fini dell’art. 79, par. 2, il titolare non deve essere un’autorità pubblica nell’esercizio dei suoi pubblici poteri[60].
L’art. 79, par. 2, invece non precisa l’identità del possibile ricorrente[61]. Non v’è dubbio questi possa essere l’interessato. Tuttavia, nel caso in cui l’interessato non risiedesse abitualmente in uno Stato membro, la norma offrirebbe un solo foro: il giudice dello Stato membro in cui il titolare abbia uno stabilimento. Invece, nel caso in cui neppure il titolare avesse uno [62] stabilimento in uno Stato membro, la norma non offrirebbe alcun foro .

Quest’ultima ipotesi infatti esula dall’ambito d’applicazione soggettivo della norma.
V’è da chiedersi se, oltre all’interessato, anche l’Ente di cui all’art. 80 possa promuovere l’azione davanti ai giudici individuati all’art. 79, par. 2. Come già esaminato:

- l’art. 79, par. 2, determina il proprio ambito d’applicazione soggettivo con riferimento all’identità del resistente, senza specificare espressamente l’identità del ricorrente;
- ’art. 80, par. 1, contempla l’ipotesi in cui l’Ente, per conto dell’interessato, faccia valere il diritto al risarcimento del danno di cui all’art. 82; e,
- l’art. 82, par. 6 specifica che tale diritto può essere fatto valere davanti ai giudici individuati all’art. 79, par. 2.

---

[57] L’interessato, per essere tale, non deve necessariamente risiedere abitualmente in uno Stato membro. Cf. art. 3, par. 2.
[58] Parzialmente diversa è la ricostruzione dell’elemento d’estraneità in *Marongiu Buonaiuti*, CDT 2017, 448, 450 punto 3.
[59] V., *inter alios*, diffusamente, *Marongiu Buonaiuti*, CDT 2017, 448, 453 punti 10 e segg. [60] Cf. consid. N. 145; *Brkan*, IDPL 2015, 257, 272-273.
[61] Il consid. n. 145 fa genericamente riferimento ai «ricorrenti».
[62] Cf. *Requejo Isidro* (n. 4), punto 4.1.1.

Alla luce del combinato disposto delle tre norme, la domanda può essere risposta affermativamente: anche l'Ente può rivolgersi ai giudici individuati all'art. 79, co. 2[63].
Eppure, nel caso in cui le cc.dd parti deboli decidessero di agire collettivamente, il privilegio giurisdizionale loro concesso potrebbe andare perduto; l'azione non potrebbe più essere esercitata davanti al loro foro. Così è stato affermato dalla Corte di giustizia, con riferimento alle norme sulla giurisdizione in materia di contratti conclusi da consumatori, oggi contenute agli artt. 17 e segg. del Reg. (UE) n. 1215/2012[64] (RB1*bis*). Da ultimo, nel caso *Schrems II*, la Corte ha infatti negato la possibilità di agire collettivamente presso il foro del consumatore, ritenendo che in tale foro possa agire soltanto il consumatore che sia «personalmente coinvolto come attore o convenuto in un giudizio»[65]. Certo, agendo tramite l'Ente, gli interessati non sarebbero "personalmente coinvolti". Ciononostante, come osservato, il tenore letterale degli artt. 79, par. 2, 80, par. 1 e 82, par. 6, consente di estendere la prima norma anche alle azioni promosse dagli Enti. Si può perciò dubitare che quanto la Corte ha affermato con riferimento agli artt. 17 e ss., RB1*bis*, possa valere anche per l'art. 79, par. 2, RGPD[66].

Ove lo si ritenesse dunque applicabile anche all'Ente, l'art. 79, par. 2, consentirebbe di promuovere l'azione collettiva, per conto di interessati- rappresentati residenti abitualmente nello stesso Stato membro, davanti ai giudici di tale Stato, oppure davanti ai giudici dello Stato membro in cui il titolare abbia uno stabilimento[67]. Invece, nella diversa ipotesi di interessati residenti abitualmente in Stati membri diversi, l'Ente potrebbe avere a disposizione soltanto i giudici dello Stato membro in cui si trovi lo stabilimento del titolare. E ciò perché, in quest'ultima ipotesi, i giudici dello Stato membro in cui risiedono abitualmente alcuni interessati potrebbero difettare di giurisdizione con riferimento alle pretese della restante parte di interessati[68].

---

[63] Cf., *inter alios*, *Feiler/Forgó/Weigl*, The EU General Data Protection Regulation (GDPR): a commentary, 1st edn. 2018, Art. 79 GDPR mn. 5 ed Art. 80 GDPR mn. 1.

[64] Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, G.U.U.E. L 351/1, 20.12.2012 (ELI: http://data.europa.eu/eli/reg/2012/1215/oj).

[65] C.G.U.E., sent. 25.1.2018 – C-498/16, *Maximilian Schrems c. Facebook Ireland Limited*, Racc., ECLI:EU:C:2018:37, punto 45.

[66] Cf. *Wolters, Pieter*, The Enforcement by the Data Subject Under the GDPR, Vol. 22 No. 8 J. Internet L. 2019, 1, 26.

[67] Cf. *Pato* (n. 4), punto 3.4; *Wolters,* J. Internet L. 2019, 1, 26.

[68] Sulle considerazioni che precedono, seppur con riferimento alle norme sulla giurisdizione del RB1*bis*, cf. *Lein*, *Eva*, Cross-Border Collective Redress and Jurisdiction under Brussels I: A Mismatch, in: Fairgrieve, Duncan/Lein, Eva (eds.), Extraterritoriality and Collective Redress, 2012, mn. 8.17 e 8.18.

Ciò detto, per quanto concerne l'ordinamento italiano, nulla sembrerebbe escludere la possibilità di esercitare azioni collettive ai sensi dell'art. 80, aventi carattere "transfrontaliero"[69]. Un ostacolo potrebbe però essere rappresentato dalla mancanza del requisito dell'omogeneità di cui all'art. 840-*bis* c.p.c., alla quale segue la dichiarazione di inammissibilità dell'azione ai sensi dell'art. 840-*ter*, co. 3, lett. b), c.p.c. Infatti. per l'operare delle norme di diritto internazionale privato, le pretese dei singoli rappresentati potrebbero essere rispettivamente governate dal diritto di ordinamenti di Stati diversi, il che – secondo alcuni – potrebbe escludere l'omogeneità delle stesse pretese. Eppure, nella specifica ipotesi dell'azione di classe ai sensi degli artt. 80, par. 1, e 82, le pretese degli interessati- rappresentati non sarebbero, a rigore, fondate sul diritto di Stati diversi, quanto piuttosto sulla stessa norma: l'art. 82, il quale – come esaminato sopra – introduce una norma di diritto materiale uniforme in tutti gli Stati membri. Si potrebbe dunque ritenere che l'eventuale carattere transfrontaliero dell'azione di classe promossa ai sensi degli artt. 80, par. 1, e 82 non escluda, di per sé, il requisito dell'omogeneità richiesto dall'art. 840-*bis* c.p.c.[70].

Infine, ritenendo che, oltre all'interessato ed agli Enti, anche soggetti terzi possano agire per ottenere il risarcimento del danno di cui all'art. 82, non si può escludere che anche tali soggetti terzi possano rivolgersi ai giudici individuati all'art. 79, par. 2.

3.2. *«autorità giurisdizionali»*

L'art. 79, par. 2, consente di agire davanti ai giudici dello Stato membro in cui si trovi lo stabilimento del titolare, oppure, in alternativa, davanti ai giudici dello Stato membro in cui l'interessato risieda abitualmente. Delle nozioni di stabilimento e residenza abituale, va data un'interpretazione [71] autonoma .

Ai fini del primo periodo dell'art. 79, par. 2, per stabilimento non si intende quello principale di cui all'art. 4, n. 16, ma, semplicemente, «uno» [72] [73]stabilimento . Secondo l'orientamento maggioritario , ai fini dell'art. 79,

---

[69] Se si ammettesse che l'azione di classe *ex* art. 80 possa essere esperita davanti ai giudici dello Stato membro di residenza abituale degli interessati-rappresentati ai sensi dell'art. 79, par. 2, secondo periodo, RGPD, in Italia si porrebbe un problema di coordinamento con la disciplina sulla competenza (interna) di cui all'art. 840-*ter* c.p.c. La norma del c.p.c. infatti individua quale giudice competente per l'azione di classe (soltanto) la «sezione specializzata in materia di impresa competente per il luogo ove ha sede la parte resistente».

[70] Sulle considerazioni che precedono, cf. *Malatesta/Vitellino*, Italy, in: Parlamento europeo, Dipartimento tematico Diritti dei cittadini e affari costituzionali, Collective redress in the Member States of the European Union, 2018, pp. 188 e segg. ed ivi i riferimenti alle nn. 574 e 577, in particolare, rispettivamente, v. *Stadler, Astrid*, The Commission's Recommendation on Common Principles of Collective Redress and Private International Law, in: Lein/Fairgrieve/Crespo Otero/Smith, Collective Redress in Europe – Why and How?, 2015, pp. 207 ss; e, seppur con riferimento all'abrogato art. 140-bis, co. 4, cod. cons., *Bariatti, Stefania*, Le azioni collettive dell'art. 140-*bis* del Codice del consumo: aspetti di diritto internazionale privato e processuale, Riv. dir. int. priv. proc. 2011, 1, 27 e segg. e 42-43.

[71] V. rispettivamente, *Franzina*, in: De Franceschi (n. 4), p. 99; *Martini*, in: Paal/Pauly (n. 8) Art. 79 DSGVO Rn. 28.

[72] V., *inter alios*, *Albrecht/Jotzo* (Hrsg.), Das neue Datenschutzrecht der EU, 1. Aufl. 2017,

[73] V., *inter alios*, *Boehm*, in: *Simitis/Hornung/Spiecker* (Hrsg.), Datenschutzrecht, 1. Aufl. 2019, Art. 79 DSGVO Rn. 18.

par. 2, occorre far riferimento alla giurisprudenza della Corte di giustizia sulla Dir. n. 95/46/CE. Infatti, la Corte si è più volte pronunciata adottando una concezione ampia, o meglio «flessibile» di stabilimento di cui al considerando n. 19, Dir. n. 95/46/CE[74], oggi riprodotto al considerando n. 22 RGPD. Secondo il Giudice europeo, in breve, stabilimento non è soltanto quello in cui il trattamento illecito abbia avuto luogo[75], ma anche quello in cui siano state condotte attività «inscindibilmente connesse» al trattamento[76]. Un esempio è quello dello stabilimento che si limiti a svolgere attività di promozione dei servizi del titolare, nel cui ambito sia avvenuto il trattamento illecito[77]. Così, nel caso in cui il titolare abbia più stabilimenti, lo stabilimento di cui all'art. 79, par. 2, secondo periodo, RGPD, potrebbe essere diverso da quello in cui sia stato compiuto il fatto generatore del danno (cf. *Fig. 1*).

Il secondo periodo dell'art. 79, par. 2 – come esaminato sopra – assicura, all'interessato che abbia residenza abituale in uno Stato membro, la possibilità di citare il titolare davanti al giudice di uno Stato membro, in ogni caso, anche quando il titolare non abbia uno stabilimento all'interno dell'Unione. Il Regolamento non spiega cosa debba intendersi per «residenza abituale», di cui peraltro manca una definizione unitaria nel diritto dell'Unione. La Corte di giustizia ha però pronunciato massime di carattere generale, che possono fare da guida, ad esempio: «[l]a residenza abituale è il luogo in cui l'interessato ha fissato, con voluto carattere di stabilità, il centro abituale o permanente dei propri interessi»[78].

3.3. Specialità

L'art. 79, par. 2 si pone in rapporto di specialità rispetto alle norme sulla giurisdizione contenute nel già citato RB1*bis* Teil 8 Rn. 29 n. 43; *contra*, *Lundstedt* (n. 4), pp. 246-247. [79] La norma del RGPD infatti ripartisce la giurisdizione, tra i giudici degli Stati membri, in ipotesi di azioni esercitate contro la violazione dello stesso Regolamento, mentre il RB1*bis* trova applicazione con riferimento ad azioni in materia civile (e commerciale) [80]

---

[74] Cf. C.G.U.E., Fashion ID, punti 64 e segg; sent. 14.5.2014 – C-131/12, Google Spain SL e Google Inc. c. Agencia Española de Protectión de Datos (AEPD) e Mario Costeja Gonzáles, Racc., ECLI:EU:C:2014:317, punto 49; 1.10.2015 – C-230/14, Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabaság Hatóság, Racc., ECLI:EU:C:2015:639, punti 32 e segg.; 5.6.2018 – C-210/16, Unabhängiges Landeszentrum für Datenschtuz Schleswig- Holstein c. Wirstschaftsakademie Schleswig-Holstein GmbH, Racc., ECLI:EU:C:2018:388, punti 54 e segg.

[75] Cf. C.G.U.E., *Google Spain*, punto 52 e *Wirtschaftsakaedmie*, punto 57.
[76] V. C.G.U.E., *Google Spain*, punti 51 e segg. e *Wirtschaftsakademie*, punto 60. [77] *Ibid.*

[78] Tribunale di primo grado, sent. 25.10.2005 – T-298/02, *Anna Herrero Romeu c. Commissione*, Racc. 2005 II-04599, ECLI:EU:T:2005:369, punto 51, citato da *Franzina*, in: De Franceschi (n. 4), p. 102 ed ivi n. 49.

[79] V. n. 64.

[80] Cf., *inter alios*, *Lundstedt* (n. 4), p. 243.

Anche l'ambito di applicazione soggettivo dell'art. 79, par. 2, è più ristretto: la norma si applica in ipotesi di azioni esercitate ai danni di titolari; mentre, in linea di principio, il RB1*bis* si applica a prescindere dall'attività esercitata dal convenuto. Benché il RGPD non disciplini espressamente il proprio rapporto con il RB1*bis*, il considerando n. 147 RGPD contiene una clausola di conflitto che riprende quella di cui all'art. 67 RB1*bis*, così formulato: «Il presente regolamento non pregiudica l'applicazione delle disposizioni che, in materie particolari, disciplinano la competenza [...] e che sono contenute negli atti dell'Unione [...]». Le norme del RGPD quindi superano quelle del RB1*bis*, allorché la contestuale applicazione delle seconde possa pregiudicare l'applicazione delle prime[81] .
Una simile situazione di pregiudizio ha luogo quando la contestuale applicazione delle norme del RB1*bis* impedirebbe all'attore di rivolgersi ai giudici individuati all'art. 79, par. 2, RGPD, compromettendo così il favore che la norma accorda all'attoread esempio, con una clausola di scelta del foro esclusiva *ex* art. 25 RB1*bis* si pretenda di derogare la giurisdizione dei giudici individuati all'art. 79, par. 2, RGPD[83].
Sul punto si è pronunciata la Commercial Court dell'Inghilterra e del Galles, il 12.4.2019, nel caso *Ramona v. Rielantco*[84] – la prima pronuncia (nota) sull'art. 79, par. 2, RGPD. In quel caso, la Sig.ra Ang, una casalinga inglese [85] con residenza abituale in Inghilterra , creava un *account* sulla piattaforma di *trading online* UFX, dove poi investiva i propri risparmi in *Bitcoin futures*[86]. L'impresa gerente la piattaforma, la società cipriota Rielantco, chiudeva l'*account* della Sig.ra Ang, i cui investimenti andavano così in [87] fumo . La Sig.ra quindi agiva davanti al giudice inglese, chiedendo di[82] .

Questa è la situazione in cui, [88] essere indennizzata della (asserita) perdita (di oltre 3.000.000 USD) .

---

[81] V., *inter alios*, *Feiler/Forgó/Weigl* (n. 63), Art. 79 GDPR mn. 7.

[82] Più in generale, una situazione di pregiudizio potrebbe ravvisarsi in tutti i casi in cui le norme del RB1*bis* contraddicano o ledano l'integrità o la coerenza del regime speciale approntato dal RGPD. V. *Franzina*, in: De Franceschi (n. 4), p. 104.

[83] V., *ex plurimis*, *Kohler*, Riv. dir. int. priv. proc. 2016, 653, 669. [84] *Ramona v. Rielantco* [2019] EWHC 879 (Comm).
[85] *Ibid.*, punti 5, 8 e 85.
[86] *Ibid.*, punti 14-15.

[87] *Ibid.*, punto 16.

[88] *Ibid.*, punto 15.

L'attrice chiedeva inoltre la rettifica e la cancellazione dei propri dati [89] personali ancora in possesso della Rielantco . La convenuta eccepiva il difetto di giurisdizione sulla scorta di una clausola esclusiva di scelta del foro cipriota *ex* art. 25 RB1*bis*, accettata dall'attrice mentre creava (*online*) il suo *account* UFX[90]. La Commercial Court riteneva che la Sig.ra Ang fosse qualificabile come consumatrice e, di conseguenza, riteneva che la [91] clausola di scelta del foro non le fosse opponibile (*ex* art. 17 RB1*bis*) . In ogni caso – aggiungeva il Giudice –, alla luce dell'art. 67 RB1*bis*, la clausola non avrebbe potuto distogliere la domanda di rettifica e cancellazione dei dati personali dalla giurisdizione del giudice anglo- gallese, (internazionalmente) competente ai sensi dell'art. 79, par. 2, primo periodo, RGPD[92].

In assenza di una siffatta situazione di pregiudizio, si ritiene che il RB1*bis* ed il RGPD possano applicarsi contestualmente[93], o meglio che i due regimi normativi debbano essere integrati/coordinati tra loro.

4. *(continua)* in ambiente *online*

Come si realizza, in concreto, l'integrazione/il coordinamento dell'art. 79, par. 2, RGPD con il RB1*bis*, è in seguito esaminato con specifico riferimento alle azioni connotate dall'elemento d'estraneità ed esercitate contro il titolare per ottenere il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*.

Con questa formula, "ambiente *online*", si allude all'ipotesi in cui il fatto generatore del danno, piuttosto che le sue conseguenze dannose, coinvolgano l'uso di Internet. Lo scenario più ricorrente sembra essere quello in cui il titolare gerente un sito – spesso un *social network* – illecitamente raccolga, trasmetta o riveli a terzi dati personali, con pregiudizio per un ampio numero di interessati. A meno che tra il titolare e gli interessati esista un contratto e la violazione del Regolamento possa quindi integrare un inadempimento contrattuale[94], il ristoro del danno sofferto dagli interessati-danneggiati può avvenire secondo le regole della responsabilità extracontrattuale, così come espressamente previsto all'art. 82 RGPD.

Quando sussista l'elemento d'estraneità ed occorra quindi determinare quale giudice, tra i giudici degli Stati membri, sia (internazionalmente) competente a conoscere simili azioni risarcitorie, oltre all'art. 79, par. 2, RGPD, "entrano in gioco" anche gli artt. 4, par. 1, e 7, nn. 2 e 5 RB1*bis*.

---

[89] *Ibid.*, punto 1.
[90] *Ibid.*, punti 2, 19 e 20. [91] *Ibid*., punti 13 e 70.
[92] *Ibid.*, punti 85 e 90.

[93] V. *inter alios*, *Werkmeister*, in: Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 79 DSGVO Rn. 15; *Hess*, in: Schütze (n. 4), p. 259; *Kohler,* Riv. dir. int. priv. proc. 2016, 653, 669.

[94] V. *Lundstedt* (n. 4), p 229 punto 2.2.; *Brkan*, IDPL 2015, 257, 266.

4.1. Norme del RB1*bis*

L'art. 4, par. 1, RB1*bis* consente di convenire in giudizio la persona domiciliata nello Stato membro, davanti ai giudici di quello stesso Stato. Ai sensi dell'art. 63 RB1*bis*, la persona giuridica «è domiciliata nel luogo in cui si trova: la sua sede statutaria; la sua amministrazione centrale; oppure, il suo centro d'attività principale». In virtù dell'art. 5, par. 1, RB1*bis*, nel caso in cui il convenuto sia domiciliato in uno Stato membro, l'attore può agire, anziché davanti al foro generale di cui all'art. 4, par. 1, davanti ai cc.dd. fori alternativi[95]. Secondo il considerando n. 16, al fine di garantire certezza del diritto e prevedibilità del foro, i fori alternativi dovrebbero basarsi sul «collegamento stretto tra l'autorità giurisdizionale e la controversia [...] aspetto [...] importante nelle controversie in materia di obbligazioni extracontrattuali derivanti da violazioni della privacy e dei diritti della personalità, compresa la diffamazione». Nel caso di simili controversie, i fori alternativi sono quelli di cui ai nn. 2 e 5 dell'art. 7 RB1*bis*. L'art. 7, n. 2, RB1*bis* conferisce giurisdizione in materia extracontrattuale in capo al giudice dello Stato membro «del luogo in cui l'evento dannoso è avvenuto o può avvenire». Sin dal caso *Mines de potasse*, la Corte di giustizia ha interpretato la formula dell'art. 7, n. 2, RB1*bis* seguendo il "principio dell'ubiquità": il danneggiato può agire davanti al giudice dello Stato membro del luogo del fatto generatore del danno, oppure, in alternativa, davanti al giudice dello Stato membro del luogo di concretizzazione del danno[96].

Nel caso *eDate*[97], la Corte ha dato una particolare interpretazione dell'art. 7, par. 2, RB1*bis*, con riferimento alle azioni per il risarcimento del danno derivante dalla violazione dei diritti della personalità per mezzo di contenuti [98] caricati *online* . Seguendo questo orientamento, il danneggiato può agire davanti ai giudici dello Stato membro dove si trovi:

---

[95] Cf. consid. n. 16 RB1*bis*.
[96] C.G.C.E., sent. 30.11.1977 – C-21/76, *Handelskwekerij G. J. Bier BV c. Mines de*

potasse d'Alsace SA, Racc. 1976 01735, ECLI:EU:C:1976:166, punto 25.
[97] C.G.U.E., sent. 25.10.2011 – C-509/09 e C-161/10, *eDate Advertising GmbH e a. c. X e*

Société MGN LIMITED, Racc. 2011 I-10269, ECLI:EU:C:2011:685.

[98] L'orientamento è stato mutuato da C.G.C.E., sent. 7.3.1995 – C-68/93, *Fiona Shevill e a. c. Presse Alliance SA*, Racc. 1995 I-00415, ECLI:EU:C:1995:61; confermato in C.G.U.E., sent. 17.10.2017 – C-194/16, *Bolagsupplysningen OÜ e Ingrid Ilsjan c. Svensk Handel AB*, Racc., ECLI:EU:C:2017:766; e, recepito dalla giurisprudenza italiana, da ultimo, in Trib. Bologna, Sez. III, sent. 1.3.2019, Leggi d'Italia.

- 1) lo stabilimento del danneggiante dal quale il contenuto

sia stato caricato *online*; Stabilimento del caricamento

- 2) il centro degli interessi del danneggiato; Centro degli interessi

oppure

- 3) il luogo in cui il contenuto sia o

sia stato accessibile *online*. Luogo di accessibilità

In merito ai tre punti di collegamento, si osserva quanto segue:

- 1) lo stabilimento del caricamento coincide con il luogo del fatto generatore del danno e, soltanto tendenzialmente, con il domicilio del danneggiante-convenuto[99];

- 2) il centro degli interessi coincide con il – o meglio, è racchiuso all'interno del – luogo di concretizzazione del danno[100] e tendenzialmente coincide con la residenza abituale del danneggiato- attore[101];

- 3) il luogo di accessibilità racchiude e tendenzialmente coincide con il luogo di concretizzazione del danno[102]; e, virtualmente, coincide con il territorio di ciascuno Stato membro[103] (cf. *Fig. 1*).

---

[99] V. C.G.C.E., *Shevill*, rispettivamente, punti 24 e 26.

[100] Cf. C.G.U.E., *Svensk Handel*, punto 33.

[101] V. C.G.U.E., *eDate*, punto 49 e v. anche C.G.U.E., *Svensk Handel*, punto 40-42.

[102] Cf. C.G.C.E., *Shevill*, punto 28-29 e cf. anche C.G.U.E., *eDate*, punto 51.

[103] V. Conclusioni dell'Avvocato Generale Michael Bobek, presentate il 13.7.2017 – C-194/16, *Bolagsupplysningen OÜ e Ingrid Ilsjan c. Svensk Handel AB*, punti 32 e 78.

La Corte di giustizia ha introdotto un temperamento alla "ploriferazione" di fori sopra descritta, adottando l'approccio "a mosaico": i giudici dello Stato membro del domicilio del convenuto, dello stabilimento del caricamento e del centro degli interessi possono conoscere della totalità del danno (cd. "foro pieno")[104]; diversamente, i giudici dello Stato membro del luogo di accessibilità sono competenti soltanto per il pregiudizio sofferto sul territorio del proprio Stato (cd. "foro parziale")[105] (cf. *Fig. 1*).

Oltre ai fori individuati agli artt. 4, par. 1, e 7, n. 2, il RB1*bis* sembra offrire al danneggiato-attore un ulteriore foro: quello dell'art. 7, n. 5. L'art. 7, n. 5, RB1*bis* consente al danneggiato di agire davanti al giudice dello Stato membro del luogo in cui si trovi la succursale, agenzia o altra sede succursale del danneggiante, allorché il danneggiante sia domiciliato in un altro Stato membro e l'illecito sia riferibile all'esercizio di tale succursale, agenzia o altra sede. A ben vedere però, in ipotesi di violazione dei diritti della personalità *online*, l'art. 7, n. 5, RB1*bis* non offre al danneggiato un ulteriore foro rispetto a quelli già resi disponibili dal n. 2 dello stesso articolo; in simili ipotesi, il punto di collegamento posto dall'art. 7, n. 5, RB1*bis* sembra coincidere con quello dello stabilimento del caricamento (cf. *Fig. 1*).

Infine, benché il RB1*bis* non contenga norme espressamente dedicate all'azione di classe, si ritiene che questa possa essere portata anche davanti ai fori di cui agli artt. 4, par. 1, 7, n. 2[106] e 5[107].

4.2. Raffronto

Nel raffrontare l'art. 79, par. 2, RGPD con gli artt. 4, par. 1 e 7, nn. 2 e 5, si osserva, anzitutto, una significativa differenza nell'ambito d'applicazione soggettivo: diversamente dalla norma del RGPD, le predette norme del RB1*bis* trovano applicazione soltanto nei casi in cui il convenuto sia domiciliato in uno Stato membro.

Nell'ipotesi in cui il titolare-danneggiante sia dunque domiciliato in uno Stato membro, mutuando la giurisprudenza *eDate*, l'attore-danneggiato potrebbe esercitare l'azione per il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*, davanti ai giudici dello Stato membro dove si trovi:

1) il domicilio del titolare;

2) lo stabilimento del titolare dal quale siano stati caricati – o meglio, trasmessi o rivelati – *online* i dati personali dell'interessato[108];

---

[104] Per il domicilio del convenuto, v. C.G.C.E., *Shevill*, punto 32 e v. anche C.G.U.E., *eDate*, punto 43; per lo stabilimento del caricamento, v. C.G.U.E., *eDate*, punto 52 e cf. C.G.C.E., *Shevill*, punto 26 e 32; e, per il centro degli interessi, v. C.G.U.E., *eDate*, punto 48 e v. anche C.G.U.E., *Svensk Handel*, punto 32.

[105] V. C.G.U.E. *eDate*, punto 51 e cf. C.G.C.E., *Shevill*, punto 30.

[106] V. C.G.C.E. sent. 1.10.2002 – C-167/00, *Verein für Konsumenteninformation c. Karl Heinz Henkel*, Racc. 2002 I-08111, ECLI:EU:C:2002:555, punti 42 e 48.

[107] Sull'azione di classe ed il RB1*bis*, v., *inter alios*, *Parlamento europeo, Dipartimento tematico Diritti dei cittadini e affari costituzionali*, Collective redress in the Member States of the European Union, 2018, pp. 97 e segg.

[108] Punto di collegamento che sembra coincidere con quello del luogo della succursale, agenzia o altra sede di cui all'art. 7, n. 5, RB1*bis*.

3) il centro degli interessi dello stesso danneggiato; oppure,

4) il luogo in cui i dati siano (o siano stati) accessibili *online*[109].

A questi 4 fori, si "aggiungono" i 2 fori individuati all'art. 79, par. 2, RGPD: i giudici dello Stato membro dove si trovi:

5) lo stabilimento del titolare; oppure,

6) la residenza abituale dell'interessato.

A ben vedere, i 2 fori dell'art. 79, par. 2, RGPD non si aggiungono ma si "sovrappongono" ai 4 fori del RB1*bis*; i primi infatti tendono a coincidere con i secondi[110] (cf. *Fig. 1*).

In dettaglio, il punto di collegamento dello stabilimento del titolare di cui all'art. 79, par. 2, primo periodo, RGPD, racchiude e tendenzialmente coincide con il punto di collegamento:

- del domicilio del convenuto di cui all'art. 4, par. 1, RB1*bis*;

- del luogo dell'agenzia, succursale o altra sede di cui all'art. 7, n. 5, RB1*bis*;

- del luogo del fatto generatore del danno; e, nella specie,

- dello stabilimento del caricamento *ex* art. 7, n. 2, RB1*bis*[111].

---

[109] La Corte di giustizia ha evocato il punto di collegamento del luogo di accessibilità anche in materia di protezione di dati personali, in C.G.U.E., *Google Spain*, punto 80.

[110] Cf. *Hess*, in: Schütze (n. 4), p. 259.

[111] Sul raffronto del punto di collegamento dello stabilimento di cui all'art. 79, par. 2, RGPD con quello del domicilio del convenuto di cui all'art. 4, par. 1, RB1*bis*, v., *inter alios*, *Pato* (n. 4), punto 3.2; del luogo della succursale, agenzia o altra sede di cui all'art. 7, n. 5, RB1*bis*, v., *inter alios*, *Lundstedt* (n. 4), p. 236-237; e, del luogo del fatto generatore del danno, v. *Marongiu Buonaiuti*, CDT 2017, 448, 451 punto 9.

Invece, il punto di collegamento della residenza abituale di cui all'art. 79, par. 2, secondo periodo, RGPD, tende a coincidere con il punto di collegamento:

- del luogo di concretizzazione del danno; e, nella specie,

- del centro degli interessi dell'interessato *ex* art. 7, n. 2, RB1*bis*

Soltanto il punto di collegamento dello Stato membro di accessibilità sembra essere "esorbitante" rispetto ai punti di collegamento di cui all'art. 79, par. 2, RGPD.
In concreto, quindi, in ipotesi di azioni per il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*, i fori dell'art. 79, par. 2, si sovrappongono a quelli del RB1*bis*.

4.3. Integrazione/coordinamento

Dal raffronto emerge come gli artt. 4, par. 1 e 7, nn. 2 e 5, RB1*bis* non pregiudichino l'applicazione dell'art. 79, par. 2, RGPD. Le predette norme del RB1*bis* non precludono infatti la possibilità per l'attore di rivolgersi ai giudici individuati dal RGPD.
Eppure, certa dottrina si esprime in senso sfavorevole alla contestuale applicazione degli artt. 79, par. 2, RGPD e 7, n. 2, RB1*bis*. In particolare, un autore ritiene che, seguendo la giurisprudenza *eDate*, la contestuale applicazione accorderebbe all'attore un *«unreasonably overextended jurisdictional privilege»*. Affermazioni di questo tenore non convincono. A parere di chi scrive, in concreto, nella maggior parte dei casi,

---

[112] Sul raffronto del punto di collegamento della residenza abituale di cui all'art. 79, par. 2, RGPD con quello del luogo di concretizzazione del danno, v., *inter alios*, *Hess*, in: Schütze (n. 4), p. 259; e, con quello del centro degli interessi del danneggiato, v., *inter alios*, *de Miguel Asensio*, REDI 2017, 75, 98 punto 42.

[113] La contestuale applicazione dell'art. 7, n. 2, RB1*bis* è ammessa, *inter alios*, da *Werkmeister*, in: Gola (n. 93), Art. 79 DSGVO Rn. 15, *Hess*, in: Schütze (n. 4), p. 261 e da *Kohler*, Riv. dir. int. priv. proc. 2016, 653, 672-673; è invece escl usa da *Marongiu Buonaiuti*, CDT 2017, 448, 453 punto 9 n. 13, *Revolidis*, MUJLT 2017, 7, 23 e da *Franzina*, in: De Franceschi (n. 4), p. 105.

[114] V. *Revolidis*, MUJLT 2017, 7, 23.

l'applicazione contestuale degli artt. 79, par. 2, RGPD e 7, n. 2, RB1*bis*, non rischia di concedere all'attore un vantaggio *«unreasonaly overextended»*. Il rischio è mitigato:

- dal rapporto di tendenziale coincidenza tra i fori individuati agli artt. 79, par. 2, RGPD e 7, n. 2, RB1*bis*;

- nel caso in cui il titolare abbia più stabilimenti, dalla difficoltà che l'attore potrebbe incontrare nell'individuazione, in concreto,

dello stabilimento nel quale sia stata svolta un'attività

«inscindibilmente connessa» all'illecita rivelazione o trasmissione *online* di dati personali (ai fini dell'art. 79, par. 2, [115] primo periodo, RGPD) , nonché dello stabilimento dal quale siano stati illecitamente trasmessi o rivelati *online* i dati personali (ai fini dell'art. 7, n. 2, RB1*bis*); e,

- dall'approccio "a mosaico" che rende meno "conveniente" rivolgersi ai giudici dello Stato membro di accessibilità ai sensi dell'art. 7, n. 2, RB1*bis*.

Non sussiste dunque alcuna decisiva ragione per escludere la contestuale applicazione degli artt. 79, par. 2, RGPD e 7, n. 2, RB1*bis*, nonché 4, par. 1, e 7, n. 5 dello stesso RBb1*bis*.
Più dubbia è invece la possibilità di estendere l'approccio "a mosaico" all'art. 79, par. 2, RGPD, e cioè nelle ipotesi in cui:

- lo Stato membro dello stabilimento del titolare-convenuto non sia quello del domicilio dello stesso titolare e neppure quello dello stabilimento del caricamento; oppure,

- lo Stato membro della residenza abituale dell'interessato non sia quello del centro degli interessi dello stesso interessato.

Secondo l'orientamento dottrinale prevalente, i giudici individuati all'art. 79, par. 2, RGPD, dovrebbero essere considerati, in ogni caso, "fori pieni", sempre competenti a conoscere della totalità del danno[116] (cf. *Fig. 1*). In effetti, se così non fosse, l'estensione dell'approccio "a mosaico" potrebbe contraddire l'obiettivo perseguito dal RGPD di favorire l'attore.

---

[115] V. *Franzina*, in: De Franceschi (n. 4), p. 100.

[116] La possibilità è esclusa da *Hess*, in: Schütze (n. 4), p. 261, *Lundstedt* (n. 4), p. 253-254 e da *de Miguel Asensio*, REDI 2017, 75, 100 punto 45; e, non è invece esclusa da *van Calster*, Obs. Bxl. 2018, 28, 29.

[117] Cf., *inter alios*, *Lundstedt* (n. 4), p. 253-254.

5. Osservazioni conclusive

Da un lato, il RGPD non assicura un livello di tutela uniforme all'interno dell'Unione. Infatti, ad esempio, i provvedimenti adottati all'esito di un ricorso giurisdizionale ai sensi dell'art. 79, par. 1, potrebbero essere disponibili in uno Stato membro, ma non in un altro; i criteri di liquidazione del danno di cui all'art. 82 potrebbero essere più "generosi" in uno Stato membro e meno in un altro; in uno Stato membro l'Ente di cui all'art. 80 potrebbe promuovere l'azione, ma non anche in un altro Stato membro. Dall'altro lato, l'art. 79, par. 2, consente un margine di *forum shopping*. Tale margine è aumentato per effetto della contestuale applicazione delle norme giurisdizionali del RB1bis, specie in ipotesi di azioni per il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*. L'aumento del margine di *forum shopping* è tutto sommato contenuto se si considera come i punti di collegamento di cui all'art. 79, par. 2, RGPD tendano a coincidere con quelli di cui al RB1bis.

In ogni caso, manovre di *forum shopping* potrebbero essere incoraggiate proprio dalla mancanza di un livello di tutela uniforme all'interno dell'Unione. Tali manovre possono essere condotte dal singolo interessato, nonché dall'Ente di cui all'art. 80 RGPD. In particolare, l'Ente potrebbe sfruttare il margine di *forum shopping* dell'art. 79, par. 2, RGPD aumentato dalla contestuale applicazione delle norme giurisdizionali del RB1*bis*, per "convogliare" le pretese di interessati, residenti abitualmente in diversi Stati, davanti ai giudici di un unico Stato membro, il cui ordinamento consenta di esercitare l'azione ai sensi dell'art. 80 RGPD.

Di tutto ciò sembra essere consapevole il pioniere della cd. *data protection litigation* in Europa, il Dr. Schrems, il quale ha di recente fondato l'ONG NOYB. Come si legge al punto 2.2. del «Public Project Summary»[118] della ONG austriaca: «Article 80 can be used to form "group actions" or "collective complaints", if a large number of users [*sic*] are represented by NOYB ("mass mandate"). *This option also allows to choose favorable jurisdictions*[119]. Subject to national law, member states can also grant NGOs the right to [...] sue independent from a mandate by an individual data subject ("abstract lawsuit"). *This option will not be available in Austria, but NOYB could set up a subsidiary in a member state that will allow abstract lawsuists*[120]»[121].

---

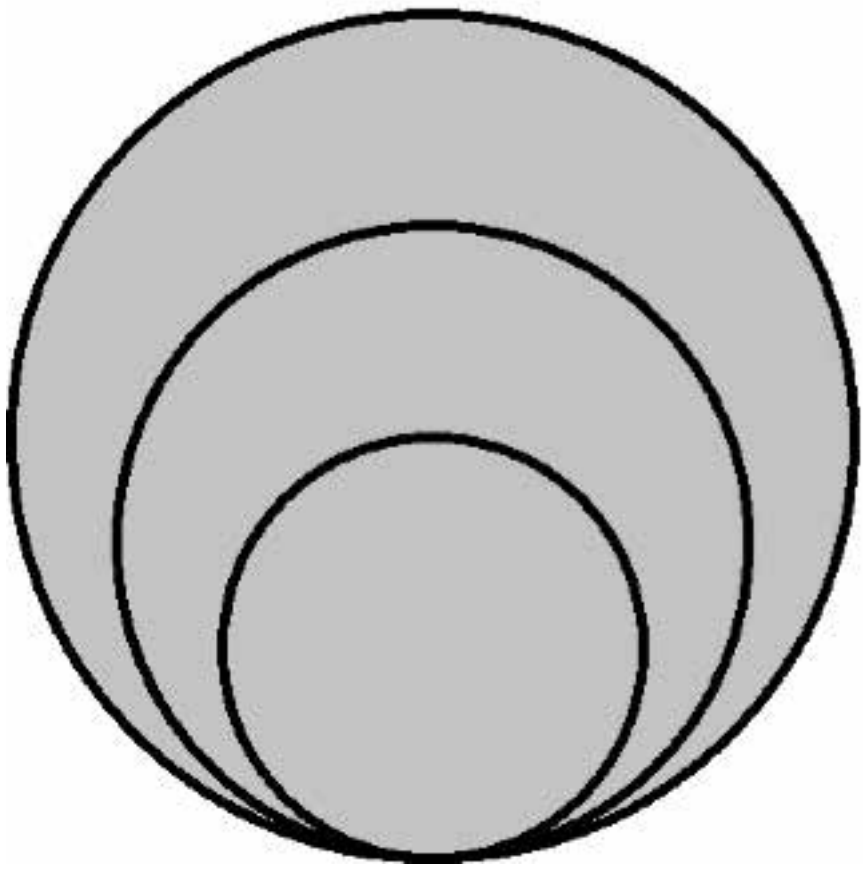
[118] Disponibile al seguente indirizzo *web*: https://noyb.eu/wp-content/uploads/2017/11/ concept_noyb_public.pdf.

[119] Cors. agg.

[120] Cors. agg.

[121] Trad. dell'a.: «L'articolo 80 può essere utilizzato per instituire "azioni di gruppo" o "ricorsi collettivi", allorché un ampio numero di utenti fossero rappresentati da NOYB ("mandato di massa"). Questa possibilità consentirebbe, tra l'altro, di scegliere giurisdizioni favorevoli. A seconda della legge nazionale, gli stati membri possono altresì garantire alle ONG il diritto di [...] agire in giudizio a prescindere dal mandato del singolo interessato ("azione astratta"). Questa possibilità non sarà disponibile in Austria, ma NOYB potrebbe costituire una sussidiaria in uno stato membro che consenta le azioni astratte».

Fig. 1 – Punti di collegamento in ipotesi di azioni per il risarcimento del danno derivante dalla violazione del RGPD in ambiente *online*.



Stabilimento del titolare (art. 79, par. 2, primo periodo, RGPD)

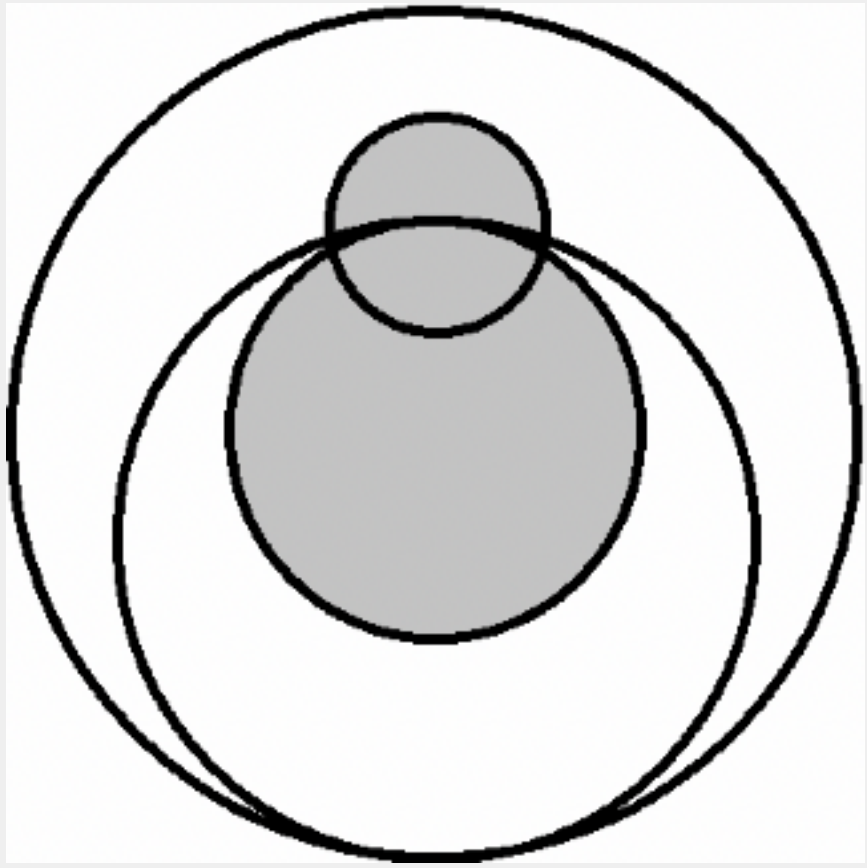
Luogo del fatto generatore del danno (art. 7, n. 2, RB1*bis* – *Mines de potasse*)

Stabilimento del caricamento (art. 7, n. 2, RB1*bis* - *eDate*)

Luogo della succursale, agenzia o altra sede

(art. 7, n. 5, RB1*bis*) Domicilio del convenuto

(art. 4, par. 1, RB1*bis*)



Luogo di accessibilità (art. 7, n. 2, RB1*bis* – *eDate*)

Residenza abituale dell'interessato (art. 79, par. 2, secondo periodo, RGPD)

Centro degli interessi (art. 7, n. 2, RB1*bis* – *eDate*)

Luogo di concretizzazione del danno (art. 7, n. 2, RB1*bis* – *Mines de potasse*)

Grigio: "foro pieno".

Bianco: "foro parziale".

SPONSORED BY

ASSOCIAZIONE GIOVANI AVVOCATI TORINO