

INTELLIGENZA ARTIFICIALE, NEUROSCIENZE, ALGORITMI: LE SFIDE FUTURE PER IL GIURISTA

INDICE:

Capitolo I – I problemi che gli algoritmi pongono oggi al giurista; pag. 3

Capitolo II – Algoritmo e diritto amministrativo; pag. 19

Capitolo III – Algoritmo e diritto penale; pag. 41

Capitolo IV – Algoritmo e contratto; pag. 58

**Capitolo V – Il governo della tecnica e il controllo umano delle sue applicazioni;
pag. 71**

Capitolo VI – Qual è oggi la più grande intelligenza artificiale del mondo? pag. 98

**Capitolo VII – Algoritmi, neuroscienze e neurodiritti. L'algoritmo e
l'adolescenza; pag. 107**

**Capitolo VIII – Strumenti normativi regolatori e prospettive future nella
dimensione euro-unitaria e in quella nazionale; pag. 130**

Capitolo IX – Servizio civile digitale; pag. 141

Capitolo X – *Hate speech*: un fenomeno incontrollabile? pag. 147

Capitolo XI – La figura degli *influencer*; pag. 162

**Capitolo XII – La commercializzazione dei dati personali: il caso Facebook; pag.
179**

Capitolo XIII – La tutela dei minori e il diritto all'oblio; pag. 188

Capitolo XIV – L'“eredità digitale”; pag. 194

Capitolo XV – Il fenomeno del c.d. *Revenge porn*; pag. 198

Capitolo XVI – La diffamazione tramite chat privata o *mailing list*; pag. 206

**Capitolo XVII – L'interoperabilità: il dialogo necessario tra il digitale e il diritto;
pag. 217**

Bibliografia; pag. 232

INDICE Allegati:

I. Digital Services Act

II. Digital Markets Act

III. Digital Governance Act

IV. Proposta della Commissione sulla IA

V. Report ONU sulla IA

VI. Raccomandazione UNESCO sull'etica dell'IA

VII. Piano Strategico Nazionale IA

VIII. Nuove Linee Guida Agid 2021

IX. Strategia Cloud Italia 2021

Capitolo I

I problemi che gli algoritmi pongono oggi al giurista

If this, then that: con questa semplice espressione, che sta ad indicare il concetto di algoritmo, ossia una sequenza di passaggi elementari in un tempo finito, si racchiude il futuro della tecnologia e del destino dell'uomo. Nella complessità che caratterizza il nostro tempo, il giurista, spinto da una visione essenzialmente antropocentrica, dovrà svolgere una funzione "ordinante", che ponga l'algoritmo non in sostituzione dell'essere umano, bensì al suo servizio.

Come, però, potrà svolgere tale funzione, con quali strumenti normativi ed interpretativi, con quali categorie giuridiche, con quali processi di modellizzazione concettuale idonei a cogliere, gestire e regolare la complessità?

«Il limite di Prometeo invocato dalla cultura greca oggi evidenzia il rischio di una tecnologia che compie un processo di mimesi e di superamento della razionalità umana. Questo, perché l'algoritmo oggi non costituisce più un "mere tool", ossia mero elemento di trasmissione della volontà umana, ma un coelemento essenziale ed imprescindibile di formazione della volontà stessa che incide sul processo di autodeterminazione dell'individuo. Le neuroscienze aprono scenari inimmaginabili nel binomio "coscienza e identità": cogito ergo sum, secondo Cartesio, l'uomo è il pensiero, ma il pensiero è il correlato neuronale della coscienza umana, quella coscienza suitas che nell'antica Grecia consentiva di distinguere l'Ardire dalla Hybris. In fondo, se ci pensiamo bene, Prometeo è colui che vede ed agisce in tempo nella consapevolezza del Katèchon, ossia del limite: il limite di ammissibilità etica, giuridica, sociale delle innovazioni tecnologiche. Non tutto ciò che è tecnologicamente possibile, è giuridicamente ed eticamente accettabile e condivisibile. Se Parmenide affermava: «il pensiero è l'essere: è la stessa cosa pensare e pensare ciò che è, perché senza l'essere in ciò che è detto non troverai il pensare», il profilo della libertà cognitiva come presupposto di autodeterminazione individuale oggi è messa a dura prova dai c.d. neuro-link: gli algoritmi entrano nell'intime sphere e nella predittività dei propri pensieri, delle decisioni e delle scelte individuali. Se l'habeas corpus ha rappresentato la base dello Stato di diritto, l'habeas data la base del diritto di autodeterminazione digitale, l'habeas mentem diventa il fulcro dei c.d. "neuro-diritti" per evitare la deriva neurodeterministica, c.d. "riduzionismo scientifico" e "determinismo tecnologico"». Sono queste le autorevoli considerazioni del Garante per la Privacy, il Professore Pasquale Stanzone, espresse in un convegno sul tema delle neuroscienze e la tutela dei dati¹.

¹ Il discorso è stato tenuto al Convegno del 28 gennaio 2021, a Roma, sul tema "Giornata europea per privacy, neurodiritti e neuroscienze", in occasione dei 40 anni della Convenzione Europea per la protezione dei dati personali firmata a Strasburgo il 28 gennaio 1981.

Occorre, dunque, uno statuto giuridico ed etico, che coniughi l'innovazione con la dignità umana, intesa sempre come fine, e mai come mezzo, facendo tesoro dell'insegnamento di Kant.

Vi è da chiedersi, però, se occorra oggi introdurre un concetto di neuroetica, ossia di etica della neurotecnologia, per proporre un approccio etico, sistematico e integrato alle tecnologie di intelligenza artificiale.

*Langdon Winner*² affermava che ogni disposizione tecnologica è espressione di potere e *Lewis Mumford*³ parlava di “*Technical arrangements as forms of order*”: oggi il problema che si affaccia all'orizzonte non è solo l'implementazione della tutela dei dati, che costituiscono i *new oils, essential facilities* della *driven data economy*, ma anche la tutela della facoltà cognitiva dei cittadini, utenti, consumatori o fruitori dei servizi. Vi è da chiedersi cosa resta della libertà e responsabilità umana?

Il dato neuronale, con le c.d. tecniche di *brain reading* nell'interfaccia uomo-computer, viene immesso per la prima volta nell'area dei dati digitali, nella c.d. *infosfera*, ecosistema digitale, andando al di là delle applicazioni di *neuro-enhancement* nel campo bio medico e ponendo il problema della «*opacità del machine learning*».

Il dato neuronale è un dato differente dagli altri:

- 1) ha un'importanza ontologica, perché è la sede dei processi vitali, è coscienza, pensiero, memoria;
- 2) ha un'importanza antropologica nell'autopercezione di sé, dimensione fenomenologica e soggettiva della persona;
- 3) ha un'importanza epistemologica, il dato neuronale è predittivo come il dato genetico;
- 4) ha un'importanza metodologica, i dati neurali possono essere rimodulati, il *brain reading* si può trasformare in *brain writing*.

Siamo oltre il test di *Turing*, criterio per determinare se una macchina sia in grado di esibire un comportamento intelligente⁴.

² L. WINNER, “*Autonomous technology*”, Cambridge, Mass., 1977.

³ L. MUMFORD, “*Technics and Civilization*”, 1961.

⁴ Interessante sul tema l'articolo del fisico I. LICATA, “*I teoremi di Gödel e l'intelligenza artificiale*”, su <https://www.indiscreto.org/i-teoremi-di-godel-e-lintelligenza-artificiale/>. Nella visione collettiva, i risultati dell'opera del matematico Kurt Gödel fissano dei “limiti” alle capacità razionali della mente umana. Si tratta della famosa teoria sulla indecidibilità, che oggi si riflette sulle teorie sull'I.A. I teoremi di Gödel (1931) fissano dei limiti molto precisi alla matematica e al metodo assiomatico del '900, riconducibile a Hilbert. Secondo il primo teorema di Gödel, ogni sistema sufficientemente potente, coerente ed assiomatizzabile è sintatticamente incompleto, per cui è sempre possibile produrre una proposizione P indecidibile, ossia della quale è impossibile stabilire, con gli strumenti del sistema, la verità o la falsità. Il secondo teorema di Gödel, ancora più drastico, prevede che ogni sistema sufficientemente potente, coerente e assiomatizzabile è incapace di dimostrare una proposizione che esprima in modo canonico la coerenza dello stesso sistema. Si veda K. GÖDEL, “*Sulle proposizioni formalmente indecidibili dei Principia Mathematica e di sistemi affini*”, in S. G.

Tale criterio, si ricorderà, fu suggerito da *Alan Turing*, inventore del computer, nel suo noto articolo “*Computing machinery and intelligence*”, apparso nel 1950 sulla rivista *Mind*; ma certamente allora Turing non poteva immaginare gli scenari attuali⁵.

SHANKER (a cura di), “*Il teorema di Gödel*”, trad. it. di P. PAGLI, Franco Muzzio Editore, Padova, 1991, che a pp. 23-25 scrive: «*La tendenza della matematica verso un sempre maggiore rigore ha portato, come è ben noto, alla formalizzazione di suoi ampi settori, così che al loro interno è possibile dimostrare un teorema usando solo poche regole meccaniche. I sistemi formali più ampi elaborati sino a questo momento sono quello dei Principia Mathematica (PM), e il sistema di assiomi di Zermelo-Fraenkel per la teoria degli insiemi (con i successivi sviluppi di J. Von Neumann). Questi due sistemi sono talmente generali che tutti i metodi dimostrativi attualmente impiegati in matematica sono stati formalizzati al loro interno, cioè ridotti a pochi assiomi e alcune regole di inferenza. Si potrebbe quindi supporre che questi assiomi e queste regole siano sufficienti a decidere ogni quesito matematico formalmente esprimibile in essi. Si dimostrerà più avanti che non è così, e che al contrario esistono nei due sistemi citati problemi relativamente semplici riguardanti la teoria dei numeri naturali che non possono venire decisi sulla base degli assiomi*». Dagli studi di Gödel, per cui la matematica non è che un sistema aperto, in grado di generare sempre nuovi problemi, deriva la teoria generale dei sistemi complessi logicamente aperti. I risultati di Gödel producono effetti sulle teorie dell’IA: se consideriamo un sistema di IA “forte”, basato sulla manipolazione simbolica e implementato tramite funzioni Turing-computabili, si tratta di un sistema formale, per cui potremmo considerare i teoremi di indecidibilità anche in questo caso. Gödel ne parlò nella “Conferenza Gibbs” del 26 dicembre 1951, quando il tema dell’IA era già nell’aria: Turing nel 1950 aveva pubblicato “*Computing Machinery and Intelligence*”, e già nel 1937 aveva teorizzato la definizione di “numeri calcolabili”. Nella conferenza si parlò della connessione tra i risultati di Gödel e quelli di Turing, contributi che portavano una limitazione precisa dei sistemi formali. Gödel introdusse la distinzione tra proposizioni matematiche obiettivamente vere e proposizioni vere in relazione ad un sistema formale e sostenne che la capacità della mente umana di gestire le prime non era limitata dai teoremi relativi al secondo tipo di proposizioni. Sostenne la possibilità di considerare una “macchina intelligente” e la possibilità di trovare una somiglianza tra il cervello e un automa finito, che, secondo Gödel, potrebbe andare incontro a questioni indecidibili, così come la mente umana, con la differenza che quest’ultima può sempre escogitare strategie per superare gli ostacoli e le difficoltà. Sull’argomento c’è una bibliografia molto vasta: si vedano, ad esempio, J. W. DAWSON JR., “*Dilemmi logici. La vita e l’opera di Kurt Gödel*”, Bollati Boringhieri, Torino, 2001; R. GOLDSTEIN, “*Incompletezza. La dimostrazione e il paradosso di Kurt Gödel*”, Codice Edizioni, Torino, 2006; J. L. CASTI, W. DE PAULI, “*Gödel. L’eccentrica vita di un genio*”, Raffaello-Cortina Edizioni, Milano, 2001; A. HODGES, “*Storia di un enigma. Vita di Alan Turing 1912-1954*”, Bollati Boringhieri, Torino, 2004; D. LEAVITT, “*L’uomo che sapeva troppo. Alan Turing e l’invenzione del computer*”, La Biblioteca delle Scienze, Milano, 2009; I. LICATA, “*La logica aperta della mente*”, Codice Edizioni, Torino, 2008; “*Piccole variazioni sulla scienza*”, Dedalo, Bari, 2016; “*Complessità. Un’introduzione semplice*”, Di Renzo Editore, 2018; A. TURING, “*Le basi chimiche della morfogenesi*”, Mimesis Edizioni, Sesto San Giovanni, 2021; S. STERRETT, “*Bringing up Turing’s “Child Machine”*”, in “*How the world computes*” Turing Centenary Conference, Springer, 2012.

⁵ Interessante, in proposito, è il recente studio dell’Università della California, che prevede che entro il 2052 l’intelligenza artificiale uguaglierà le funzioni del cervello umano, fino a superarle, così che non riusciremo più a superare il test di *Turing*. Questo perché gli algoritmi ci studiano, scelgono per noi, ci ricordano le nostre preferenze e i nostri impegni, scrivono per noi, completando i nostri discorsi digitali; v. <https://www.ilfoglio.it/bandiera-bianca/2021/11/03/news/scommettiamo-che-tra-un-po-non-riusciremo-piu-a-superare-il-test-di-turing--3328633/>.

“Il futuro non è ciò che progettiamo, ma è Kairòs, ciò che ci sorprende”, diceva San Paolo di Tarso. Stiamo andando verso l’iperumano, il transumano e postumano, il c.d. *Übermensch* di cui parlava Nietzsche?

Le scienze contemporanee hanno contribuito a definire l’uomo come un “sé multiplo”, la mente è l’idea del corpo, il corpo è *brain feeling*, siamo un complesso di mente e corpo: così si esprime *Antonio Damasio* nel suo scritto *“l’errore di Cartesio”*.

Ma se spostiamo la nostra analisi nell’universo quantistico, non possiamo non tener conto di quanto ha affermato *Roger Penrose*, premio Nobel per la fisica, con riferimento alla c.d. *“libertà dell’evento”*. In altri termini, oggi noi viviamo in un universo quantistico in cui il possibile è la base di comprensione dell’evento, *“brain imaging”*. Se questo è vero, allora le neurotecnologie possono anche favorire uno sviluppo qualitativo dell’uomo, inteso come complesso unico di mente e corpo, pensieri, emozioni, coscienza, critica. È questa la sfida che attende il giurista: a lui l’arduo compito di individuare, attraverso un approccio multidisciplinare, principi, regole, *principles and model-rules* capaci di realizzare quello che è stato di recente definito *“l’umanesimo digitale”*⁶.

⁶ Nell’elaborazione filosofica dell’IA e del rapporto tra uomo e macchina, possiamo ricordare le parole di Gödel, sopra richiamato, che nel suo platonismo critico e moderato dichiarò che *«o la mente umana oltrepassa infinitamente la potenza di ogni macchina finita, o altrimenti devono esistere problemi diofantini insolubili in modo assoluto»*. Per Gödel le teorie sull’IA, come la tesi di Church-Turing che sostiene sia possibile simulare qualunque processo mentale tramite funzioni Turing-computabili, erano ingenui; tuttavia, i suoi argomenti non erano ancora abbastanza forti. Quando fu pubblicato l’articolo “anti IA” del filosofo J. R. LUCAS, *“Mind, Machines and Gödel”*, in *Philosophy*, 36, nel 1961, incentrato sulla possibilità per un sistema logico-formale di “restare in scacco” davanti a una proposizione indecidibile ottenuta con la procedura di Gödel, quest’ultimo non si oppose criticamente. Tra l’altro questa tesi è stata ripresa nel libro di R. PENROSE, *“La Mente Nuova dell’Imperatore”*, nel 1992. Se secondo Turing *«la memoria umana è necessariamente limitata»*, secondo Gödel, invece, *«la mente nel suo uso, non è statica, ma si sviluppa costantemente (...) Quindi, benché a ogni stadio del suo sviluppo il numero dei suoi stati possibili discernibili sia finito, non c’è motivo per cui questo numero non possa divergere all’infinito nel corso di questo sviluppo»*. L’idea di Gödel era la seguente: si può costruire una macchina intelligente fondata su un gruppo di assiomi di partenza, ma durante l’interazione con l’ambiente, a causa di elementi casuali, questa può diventare via via più complessa, modificandosi strutturalmente in modo impreveduto, fino a sfuggirci. Per Gödel le capacità innovative, intuitive, strategiche della mente umana non hanno quasi nulla a che fare con le proposizioni indecidibili dei sistemi formali. Per quanto si possa spiegare un comportamento umano con le Macchine di Turing, ciò è diverso dalla capacità di produrre quei comportamenti. Gödel aveva capito che la mente umana è logicamente aperta ed in grado di produrre nuova informazione, potendo cambiare continuamente le “regole del gioco” (si pensi ai modelli distribuiti sub-simbolici connessionisti e bio-morfi), mentre le architetture “classiche” dell’IA “forte” hanno dimostrato di essere logicamente chiuse, avendo successo solo nei mondi limitati semanticamente. Quanto detto ci porta a pensare che verosimilmente la mente artificiale sarà meno “meccanica” di quanto si pensi e sarà basata su modelli capaci di implementare un’apertura logica, e allora ci chiederemo (come un nuovo test di Turing): le macchine intelligenti avranno la capacità di gestire l’incertezza e fare scommesse sul mondo?

Sembrerà strano, ma il primo computer è stato un computer a vapore, un calcolatore universale, risalente alla prima metà dell'800⁷, e la prima programmatrice è stata una donna, *Ada Lovelance*, definita da Charles Babbage “incantatrice dei numeri”.

Certo molti anni dovettero trascorrere prima che *Tim Berners-Lee*, nel 1989, presso i laboratori Cern di Ginevra, presentasse il primo sistema di “*information management*” (*called Mesh*), il primo *website* concepito come “*a democratic arena*” per lo scambio di informazioni al servizio dei cittadini, senza *royalties* o speculazioni. Ma tale idea democratica e gratuita del web è stata oggi vanificata dalle grandi piattaforme Facebook, Google e Amazon, che ne hanno monopolizzato l'utilizzo, disponendo di un'enorme quantità di dati, senza precise regole volte ad una loro effettiva responsabilizzazione. *Tim Berners-Lee*, insieme ad altri scienziati, sta lavorando oggi ad un progetto chiamato *Solid* per ridecentrare il web e renderlo di nuovo uno spazio libero. È emblematico che, nel 1909, lo scrittore britannico *Forster* abbia scritto una storia di fantascienza intitolata “*The machine stops*”, in cui l'autore immagina che le persone vivono isolate accanto ad una macchina che provvede a tutti i loro bisogni. Gli umani in tale racconto vivono connessi, pur rimanendo isolati, determinando in loro la paura delle esperienze dirette. Questo è il motivo per cui la tecnologia deve considerarsi “*as a tool, not a master*”.

Ma dal punto di vista giuridico, come deve considerarsi il rapporto uomo-macchina? Il grande giurista *Gunther Teubner* ha, per primo, affrontato il tema dell'algoritmo e degli agenti digitali autonomi, ossia di quelli che possono elaborare e prendere decisioni indipendentemente dal produttore e dall'utilizzatore del programma. Secondo tale autore, occorre analizzare il rapporto che si instaura tra l'uomo e il *software* utilizzato, nonché la distribuzione della responsabilità per danni cagionati nella sfera giuridica di coloro i quali hanno fatto affidamento incolpevole sulla dichiarazione dell'agente digitale autonomo, soprattutto se si tiene conto della prevalenza nel sistema della teoria oggettiva della dichiarazione di volontà. L'assistente digitale è diventato sempre meno un semplice *nuncius* della volontà della persona fisica. E, sicuramente, non è tale quando è capace di prendere decisioni autonome e, in quanto tale, causare danni a terzi. Le categorie che vengono in rilievo sono chiaramente la rappresentanza e il rapporto associativo uomo/macchina. Occorrerà soffermarsi sul nuovo concetto di informazione, sempre più alterata non solo dalle c.d. *fake news*, ma dalla c.d. “*information pollution*”, ossia dall'inquinamento delle informazioni. Tale concetto si

⁷ Le macchine hanno cominciato a fare calcoli semplici e oggi, dopo “appena” 200 anni, un'intelligenza artificiale ha formulato, per la prima volta, congetture matematiche. È un risultato di uno studio condotto dai ricercatori di *DeepMind* e dell'Università di Oxford, pubblicato sulla rivista scientifica *Nature*: si è scoperto che i moderni computer, che da molti anni ci aiutano nella soluzione di problemi di matematica, grazie all'apprendimento automatico sono riusciti a rilevare connessioni matematiche altrimenti invisibili agli esseri umani. Si tratta di un grande passo avanti e sono auspicabili applicazioni in altri campi, come la biologia e l'economia, v. <https://www.wired.it/article/intelligenza-artificiale-deepmind-matematica-nodi/>.

declina nei fenomeni di *clickbait*, *sloppy journalism*, *misleading headings*, *biased news* and *filter bubble*. Sono tutti processi che contengono notizie false, notizie manipolate o informazioni modellate su profilazioni del soggetto che effettua delle ricerche sul web, riuscendo a trovare le informazioni sempre più corrispondenti alla propria formazione culturale e ai propri interessi, con una selezione subdola di dati che avviene a sua insaputa. Siamo in una dimensione ben lontana dalla *parresia*, ossia dalla verità di cui parlavano i greci nel sistema democratico della *polis*.

Luciano Floridi, docente di Filosofia ed Etica dell'Informazione a Oxford, nel suo libro *"Pensare l'infosfera"*, sostiene che viviamo ormai in un mondo virtuale, l'*infosfera* appunto, in cui tutti siamo degli *inforgs*, organismi del sostrato informazionale⁸. La postmodernità rifugge sempre più dalle cose, per andare verso relazioni con inarrestabile astrazione dal materiale. Siamo passati da una posizione ontologica assoluta – modellata su un mondo letto in termini aristotelici (c.d. primato della cosa) e newtoniani (primato nello spazio e nel tempo) – a quella epistemologica-relazionale, dominante nell'*infosfera*; un costruzionismo di ispirazione neo-Kantiana, definito come processo di modellizzazione (non copia platonica del modello) che dà forma alla realtà, rendendola intelligibile. Se Cartesio affermava *"cogito ergo sum"*, oggi possiamo dire *"videor ergo sum"*: la costruzione del sé (c.d. *Bildung*) passa attraverso lo strumento digitale. Il *selfie* è il sentirsi, il realizzarsi nello sguardo dell'altro, *Leib a Korper*, la pietrificazione del sé, di cui parla Sartre in pagine memorabili di *"L'essere e il nulla"*. Il *selfie* è l'esposizione del corpo *online*, che ha come unità di misura i *likes*. Un famoso psichiatra, Giovanni Stanghellini, parla di *"selfie come sentirsi nello sguardo dell'altro, l'altro è l'unica possibilità di essere riconosciuti"*.

Tutto questo a che prezzo per l'uomo? Il c.d. *"effetto Flynn"* ci dovrebbe far riflettere: Richard Flynn ha condotto uno studio tra il 1990 e il 2009, dimostrando che il quoziente intellettivo (Qi) stia cominciando lentamente, ma inesorabilmente, a calare. Un calo costante che, oggi, è diventato un vero e proprio tracollo, se pensiamo alla percentuale di persone afflitte dal c.d. *"analfabetismo funzionale"* (sanno leggere, ma non capiscono il senso, né sono in grado di rielaborarlo). I giovani hanno oggi molte informazioni e poca conoscenza, o meglio, una *"conoscenza irrelata e non correlata"*. Le nuove tecnologie digitali, specialmente per i più giovani, rappresentano un

⁸ Interessante anche l'analisi del suo nuovo libro, *"Intelligenza Artificiale. L'uso delle nuove macchine"*, Bompiani, 2021. Nella sua intervista su *"Il Foglio"*, di G. LEGANZA, *"Luciano Floridi ci spiega cosa c'è di antico nell'intelligenza artificiale"*, l'autore spiega che *"siamo noi che adattiamo il mondo alle macchine, non viceversa. Nell'AI è presente la tradizione filosofica greca. La differenza con l'intelligenza umana? I computer sono più bravi, ma noi sappiamo adattarci meglio"*, su <https://www.ilmagnum.it/cultura/2021/12/04/news/luciano-floridi-ci-spiega-cosa-c-e-di-antico-nell-intelligenza-artificiale-3426829/>.

potentissimo e pervasivo elemento di degradazione delle facoltà cognitive, emotive e relazionali. Perché questo accade, quali sono le ragioni?

Il neurobiologo *Laurent Alexandre*⁹ ritiene che la ragione risieda in questa considerazione: “*laddove il libro favoriva una concentrazione duratura e creativa, internet incoraggia la rapidità, il campionamento distratto di piccoli frammenti di informazioni provenienti da fonti diverse*”. Il processo che consiste nell’immagazzinare i dati, creando così la memoria, per poi elaborarli, creando un ordine diverso, si chiama “apprendimento”.

Il problema è che oggi è l’intelligenza artificiale ad occuparsi del processo di immagazzinamento dei dati (memoria ed elaborazione dei dati), con l’intelligenza umana ridotta a svolgere un ruolo ausiliario e sempre più ininfluente.

Ecco che, allora, abbiamo assistito alla nascita del GPT3, *Generative Pre-trained Transformer*: l’11 giugno 2020 è stata presentata GPT3, un’intelligenza artificiale in grado di scrivere un romanzo nello stile dello scrittore che si preferisce, che scrive in pochi istanti il racconto che si preferisce. Ricorda il generatore automatico di lettere d’amore che *Alan Turing* sperimentò nel 1952 a Manchester.

GPT3 è la terza versione di un progetto di ricerca di un laboratorio fondato a San Francisco nel 2015, *Open AI*, che, tra i fondatori, ha *Elon Musk* e tra i finanziatori *Microsoft*.

Non è trascorso nemmeno un anno e GPT3 non scrive romanzi, ma è già utilizzato da oltre 10.000 sviluppatori ed è presente in oltre 300 applicazioni.

Rientrano in questo processo le risposte ancora semplici di *Alexa* e *Siri* nei nostri *smartphone* e gli assistenti vocali, i dialoghi non facili con le *chatbot* quando andiamo sul sito della nostra banca o di una grande azienda che fornisce telefonia, acqua e luce; qui sappiamo di dialogare con un risponditore automatico.

Il confine tra umano e artificiale nel GPT3 è meno netto, impercettibile, sarà sempre più difficile distinguere volti, suoni e testi creati da un’intelligenza artificiale da quelli reali.

È innegabile la difficoltà di lettura di algoritmi che utilizzano grandi quantità di dati (*big data*) e, in misura crescente, si caratterizzano per l’impiego di tecnologie basate sull’intelligenza artificiale che non si limitano a seguire fedelmente le istruzioni del programmatore, ma diventano intelligenza *spontaneus*, autocreativa, autoevolutiva, inventando soluzioni e percorsi inediti, con il risultato che neppure colui che ha fornito le istruzioni alla macchina attraverso l’algoritmo è pienamente in grado di ripercorrere il processo decisionale e offrire una spiegazione comprensibile.

⁹ L. ALEXANDRE, “*La guerra delle intelligenze, intelligenza artificiale contro intelligenza umana*”, pag. 75, ed. Torino, 2017.

Il problema del carattere non neutrale dell'algoritmo, e la sua scarsa trasparenza, assume un ruolo centrale nel dibattito giuridico recente, da qui il pericolo che la società possa diventare una grande, unica scatola nera, una “*black box society*”¹⁰.

È il c.d. “*surveillance capitalism*” di cui parla S. Zuboff¹¹.

Sulla base della complessità di tali considerazioni, la Commissione Europea ha elaborato il *Digital Services Act* che, considerando essenziale “*la legalità procedimentale della conservazione dei dati*”, il c.d. *Digital Due Process*, predispone una tutela del cittadino basata su due principi fondamentali: il principio dell'autodeterminazione del singolo e il principio di responsabilizzazione delle piattaforme digitali.

Sono questi i binari lungo i quali dovranno essere definite, a livello europeo, le norme che saranno determinanti per costruire un corretto rapporto uomo-macchina.

Sul piano della qualità e del livello della regolamentazione¹², si distingue tra auto-regolazione, co-regolazione ed eteroregolazione, ponendosi il problema se e in che termini la regolamentazione dei *social network* debba essere affidata alle grandi società monopoliste del web, o se occorra un intervento più incisivo della normativa nazionale e sovranazionale. Sappiamo che Facebook ha, al suo interno, sotto forma di *trust*, il

¹⁰ F. PASQUALE, “*The Black Box Society. The secret Algorithms that Control Money and Information*”, Cambridge – Ma 2015.

¹¹ S. ZUBOFF, “*Big other: surveillance capitalism and the prospects of an information civilization*”, “*Journal of Information Technology*” (2015) 30, 75-89; ID., “*The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*”, London, 2019.

¹² Per quanto concerne il problema relativo al tipo di legislazione che deve regolare l'IA, ad oggi abbiamo due fondamentali esempi di approccio globale all'IA da parte delle legislazioni dei vari paesi nel mondo. Da un lato, abbiamo l'esempio del Rapporto dell'Alto Commissario delle Nazioni Unite per i diritti umani sul “*Diritto alla Privacy nell'era digitale*”, commissionato dal Consiglio per i diritti umani nella sua risoluzione 42/15, in cui si analizza come l'uso diffuso da parte degli Stati e delle imprese dell'I.A., tra cui rientrano la profilazione, il processo decisionale automatizzato e le tecnologie di apprendimento automatico, influenzi il godimento del diritto alla privacy e dei diritti connessi, fornendo alcune raccomandazioni agli Stati e alle imprese in merito alla progettazione e all'attuazione di salvaguardie per prevenire e minimizzare i risultati dannosi. Dall'altro lato, c'è il primo accordo mondiale sull'etica dell'I.A. stipulato recentemente dall'Unesco, approvato il 25 novembre 2021, che prende atto che l'I.A. pone importanti quesiti e problemi etici, che necessitano un intervento sovranazionale. Il direttore generale dell'Unesco, Audrey Azoulay, ha presentato una “*Raccomandazione*” di 28 pagine, ratificata dai 193 stati membri, tra cui anche la Cina. A fronte di un cospicuo aumento dei pregiudizi di genere ed etnici e di minacce significative alla privacy, alla dignità e ad altri diritti, si vuole, infatti, rispondere con un testo che assicuri la massima trasparenza e intelligibilità sul funzionamento degli algoritmi, dato che si influisce sui diritti dell'uomo e sulle libertà fondamentali. I valori e i principi comuni che devono guidare la costruzione delle macchine che impiegano l'Intelligenza Artificiale sono elencati dal secondo articolo della Raccomandazione e sono i seguenti: equità e non discriminazione, sostenibilità, privacy, sicurezza e protezione, trasparenza e “*spiegabilità*”, responsabilità e *accountability*, consapevolezza e alfabetizzazione. Per un approfondimento sul tema di veda L. MISCHITELLI, “*Intelligenza artificiale etica: ecco l'approccio “globale” Unesco (approvato anche dalla Cina)*”, su agendadigitale.eu.

Facebook Oversight Board, che esamina le questioni poste dalla *Community*, ma occorre un intervento di eteroregolazione sovranazionale, capace di impedire che pubbliche funzioni siano esercitate da poteri privati.

In questa ottica, il *Digital Services Act*, attualmente a livello di proposta della Commissione, si pone l'obiettivo di prevenire il disordine normativo e di creare un mercato digitale *online* sicuro ed affidabile¹³. Nella nuova regolazione delle piattaforme digitali, la Commissione europea sta cercando di affermare uno *Standard Europeo Regolatorio* per la definizione del nuovo capitalismo digitale, che si basi su un concetto di “sicurezza funzionale”, *security by design*. La Commissione europea sollecita gli Stati membri non con regole, ma con obiettivi, per far diventare l'Europa un *Hub* di regole digitali, il protagonista della trasformazione digitale ed ecologica entro il 2030. In un'epoca caratterizzata da un eccesso di informazioni, la c.d. *Infodemia*, è necessaria anche un'igiene informativa: secondo Vittorio Loreto, fisico della materia presso l'Università La Sapienza di Roma, che collabora ad un progetto di ricerca definito “*Cartesio, ergo news*”, se il dubbio è l'inizio della conoscenza, occorrono sistemi per valutare l'affidabilità di una notizia. Viviamo attualmente in delle “bolle informative”, con i c.d. “*sistemi di raccomandazione*” che non consentono di esplorare “*l'Adiacente possibile*”.

Ma come controllare la qualità dell'informazione? Sono sufficienti gli appositi *software* per controllare la tracciabilità della notizia? Possiamo parlare di graduazione delle falsità informative? Il fisico Pauli, fondatore della meccanica quantistica, parlava di “*nothing in wrong*”; noi possiamo parlare di “*nothing in fake*”?

Ognuno di noi è alle prese con *cookies* di funzionalità, *cookies* analitici e *cookies* di profilazione di terze parti. Per prestare il proprio consenso, siamo costretti a consultare

¹³ Il mercato digitale è in continua espansione. Sul nuovo fenomeno dell'acquisto di terreni virtuali vedi W. FERRI, “2,4 milioni per 500mq di cyber spazio: il Metaverso e la corsa all'oro digitale”, su [lindipendenteonline.it](https://www.lindipendenteonline.it), che spiega bene questa “corsa all'oro in salsa digitale”: gli investitori accorrono oggi alle risorse offerte da *Metaverso* per ottenere (in futuro) grandi ritorni economici. Non è una novità, ma la portata del fenomeno cresce quanto più si ingigantisce “*la febbre per il digitale*”. Lo dimostrerebbero i dati pubblicati da *DappRadar*, portale secondo cui il mercato dei terreni virtuali ha smosso circa 100 milioni di dollari sui soli *The Sandbox*, *Decentraland*, *CryptoVoxels* e *Somnium Space*. Non sarebbero solo piccoli investitori in ricerca di facili guadagni. Si parla anche di agenzie immobiliari virtuali, che comprano grandi lotti per scommettere su un loro aumento di valore nel prossimo futuro. *The Metaverse Group*, nell'ultimo periodo, ha riscattato 500 metri quadrati digitali sulla piattaforma virtuale *Decentraland*: la transazione ha mosso 2,43 milioni di dollari. È il fenomeno dei latifondisti 4.0, letteralmente in espansione; v. <https://www.lindipendenteonline.it/2021/12/04/24-milioni-per-500mq-di-cyber-spazio-il-metaverso-e-la-corsa-alloro-digitale/>. Interessante anche il tema dell'acquisto del mattone virtuale, v. A. GRECO, “*Il metaverso come il Monopoli: scatta la corsa al mattone virtuale*”, su *Repubblica.it*; il fenomeno si sta sviluppando negli ultimi 5 mesi con *Metaverso*, gli acquisti immobiliari con le criptovalute stanno diventando virtuali, v. https://www.repubblica.it/cronaca/2021/12/06/news/il_metaverso_come_il_monopoli_scatta_la_cor_sa_al_mattone_virtuale-329215917/.

la *Cookie policy*, con la automatica conseguenza che, chiudendo il *banner* o accedendo a qualunque elemento del sito, acconsentiamo automaticamente all'uso dei *cookies*.

La credibilità, la decentralizzazione e l'intermediazione sono presenti nei c.d. "*filter bubbles*", "gabbie virtuali", in cui gli algoritmi rinchiudono gli utenti, raccogliendo dati e preferenze sulla base di precedenti *click*, cronologia delle ricerche e localizzazioni¹⁴. La dottrina parla di disordini dell'informazione, di varie categorie di disturbi dell'informazione, distinguendo tra "*disinformazione*", "*misinformazione*" e "*malainformazione*".

Le stesse piattaforme digitali si stanno attrezzando per arginare tale fenomeno: ad esempio, Facebook utilizza i c.d. "*educational pop-ups*", *pop ups* informativi con etichettature specifiche sulle notizie e con rimozione automatica dei contenuti falsi; Twitter distingue tra notizie *misleading*, *disputed* and *unverified*, con sistemi c.d. di *Strike System*, nel senso che, dopo alcuni richiami, vi è il blocco dell'account.

Ma quali rimedi possono/devono essere rimessi allo Stato e ad organismi sovranazionali, e quali alle stesse piattaforme? La comunicazione sui *social network*, infatti, è caratterizzata da pervasività ed invasività, dalla illimitatezza spazio/temporale, dalla disintermediazione e dalla semplificazione del messaggio.

In Francia è stata approvata nel 2018 la legge n. 1202, contro la manipolazione dell'informazione; in Germania è stata approvata il 30 giugno 2017 la legge sull'*hate speech*, prevedendo fattispecie criminosi sulle figure già previste dal codice penale tedesco, con un sistema di "*notice and take down*", ossia di reclamo da rivolgere alla stessa piattaforma, prima di un vero e proprio ricorso all'autorità giurisdizionale. In Italia, vi è stata la presentazione del disegno di legge Gambaro nel 2017, e di recente un nuovo DDL approvato alla Camera e attualmente in discussione al Senato con la

¹⁴ Come è noto, le *app* installate sui nostri *smartphone* "ci spiano" e vivono di dati sempre più numerosi sulle nostre abitudini, sui luoghi che frequentiamo; tuttavia, non tutti sanno che i dati raccolti sulla posizione non sono solo quelli che si ricavano dal GPS. Una definizione che non tutti conoscono è quella di "*location tracking*", dietro cui si cela una articolata serie di dati, tra cui rientrano la posizione (coordinate, indirizzo IP, posizione del Wi-Fi), la pressione barometrica, i dati del giroscopio e dell'accelerometro. Questi ultimi due strumenti permettono di tracciare il profilo di utilizzo del telefono, fungendo da "*backdoor*" per la privacy, soprattutto su sistemi iOS. L'accelerometro, infatti, è molto sofisticato e arriva a captare le vibrazioni del luogo frequentato, i nostri stessi passi, la nostra voce, i rumori e le voci nel luogo in cui ci troviamo. Ciò avviene anche senza il nostro esplicito consenso e non solo sul telefonino (si pensi agli *smartwatch*, ai braccialetti e ai *trackers* da polso, che usano gli sportivi). A volte è lo stesso sistema di un'*app* ad essere progettato per raccogliere dati da molti sensori, spesso necessari per far sì che il sistema stesso funzioni. Il problema è che le *app* possono arrivare a rintracciare quello che facciamo con il nostro telefono, su quali siti navighiamo, come ci muoviamo sul *touchscreen*, quanto tempo passiamo su una pagina internet, ecc. I produttori dei sistemi operativi come *Apple* ed *Android*, prima di concedere le autorizzazioni alle *app*, dovrebbero potenziare il controllo sulla privacy, evitando il aggirio di blocchi espliciti. Si veda l'articolo di N. RUGGIERO, "*Quanto (e come) ci spia lo smartphone? Tutte le trappole che ignoriamo*", su *agendadigitale.eu*.

istituzione di una commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false. Presso l'AgCom è stato istituito un tavolo Tecnico sulle piattaforme digitali e il pluralismo informativo, mentre al livello europeo è stato approvato, il 26 settembre 2018, il *Code of Practice on Disinformation*.

Ma occorre chiedersi se vi sia la necessità di valutare la *privacy policy* in un sistema di *merger control*, attraverso un'azione di collaborazione e di coordinamento tra le varie Autorità regolatorie, e se sia necessario affiancare agli strumenti di *enforcement* una regolazione *ex ante* con sistemi di *pre-emptive remedy*, ossia rimedi preventivi e proattivi.

Soprattutto chiarire che tipo di regolazione introdurre: funzionale o strutturale? Omogenea o differenziata a seconda dei settori?

Occorre un coordinamento a livello di regolamentazione euro-unitaria tra *Digital Services Act*, *Digital Governance Act* e *Digital Markets Act*; sono questi i tre elementi nel nuovo pilastro digitale europeo.

Sempre più il processo di “monetizzazione dei dati”, nella *data driven economy*, pone una stretta relazione tra “informazione e concorrenza”, inducendoci a chiederci se le regole preposte alla tutela della concorrenza siano ancora adatte o vadano integrate per i mercati digitali. Il primo problema è l'individuazione della nozione di “quote di mercato”, “indici di concentrazione”, di “mercato rilevante” per i mercati digitali, che sono “*mercati con strutture multiversanti*”, le c.d. piattaforme di attenzione (“*attention platforms*”), con effetti di rete diretti e indiretti, *switching benefits and costs*, economie di scala e di scopo e con assenza di prezzo.

I dati personali sono utilizzati come “controprestazioni” per un servizio gratuito. Il potere di mercato risiede non nel possesso dei dati, ma nel c.d. “*data mining*”, ossia nella capacità di estrarre valore dai dati, (TEST SSNDQ: “*small, but significant non-transitory decrease in quality*”).

La tutela della privacy e la trasparenza sono «fattori qualitativi del confronto concorrenziale», l'utente è concepito non solo come consumatore, ma anche come produttore di dati. Partendo da R. Posner e G. Weyl¹⁵, i dati personali non sono solo

¹⁵ V. l'opera di R. A. POSNER, “*The Right of Privacy*”, 12 *Georgia Law Review* 393, 1977. La patria della privacy viene indicata negli USA. “*The concept of privacy is elusive and ill defined*” scriveva Richard Posner nel suo saggio del 1977. Sul finire dell'800, soprattutto a partire dalla città di Boston, si delinea “*the right to be let alone*”, lo “*jus solitudinis*”, da parte di S. D. WARREN e L. D. BRANDEIS, “*The Right to privacy*”, *Harvard Law Review*, 1890; nell'ambito della *law of torts*, si veda anche l'opera di T. M. COOLEY, “*A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*”, Chicago, 1888. Riguardo al “*the right to be forgotten*” il caso noto è quello *Melvin* contro *Reid*, definito nel 1931, originato dall'utilizzo di dati personali all'interno di una pellicola cinematografica. La Corte d'Appello della California si era occupata delle doglianze formulate da un'ex prostituta, accusata di omicidio e poi assolta. La signora aveva cercato di “lasciarsi alle spalle” il caso di cronaca che l'aveva vista coinvolta, un tentativo (in parte riuscito) di rifarsi una vita

risorse, ma beni giuridici attinenti alla tutela dei diritti fondamentali della persona. Nelle controversie che hanno visto coinvolti Facebook e l'AgCom, è venuta spesso in rilievo la violazione degli artt. 20, 21, 22, 24 e 25 del D.lgs. n. 206/2005, ossia la sanzione per pratiche commerciali ingannevoli e pratiche commerciali aggressive, con abuso di posizione dominante di sfruttamento e *privacy policy* in violazione dell'art. 6 GDPR. Nelle sentenze del Tar Lazio nn. 260 e 261 del 10 gennaio 2020, si è fatto per la prima volta riferimento al “*fenomeno della patrimonializzazione del dato personale*” e, più recentemente, il Consiglio di Stato, sez. VI, con le sentenze nn. 2630 e 2631 del 29 marzo 2021, ha posto l'esigenza di garantire una “*tutela multivello*”, un sistema di tutela integrato che coinvolga in un *unicum* la privacy con il profilo consumeristico del fruitore del servizio digitale.

Ma vediamo come il *Digital Services Act* ha definito, da un punto di vista giuridico, i *social network* e come ha predisposto il sistema di tutela per fare poi un confronto con il *Digital Markets Act*, basato sui principi di equità e contendibilità, considerata la stretta connessione tra tutela della privacy e tutela della concorrenza.

Nel primo Considerando del Regolamento del parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, si legge testualmente, con un'esplicita dichiarazione di intenti, che:

Considerando (1) «*I servizi della società dell'informazione e in particolare i servizi intermediari sono diventati, una componente significativa dell'economia dell'Unione e della vita quotidiana dei suoi cittadini. A vent'anni dell'adozione del quadro giuridico esistente applicabile a tali servizi stabilito nella direttiva 2000/31/CE del Parlamento europeo e del Consiglio, modelli aziendali e servizi nuovi e innovativi, quali i social network e i mercati online, hanno consentito agli utenti commerciali e ai consumatori di accedere alle informazioni, diffonderle ed effettuare transazioni in modi nuovi. Attualmente la maggior parte dei cittadini dell'Unione utilizza tali servizi su base giornaliera. La trasformazione digitale e il maggior utilizzo di tali servizi hanno tuttavia anche dato origine a nuovi rischi e sfide sia per i singoli utenti sia per la società nel suo insieme*».

Considerando (2) «*Gli Stati membri stanno sempre più introducendo, o stanno valutando di introdurre, legislazioni nazionali sulle materie disciplinate dal presente regolamento, imponendo in particolare obblighi di diligenza per i prestatori di servizi intermediari. Tenendo conto del carattere intrinsecamente transfrontaliero di Internet, generalmente utilizzato per prestare i suddetti servizi, tali legislazioni nazionali*

“normale”. Tuttavia, il film “*The Red Kimono*” rivelava la storia della prostituta, andando a ripercorrere i gravi fatti di cui la signora era stata accusata. La Corte accolse le richieste dell'istante, affermando che «*a qualsiasi persona condannata ma poi assolta va riconosciuto il diritto alla felicità, che include il diritto di difendersi da attacchi inutili alla propria sfera personale, alla condizione sociale e alla reputazione*».

divergenti incidono negativamente sul mercato interno, che, ai sensi dell'art. 26 del Trattato, comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione di merci e di servizi e la libertà di stabilimento. Le condizioni per le prestazioni dei servizi intermediari in tutto il mercato interno dovrebbero essere armonizzate in modo da offrire alle imprese accesso ai nuovi mercati e opportunità di sfruttare i vantaggi del mercato interno, consentendo nel contempo ai consumatori e agli altri destinatari dei servizi di disporre di una scelta più ampia».

Se in questi due primi considerando vengono prese in considerazione le ragioni del mercato, nel terzo Considerando viene in rilievo il profilo della “responsabilità”:

Considerando (3) *«Un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile e per consentire ai cittadini dell'Unione e ad altre persone di esercitare i loro diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare la libertà di espressione e di informazione, la libertà di impresa e il diritto alla non discriminazione».*

Da qui l'enunciazione della necessità di una regolamentazione euro-unitaria enunciata nel Considerando (4): *«E', pertanto, opportuno stabilire una serie mirata di norme obbligatorie uniformi, efficaci e proporzionate a livello dell'Unione, al fine di tutelare e migliorare il funzionamento del mercato interno. Il presente regolamento stabilisce le condizioni per lo sviluppo e l'espansione di servizi digitali innovativi nel mercato interno. Il ravvicinamento delle misure nazionali di regolamentazione a livello dell'Unione in materia di obblighi per i prestatori di servizi intermediari è necessario per evitare la frammentazione del mercato interno, porvi fine e garantir e la certezza del diritto, così da ridurre l'incertezza per gli sviluppatori e promuovere l'interoperabilità. Il ricorso a prescrizioni tecnologicamente neutre dovrebbe stimolare l'innovazione anziché ostacolarla».*

La necessità di una regolamentazione eurounitaria viene collegata al concetto di neutralità della tecnologia, laddove i servizi di intermediazione vengono distinti in servizi di “*mere conduit*”, ossia di semplice trasporto, “*caching*”, memorizzazione temporanea e di “*hosting*”, consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo. Sono le definizioni dell'attività poste in essere dalle piattaforme digitali, definite giuridicamente per la prima volta nell'art. 2 del *Digital Services Act*, assieme alla nozione di “*contenuto illegale*”, rispettivamente nella lettera h) e g).

La lettera h) dell'art. 2 recita espressamente: *«“piattaforma on line” (è) un prestatore di servizi di hosting che, su richiesta di un destinatario del servizio, memorizza e diffonde al pubblico informazioni, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio, e, per ragioni oggettive e tecniche, non*

possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione nell'altro servizio non sia un mezzo per eludere l'applicabilità del presente regolamento».

La lettera g) definisce “contenuto illegale” *«qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro, indipendentemente dalla natura o dall'oggetto specifico di tali disposizioni».*

Se il criterio ispiratore del *Digital Services Act* è la responsabilizzazione delle piattaforme digitali, è pur vero che resta in piedi la clausola del buon samaritano nell'art. 7, rubricato “Assenza di obblighi generali di sorveglianza o di accertamento attivo”, in cui si prevede che *«Ai prestatori di servizi intermediari non è imposto alcun obbligo generale di sorveglianza sulle informazioni che tali prestatori trasmettono, né di accertare attivamente fatti o circostanze che indichino la presenza di attività illegali».* Vi è, però, l'obbligo di attivarsi nel rimuovere i contenuti illegali o disabilitare l'accesso non appena si venga a conoscenza di attività o contenuti illegali o si diviene consapevoli di fatti o circostanze illecite, lasciando impregiudicata, secondo gli ordinamenti giuridici degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga al prestatore di lavoro di impedire o porre fine ad una violazione. Viene mantenuto un sistema di “notifica ed azione” con l'introduzione, però, di un sistema di valutazione del rischio (art. 26 e 27), che costituisce un sistema preventivo e non repressivo della tutela, con un'evoluzione qualitativa dall’“enforcement” al “pre-emptive remedy”, ossia al rimedio preventivo e proattivo, incentrato sul “concetto di rischio di sistema”. L'art. 26, infatti, prevede che almeno una volta all'anno *«le piattaforme on line di dimensioni molto grandi individuano, analizzano e valutano eventuali rischi sistemici significativi derivanti dal funzionamento e dall'uso dei loro servizi nell'Unione. La valutazione del rischio deve essere specifica per i loro servizi e comprendere i seguenti rischi sistemici:*

- a) La diffusione di contenuti illegali tramite i loro servizi;*
- b) Eventuali effetti negativi per l'esercizio dei diritti fondamentali al rispetto della vita privata e familiare e alla libertà di espressione e di informazione, del diritto alla non discriminazione e dei diritti del minore, sanciti rispettivamente dagli articoli 7, 11, 21 e 24 della Carta;*
- c) La manipolazione intenzionale del servizio, anche mediante un uso non autentico o uno sfruttamento automatizzato del servizio, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori, del dibattito civico, o con effetti reali o prevedibili sui processi elettorali e sulla sicurezza pubblica».*

Alla valutazione di analisi del “rischio di sistema” segue la fase attiva di “*Attenuazione dei rischi*”, prevista dall’art. 27: «*Le piattaforme online di dimensioni molto grandi adottano misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici ... Tali misure possono comprendere, ove opportuno:*

- a) *L’adeguamento dei sistemi di moderazione dei contenuti o di raccomandazione, dei loro processi decisionali, delle caratteristiche o del funzionamento dei loro servizi, o delle loro condizioni generali;*
- b) *Misure mirate volte a limitare la visualizzazione della pubblicità associata al servizio da esse prestato;*
- c) *Il rafforzamento dei processi interni o della vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici;*
- d) *L’avvio o l’adeguamento della cooperazione con i segnalatori attendibili (figura qualificata introdotta nell’art. 19 del Digital Services Act);*
- e) *L’avvio o l’adeguamento della cooperazione con altre piattaforme on line attraverso i codici di condotta e i protocolli di crisi (previsti dagli art. 35 e 37 del Digital Services Act).»*

Un aspetto di grande rilievo è da rinvenirsi nell’obbligo di *disclosure* e di trasparenza, che viene introdotto come finalità principale dell’attività svolta dalla nuova figura dei “*Responsabili della Conformità*” (art. 32), figura chiave che assicura, assieme al “*coordinatore dei servizi digitali*”, la conformità dell’attività delle piattaforme alle norme contenute nel *Digital Services Act*. Viene definito e mitigato l’automatismo informativo dei c.d. “*sistemi di raccomandazione*”, ossia di quei sistemi che forniscono informazioni tramite le profilazioni, impedendo di ricevere notizie legate al c.d. “*adiacente possibile*”. L’art. 29 “*Sistemi di raccomandazione*” del *Digital Services Act* prevede che:

«1. *Le piattaforme on line di dimensioni molto grandi che si avvalgono di sistemi di raccomandazione specificano nelle loro condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione che possano avere messo a disposizione dei destinatari del servizio per consentire loro di modificare o influenzare tali parametri principali, compresa almeno un’opzione non basata sulla profilazione, ai sensi dell’articolo 4, punto 4) del regolamento (UE) 2016/679.*

2. *Qualora siano disponibili più opzioni a norma del paragrafo 1, le piattaforme online di dimensioni molto grandi mettono a disposizione una funzionalità facilmente accessibile sulla loro interfaccia online che consenta ai destinatari del servizio di selezionare e modificare in qualsiasi momento l’opzione da essi preferita per ciascuno dei sistemi di raccomandazione che determina l’ordine relativo delle informazioni loro presentate».*

Tale previsione cerca di garantire al singolo un'autonomia operativa, valutativa e decisionale nel suo rapporto con la piattaforma, superando quella asimmetria di posizioni che lo vede attualmente ingabbiato in automatismi informativi, collegati alla sua inconsapevole profilazione.

Naturalmente, le previsioni sopra descritte dovranno seguire il loro *iter* legislativo prima di costituire un rilevante elemento di riferimento normativo che valga a costituire un preciso centro autonomo di imputazione della responsabilità.

Per ora, occorre puntualizzare i principi elaborati soprattutto dalla giurisprudenza per poter definire i principi guida della materia in esame.

Capitolo II

Algoritmo e diritto amministrativo

Tra le varie giurisdizioni, quella amministrativa è stata la più incisiva nell'affermazione di una visione antropocentrica dell'utilizzo degli algoritmi, attraverso il criterio dello *human in the loop*, ossia attraverso la configurazione di un centro di imputabilità della responsabilità in capo esclusivamente all'agente umano.

Il riferimento principale è l'art. 22 del GDPR, rubricato "*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*", articolo che afferma il c.d. "*principio di non esclusività*". Tale articolo recita espressamente:

«1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*

2. *Il paragrafo 1 non si applica nel caso in cui la decisione:*

- a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*
- b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;*
- c) si basi sul consenso esplicito dell'interessato».*

Tale principio "*di non esclusività*" è, oggi, secondo parte della dottrina¹⁶, un principio "debole" che, a fronte di tecniche algoritmiche sempre più invasive, pervasive ed incisive sui diritti fondamentali, necessita di essere integrato dal principio di comprensibilità e di motivabilità (c.d. "*right to explainability*"). Tale principio si traduce, sul piano operativo, nel principio di trasparenza, nel diritto di accesso al codice sorgente: se le decisioni interferiscono con i diritti fondamentali, si radica un obbligo stringente di motivazione, sottoposto a controllo giurisdizionale, nel rispetto del principio di legalità, proporzionalità e ragionevolezza. È bene precisare che tali principi si applicano sia alle decisioni private, laddove vengano in rilievo asimmetrie legate ai c.d. poteri privati (si pensi alla posizione dei lavoratori nei confronti del datore di lavoro o al delicato settore anti-trust), sia alle decisioni pubbliche, laddove l'art. 41 e 47 della Carta dei diritti Fondamentali dell'Unione Europea sanciscono il diritto ad una buona Amministrazione, con obbligo di dare adeguata motivazione ai provvedimenti e l'art. 97 della Costituzione sancisce il principio del buon andamento dell'attività amministrativa, ispirata a criteri di efficienza, efficacia ed economicità.

È, però, bene precisare che l'algoritmo deve essere creato in modo da rispettare i diritti fondamentali dell'uomo: il modello degli *Oversight Board* e dei comitati etici,

¹⁶ A. SIMONCINI, "L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà", 2019.

incentrato sul controllo *ex post*, non ha funzionato. Il principio della configurazione predefinita degli standard di sicurezza, sin dal momento della progettazione del sistema, c.d. *privacy by design and default*, che è posto alla base del principio di *accountability*, deve evolvere in *design by education*, che veda i suoi strumenti nella co-regolazione (e non nella *self-regulation*), nella *paideia*, ossia nella formazione digitale integrata, consapevole, continua dei cittadini e nella collaborazione fra le varie Autorità regolatorie, per promuovere una tutela proattiva e preventiva della tutela dei dati.

Il Consiglio di Stato è la giurisdizione che ha affrontato in maniera più approfondita il cambiamento dell'Amministrazione 4.0, giungendo ad analizzare la c.d. *tecnificazione* dei principi amministrativi: se, infatti, il XX secolo ha visto il passaggio dall'amministrazione tradizionale, caratterizzata dall'utilizzo della carta e macchina da scrivere, a un'amministrazione 2.0, che fa uso di computer e stampanti, per poi giungere, all'inizio del XXI secolo, nell'era dell'amministrazione digitale 3.0, nella quale il soggetto pubblico fa ampio ricorso alla comunicazione via internet, il nuovo processo al quale si comincia ad assistere è quello di un'attività amministrativa che, sempre più frequentemente, ricorre a forme di automazione della decisione amministrativa. Si pensi al procedimento per la formazione delle liste dei professori universitari che possono far parte delle commissioni per l'ASN (Abilitazione scientifica nazionale)¹⁷. Tale ipotesi è un esempio di «automazione del provvedimento» per la dichiarazione di “sorteggiabilità” di quanti aspirino a divenire commissari, nel procedimento di attribuzione dell'abilitazione scientifica per rivestire il ruolo di professore universitario. Molti regolamenti comunali ricorrono a un algoritmo al fine di determinare l'ammontare della sanzione paesaggistica, ai sensi dell'art. 167, comma 5, del D.lgs. 42 del 2004. Assai frequenti sono anche i provvedimenti di esclusione dalle procedure concorsuali, la cui domanda di partecipazione avviene attraverso una piattaforma informatica, materia che ha conosciuto un ricco contenzioso amministrativo maturato in tutte quelle ipotesi in cui viene disposta l'esclusione dalla procedura per problemi legati al cattivo funzionamento del sistema informatici. In altri casi ancora, le amministrazioni hanno fatto ricorso a sistemi informatici per i provvedimenti di assegnazione delle farmacie¹⁸. Più di recente, il ricorso all'algoritmo si è avuto nella vicenda nota come la riforma della “buona scuola”. Con la legge n. 107 del 2015, il Miur aveva avviato un Piano straordinario di assunzioni a tempo indeterminato e di mobilità su scala nazionale,

¹⁷ M. D'ANGELOSANTE, “La consistenza del modello dell'amministrazione invisibile nell'età della tecnificazione della formazione delle decisioni alla responsabilità per le decisioni”, in S. CIVITARESE MATTEUCCI – L. TORCHIA (a cura di), “La tecnificazione”, pag.165.

¹⁸ Vedi Sent. Tar Lazio, Roma, sez. III, 3 luglio 2018, n. 7368; Sent. CdS, sez. VI, 7 novembre 2017, n. 5136, Sent. Tar Trentino-Alto Adige, sez. I, 15 aprile 2015, n. 149.

riguardante la scuola primaria e secondaria, nell'ambito di un progetto complessivo di riforma della scuola. Le assunzioni erano avvenute anche attraverso un piano di trasferimenti interprovinciali del personale docente (c.d. mobilità della "buona scuola"), la cui gestione è stata attuata attraverso il ricorso a un codice sorgente, elaborato da una società privata, la HPE Services S.r.l., su incarico del Miur, al fine di consentire all'amministrazione di svolgere più agevolmente la complessa procedura di mobilità dei docenti. In questa vicenda, l'algoritmo aveva sostituito il procedimento amministrativo, nel senso che, l'individuazione della sede spettante al singolo docente nell'ambito della mobilità è avvenuta attraverso l'implementazione del predetto algoritmo, per mezzo del codice sorgente, elaborato dalla società HPE Service S.r.l. La vicenda è divenuta nota, anche perché dall'applicazione di tale algoritmo è scaturito un cospicuo contenzioso dinanzi al giudice amministrativo, nonché davanti al giudice del lavoro.

Occorre incentrare l'analisi sui profili di ammissibilità di tali forme variabili di decisioni automatizzate, per ricondurre a sistema le principali questioni di integrazione dell'algoritmo con i principi del diritto amministrativo ad esso sottesi: in particolare, l'individuazione dei criteri di imputazione e le conseguenti forme di responsabilità a cui le stesse rimandano.

È opinione diffusa, sia dottrina che in giurisprudenza¹⁹, che il terreno di elezione della decisione amministrativa in forma automatizzata sarebbe quello dell'attività vincolata, mentre la stessa sarebbe preclusa nel campo dell'attività discrezionale. Ciò perché, l'attività vincolata di un'amministrazione implica la nota sequenza *norma-fatto-effetto*, tale per cui l'individuazione univoca ed incontrovertibile dei presupposti fissati dalla legge rende certa la conseguente decisione amministrativa²⁰. Per tale ragione, è possibile per l'attività vincolata affidare a un *software* la costruzione dei passaggi necessari: si realizza così l'immissione di una serie di *input*, vale a dire di presupposti predeterminati dalla legge, cui segue lo svolgimento «di una serie finita di passi elementari», cioè la verifica della sussistenza di quei presupposti nel caso di specie,

¹⁹ Cass. Civ., sez. I, 28 dicembre 2000, n. 16204, secondo cui «sono atti amministrativi informatici in senso stretto quegli atti provenienti dalla p.a., direttamente ed automaticamente elaborati dal sistema informatico, in quanto non richiedono valutazioni discrezionali e motivazioni correlate alla particolarità del caso concreto»; M. D'ANGELOSANTE, op. cit., p. 164; P. OTRANTO, "Decisione amministrativa e digitalizzazione della p.a.", in *federalismi.it*; F. PATRONI GRIFFI, "La decisione robotica e il giudice amministrativo", in *giustizia-amministrativa.it*.

²⁰ Su tali questioni, qui semplicemente evocate, si veda E. CAPACCIOLI, "Manuale di diritto amministrativo", Padova, 1983, p. 267; A. PROTO PISANI, "Appunti sulla c.d. tutela costitutiva e sulle tecniche di produzione degli effetti sostanziali", in *Riv. dir. proc.*, 1991, 62 ss; più in generale, N. IRTI, "Norme e fatti. Saggi di teoria generale del diritto", Milano 1984, p. 51 ss; rimane centrale, in tema di efficacia giuridica, A. FALZEA, "Teoria dell'efficacia giuridica", oggi in "Ricerche di teoria generale del diritto e di dogmatica giuridica", vol. I, Milano, 1999, p. 45 ss; in giurisprudenza si veda Cass., Sez. Un., 4 maggio 2004, n. 8430.

per giungere alla «soluzione del problema», che coincide con la decisione finale, o *output*²¹. Al contrario, una simile operazione non potrebbe trovare applicazione nell'ambito dell'attività discrezionale che, invece, implica la sequenza *norma-potere-effetto* e che presuppone un apprezzamento e una valutazione comparativa di più interessi pubblici e privati, il cui svolgimento non può in alcun modo essere affidato alla macchina.

In realtà, la questione non è così semplice, non solo perché la distinzione sopra esposta tra attività vincolata e attività discrezionale non è unanimemente condivisa²², ma soprattutto perché, anche a volere ammettere che l'attività vincolata si presti maggiormente all'automazione della decisione, è pur vero che in taluni casi anche siffatta attività implica un processo di valutazione, o quantomeno di interpretazione, rispetto al presupposto che giustifica l'adozione dell'atto. Circostanza questa, che rimanda all'altra questione rilevante, ossia l'imputazione dell'atto automatizzato e la relativa responsabilità. Se, infatti, il ricorso alla procedura automatizzata da una macchina risponde a logiche di efficienza ed efficacia dell'azione amministrativa, sulla base del presupposto che, laddove l'attività tradizionalmente svolta dal funzionario venga affidata a una macchina, si riducono i tempi di realizzazione e si ottengono soluzioni certe ed esatte, ciò nonostante, a parte le frequenti ipotesi di fallibilità del *software* (vedi i casi frequenti di *malware*), l'automazione dell'attività amministrativa non può mai comportare la totale sostituzione dell'essere umano nelle scelte amministrative, e la stessa attività deve essere imputata all'amministrazione nel rispetto del principio di responsabilità. Il problema centrale è il carattere non neutrale dell'algoritmo e la sua scarsa trasparenza. Questa considerazione emerge in tutta la sua criticità nel caso della “buona scuola” che mi accingo a descrivere.

Una prima sentenza²³ aveva avuto ad oggetto il diritto di accesso all'algoritmo. L'istanza di accesso era stata formulata da un'organizzazione sindacale ed era giustificata dalla necessità di garantire l'eventuale diritto di difesa degli iscritti alla stessa organizzazione, nell'eventualità di un'impugnazione del provvedimento di assegnazione della sede di docenza. Il Miur aveva esibito il documento descrittivo dell'algoritmo che gestiva il *software*, negando, invece, l'accesso al codice sorgente, in quanto riteneva che lo stesso dovesse essere protetto dai principi in materia di proprietà intellettuale. Il Tar ha, invece, consentito l'accesso, perché il *software* è il provvedimento amministrativo: nella ricostruzione fatta dai giudici si sostiene che «l'algoritmo è diretta espressione dell'attività svolta dalla pubblica amministrazione che è indubbiamente attività di pubblico interesse, in quanto relativo

²¹ P. FERRAGINA – F. LUCCIO, “Il pensiero computazionale. Dagli algoritmi al coding”, Bologna, 2017.

²² F. SAITTA, “Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo”, in *Riv.dir.amm.elettronico*, disponibile on line, 2003, 10.

²³ Tar Lazio, sez. III bis, 14 febbraio 2017, n. 3769.

all'organizzazione del servizio di pubblica istruzione. Tale algoritmo è entrato nella procedura di mobilità quale elemento decisivo».

Pur non condividendo del tutto la suddivisione sopra menzionata, secondo cui l'automazione della decisione amministrativa può essere ammessa nell'attività vincolata, ma non in caso di attività discrezionale, il Tar afferma che nel caso di specie si è, comunque, in presenza di attività vincolata, particolarmente complessa in considerazione degli innumerevoli elementi che devono essere valutati: ciò non comporta un apprezzamento discrezionale, trattandosi di elementi di tipo oggettivo e di immediato riscontro, che l'Amministrazione ha il dovere di acquisire al procedimento e di interrelazionare correttamente tra loro, ai fini dell'adozione dell'atto finale. Dunque, nel caso considerato, il *software* *«assume una rilevanza centrale nel procedimento amministrativo»*. Tenuto conto che il *software* ha natura informatica, che la sua elaborazione è imputabile ad una società esterna e non all'amministrazione e che la sua funzione è di ausilio e di supporto rispetto all'attività dell'amministrazione e del funzionario, il Tar conclude nel senso che *«è con il software che si concretizza la volontà finale dell'amministrazione procedente»* e *«che l'amministrazione costituisce, modifica o estingue le situazioni giuridiche individuali»*. Per tale ragione, il Tar, con l'ordinanza soprarichiamata, ha ordinato la esibizione del *software*, annullando il diniego di accesso opposto dall'amministrazione.

Diversa è, invece, l'impostazione seguita dal Tar in una diversa sentenza²⁴, sempre relativa alla vicenda della “buona scuola”, ma riguardante l'impugnazione della graduatoria di mobilità, nella quale i ricorrenti contestavano il trasferimento in province più lontane da quella della propria residenza o da quella indicata come scelta prioritaria, sottolineando, soprattutto, il fatto che nelle predette province fossero presenti posti disponibili. In tal caso, i privati lamentavano prevalentemente l'assenza di ogni attività amministrativa, essendo stata integralmente affidata la decisione sulla mobilità alla procedura informatica. A differenza di quanto sostenuto nella precedente pronuncia, in tale caso il Tar ha stigmatizzato l'assenza *«di una vera e propria attività amministrativa, essendosi demandato a un impersonale algoritmo lo svolgimento dell'intera procedura di assegnazione dei docenti alle sedi disponibili»*, con evidente pregiudizio dei principi di trasparenza, di partecipazione e di imparzialità dell'amministrazione. In tale vicenda il giudice amministrativo afferma che la procedura così automatizzata non può mai sostituire *«l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata a un funzionario persona fisica è in grado di svolgere»*, anche e soprattutto al fine di assicurare *«l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale e di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento»*. Anche volendo

²⁴ Tar Lazio, Roma, sez. III bis, 11 luglio 2018, n. 9230.

ammettere che la procedura informatica possa dare un esito corretto e indiscutibile, rimane il fatto che una decisione del tutto automatizzata è priva di motivazione, con grave pregiudizio per le aspettative di tutela dei privati, particolarmente delicate e rilevanti, dal momento che nella vicenda considerata la decisione amministrativa ha un impatto rilevante sulla vita lavorativa dei docenti, incidendo inevitabilmente sui diritti costituzionalmente garantiti.

Le due sentenze sopraesaminate presentano una contraddizione intrinseca. Nel primo caso, per l'esigenza comprensibile e condivisibile di consentire l'accesso al codice sorgente, al fine di assicurare la garanzia del diritto di difesa dei ricorrenti, il Tar si spinge ad affermare che *“l'algoritmo è il provvedimento amministrativo”* e, dunque, deve essere esibito. Nel secondo caso, al contrario, pur se la finalità rimane quella di garantire le aspettative di tutela dei ricorrenti, il Tar esclude che l'algoritmo possa sostituire integralmente il procedimento e il provvedimento amministrativo, nonostante si tratti di una vicenda analoga a quella precedentemente esaminata e si possa affermare che si tratti di attività vincolata, nella quale è assente (o quasi del tutto assente) ogni apprezzamento discrezionale e, dunque, una valutazione comparativa di interessi. Alla luce dei principi di partecipazione e di istruttoria procedimentale a cui l'Amministrazione è tenuta a conformarsi, unitamente all'obbligo di motivazione che in caso di decisione automatizzata rimarrebbe inosservato, occorre ritenere necessaria la riconducibilità di ogni decisione amministrativa a un organo, che ne è responsabile, escludendo forme di tale automatizzazione della decisione.

L'algoritmo deve, dunque, considerarsi il presupposto su cui la decisione si fonda, secondo il modello, già noto, dell'apprezzamento tecnico come presupposto del provvedimento amministrativo. Così posta la questione, viene in rilievo il rapporto assai discusso tra tecnica ed amministrazione, che a sua volta trova soluzione nella nozione di discrezionalità tecnica²⁵. Secondo la più tradizionale elaborazione, a differenza della discrezionalità pura, che implica la ponderazione tra i diversi interessi coinvolti dalla decisione amministrativa (c.d. *Ermessen*), la discrezionalità tecnica non necessariamente comporta una ponderazione comparativa degli interessi, bensì tra fatti da accertare alla stregua di canoni scientifici, tecnici, letterari, artistici, ecc.

Il potere di scelta in ordine allo strumento più idoneo ad assicurare la migliore cura dell'interesse pubblico è un potere successivo, che consegue all'esito del giudizio tecnico, laddove questo abbia un esito incerto che apre a più soluzioni.

In ogni caso, la valutazione tecnica e l'accertamento tecnico (a seconda del livello di esattezza della scienza preso a modello di riferimento) operano come presupposto della

²⁵ Sull'autonomia concettuale della tecnica rispetto all'esercizio del potere discrezionale vedi M. S. GIANNINI, *“Il potere discrezionale della pubblica amministrazione. Concetto e problemi”*, Milano, 1939; V. BACHELET, *“L'attività tecnica della pubblica amministrazione”*, 1967; F. LEDDA, *“Potere, tecnica e sindacato giudiziario”*, in *“Studi in memoria di V. Bachelet”*, Milano, 1987, p. 247.

decisione amministrativa²⁶. Ed è proprio questa la chiave di lettura che, sia pure implicitamente, rileva dal confronto tra le due sentenze.

Come evidenziato dagli stessi giudici, l'automatizzazione della procedura si traduce in un supporto di tipo tecnico a un'attività che altrimenti dovrebbe essere svolta dal funzionario e, in tal modo, è possibile conseguire in tempi più ragionevoli la decisione finale. Ma questa attività non può integralmente sostituire la decisione finale, perché ne sarebbero pregiudicati i principi di imparzialità, di buon andamento e di trasparenza dell'azione amministrativa.

Prescindendo dalla distinzione tra attività vincolata ed attività discrezionale, la soluzione più condivisibile è quella di considerare la procedura automatizzata alla stregua di un accertamento tecnico, che presuppone, comunque, l'adozione di un provvedimento finale che ne faccia proprio l'esito.

Riprendendo le osservazioni svolte dal giudice amministrativo, le procedure informatiche sono predisposte *«in funzione servente»* e ad esse va affidato un *«ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo»*.

Tale ricostruzione è confermata dal Supremo Consesso Amministrativo che, con la sentenza dell'8 Aprile 2019, n. 2270, in una vicenda relativa all'impugnazione della proposta di assunzione conseguente al piano straordinario di mobilità dei docenti, ha prospettato una soluzione per certi versi intermedia rispetto alle pronunce dei giudici di prime cure.

Per un verso, il Consiglio di Stato ammette che in alcuni casi come quello relativo alla "buona scuola", il ricorso a una procedura automatizzata deve ritenersi legittimo, anzi utile e vantaggioso, poiché in presenza di procedure seriali o standardizzate, consente di addivenire a una decisione in tempi più celeri, a garanzia dell'interesse pubblico e dei principi di efficienza e di buon andamento.

D'altra parte, prosegue: *«l'utilizzo di procedure robotizzate non può essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa»*. Ciò significa che, se è vero che *«l'algoritmo, ossia il software deve essere considerato a tutti gli effetti come un atto amministrativo informatico»* che si fonda su una *«regola tecnica»*, va, altresì, considerato che l'atto così generato, e la regola tecnica che esso incorpora, devono essere soggetti ai principi fondamentali dell'azione amministrativa, tra cui la trasparenza e la conoscibilità, nonché il pieno sindacato del giudice amministrativo, il quale deve poter valutare *«la correttezza del processo informatico in tutte le sue componenti: dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione»*.

²⁶ Si veda F. VOLPE, "Discrezionalità tecnica e presupposti dell'atto amministrativo", in *Dir. Amm.*, 2008, 791.

Il punto è che può accadere che l'algoritmo, inteso come regola tecnica, assuma un ruolo che si spinga al di là del mero presupposto su cui si fonda la decisione, potendo giungere a costituire un sistema di formazione della stessa volontà procedimentale.

Il tema evoca il rapporto tra tecnica e amministrazione e la soluzione potrebbe essere quella che individua nel sapere tecnico e scientifico, e dunque nell'algoritmo, il presupposto della decisione amministrativa.

Per altro verso, il *quid novi* dell'algoritmo consiste nella possibilità che esso, in quanto strumento di formazione della volontà dell'amministrazione, possa sostituirsi alla decisione finale. Pertanto, sulla scorta delle argomentazioni condotte dal giudice amministrativo, come pure dalle indicazioni contenute nel Regolamento UE 2016/679, appare utile provare a cogliere “*nella sequenza di passaggi elementari*” che caratterizzano un algoritmo e che, dunque, costituiscono l'essenza della decisione automatizzata, i principi fondamentali dell'ordinamento che assicurano il corretto dispiegarsi del procedimento amministrativo.

Occorre, dunque, enucleare un complesso di regole e principi che definiscano “*un giusto processo tecnologico*”, c.d. *Digital o Technological Due Process*, secondo un'espressione che riassume l'esigenza che gli algoritmi che ci governano riflettano i valori fondanti e condivisi della nostra società e siano soggetti al controllo democratico²⁷.

Occorre considerare anche il rapporto tra algoritmi e diritti fondamentali della persona alla luce degli artt. 13 e 14 del GDPR, secondo cui l'interessato deve essere informato dell'eventuale esecuzione di un processo decisionale automatizzato e dell'art. 22 (c.d. *principio di non esclusività*), che esclude la possibilità che la decisione sia basata unicamente sul trattamento automatizzato²⁸.

Il Sistema di tutela deve, dunque, incentrarsi sul principio di trasparenza, condizione necessaria per la comprensione dei meccanismi di funzionamento dei processi decisionali compiuti dalle macchine. La trasparenza, in tal caso, è intesa quale sinonimo di conoscenza del percorso seguito per giungere alla decisione automatizzata. Ed è in un'ottica di trasparenza che, da più parti, si sollecita l'intervento di

²⁷ A. MORETTI, “Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento UE 2016/679”, in “Diritto dell'informazione e dell'Informatica”, 2018, 799; D. KEATS CITRON, “Technological Due Process”, 85, Wash. Un.L.Rev.1249; D. KEATS CITRON & F. PASQUALE, “The Scored Society: Due Process for Automated Predictions”, 89 WASH.L.REV. 1 (2014); K. CRAWFORD & J. SCHULTZ, “Big Data and Due Process: toward a Framework to Redress Predictive Privacy Harms”, 55 B.C.L. REV.93 (2014).

²⁸ Su questa falsariga si vedano, ad esempio, EPRS /European Parliamentary Research Service - *Panel for the future of Science and Technology* (STOA), “A governance framework for algorithmic accountability and transparency”, March 2019; High-Level Expert Group on Artificial Intelligence, “Ethics guidelines for trustworthy AI”, April 2019; in tal senso, M. ZALNIERIUTE, L. BENNETT MOSES, G. WILLIAMS, “The Rule of law and Automation of Government Decision-Making”, in “The modern law review”, 2019, 425.

“algoritmisti”, una sorta di consulente tecnico d’ufficio con competenze informatiche che svolga il ruolo di controllore delle società dell’algoritmo, con il compito di attestare la correttezza di un certo algoritmo²⁹.

Il tema centrale nella decisione automatizzata diviene, così, quello della sua “spiegabilità” (*explanability*), attraverso l’individuazione di strumenti che consentano di interpretarne il codice sorgente per ricostruire i passaggi logici che lo compongono e stabilire, per questa via, i passaggi e le procedure che hanno determinato i risultati. Sotto tale profilo, la spiegabilità della procedura automatizzata, la cui necessità è stata sottolineata dal Consiglio di Stato nella sentenza sopra richiamata, non si allontana molto dalla necessaria motivazione del provvedimento: l’amministrazione che assume una decisione attraverso il ricorso a un algoritmo deve essere in grado di spiegare l’*iter* logico-giuridico che conduce alla decisione finale.

Trasparenza e conoscenza, o spiegabilità, della procedura automatizzata assicurano, a loro volta, un’adeguata *partecipazione* del privato alla procedura algoritmica. In qualunque passaggio della procedura, deve sempre essere assicurata al privato la facoltà di intervenire nel procedimento, di interloquire con il responsabile, di presentare memorie e documenti per orientare la decisione che lo riguarda, ma soprattutto per anticipare in sede procedimentale le proprie aspettative di tutela. Ed è proprio questo il *vulnus* della decisione sulla mobilità dei docenti che, nella ricostruzione del TAR, ha comportato l’illegittimità della decisione medesima affidata per intero ad un algoritmo.

L’esigenza è quella di evitare che l’automatizzazione della procedura possa generare un processo di spersonalizzazione della decisione, con un duplice effetto distorsivo: per un verso, perché impedisce la virtuosa partecipazione del privato al procedimento, in quanto manca un interlocutore al quale il privato possa rivolgersi; per altro verso, perché rischia di generare una polverizzazione della responsabilità conseguente alla decisione assunta³⁰. È, dunque, nel processo di procedimentalizzazione dell’attività algoritmica che si declina la tutela per il privato.

Se l’algoritmo si proietta nella decisione finale, sino a sostituirla del tutto, ancor di più i profili di interesse si concentrano sulle prospettive di tutela e le garanzie dei privati dinanzi a una decisione pubblica assunta attraverso procedure automatizzate. In tal caso, oltre ai menzionati principi di trasparenza e partecipazione, a venire in rilievo è soprattutto il principio di *responsabilità* declinato in una duplice direzione: se, infatti, esso impone di ritenere sempre responsabile il funzionario che abbia agito “in

²⁹ V. MAYER-SCHOENBERGER, K. CUKIER, “*Big Data. Una rivoluzione che trasformerà il nostro modo di vivere*”, Garzanti, Milano, 2016.

³⁰ Sul tema, si rinvia alle suggestive riflessioni di E. PICOZZA, “*Problems about enforcement*”, in E. PICOZZA, “*Neurolaw. An Introduction*”, Ed. Springer, 2016, p. 79 ss.

violazione dei diritti”³¹, sotto altro profilo, la decisione automatizzata implica la necessità di una responsabilità già nella “costruzione” e nell’“educazione” dell’algoritmo. Il modo in cui l’amministrazione decide di selezionare e scegliere i dati su cui dovrà essere costruito l’algoritmo, ne condiziona fatalmente il risultato.

È in questa fase, ad esempio, che si è parlato di “non discriminazione algoritmica”³², nel senso che i dati su cui si sviluppa l’algoritmo devono essere selezionati in modo da evitare ogni effetto discriminatorio all’esito della decisione algoritmica. Se, allora, l’automatizzazione di una decisione pubblica consente la formazione della volontà dell’amministrazione, il processo che ne sta alla base, dall’inserimento degli *input* alla gestione dell’*output*, deve conformarsi ai principi generali che governano l’agire amministrativo; deve cioè, essere chiaro, conoscibile e partecipato per rispondere adeguatamente alle esigenze di tutela dei destinatari della decisione automatizzata. Il rischio, infatti, risiede nella circostanza che l’assunzione sempre più frequente e nei settori più variegati di decisioni automatizzate, che dovrebbero proiettare l’amministrazione verso forme di azioni innovative, tecnologicamente avanzate, assicurando l’efficienza, la correttezza e la oggettiva imparzialità della decisione, possa generare un arretramento sotto il profilo delle garanzie procedurali del cittadino, dalla partecipazione in senso tecnico, attraverso la presentazione di memorie e documenti, alla possibilità di una concreta interlocuzione con il responsabile del procedimento.

Per questo, si fa sempre più stringente la necessità di ancorare il procedimento di formazione della decisione automatizzata ai principi generali che conformano l’agire amministrativo, ivi inclusa le condizioni per l’esercizio di un sindacato giudiziario e delle relative conseguenze, anche in termini di responsabilità dell’amministrazione e dei suoi agenti³³. Al di là dell’inquadramento teorico della responsabilità dell’amministrazione in generale, è comunque evidente che se la decisione automatizzata è espressione di un potere, rispetto al cui esercizio l’algoritmo costituisce un presupposto ovvero coincide con il provvedimento, sovrapponendosi ad esso, quella

³¹ Sul principio di responsabilità dell’amministrazione, v. A. POLICE, “Il principio di responsabilità”, in M. RENNA, F. SAITTA, (a cura di) “Studi sui principii del diritto amministrativo”, Milano, 2012, 195 ss.; sull’art. 28 Cost., v. *ex multis*, M. CLARICH, “La responsabilità della pubblica amministrazione nel diritto italiano”, in *Riv. Trim. Dir. Pubbl.*, 1989, 1085.

³² A. SIMONCINI, “L’algoritmo incostituzionale, intelligenza artificiale, il futuro delle libertà”, cit., che riporta il caso della c.d. “decisione Compas”, rispetto alla quale, da uno studio condotto su un campione di 10.000 imputati, nella predizione della recidiva l’algoritmo sovrastimava sistematicamente il rischio di recidiva per gli imputati neri ed altrettanto sistematicamente sottostimava il rischio per i bianchi.

³³ Il tema della responsabilità dell’amministrazione è estremamente complesso e variegato e racchiude una pluralità di questioni che difficilmente possono trovare composizione: per un’idea del contesto al quale ci si riferisce, v. A. CASSATELLA, “La responsabilità funzionale nell’amministrare. Termini e questioni”, in *Dir. Amm.*, 2018, 677.

appena considerata rappresenterebbe un'ipotesi di responsabilità per illegittimo esercizio del potere, la cui azione trova oggi fondamento nell'art. 30 c.p.a.

Dopo la sentenza n. 500 del 1999 sulla risarcibilità dell'interesse legittimo e dopo l'entrata in vigore del codice del processo amministrativo nel 2010, la previsione di una specifica azione di condanna dinanzi al giudice amministrativo, soggetta a un termine di decadenza, consente di ipotizzare un superamento del paradigma di responsabilità extracontrattuale, lasciando invero irrisolte non poche questioni, tra cui quella della giurisdizione³⁴.

Questa è, dunque, la linea interpretativa che ha tracciato il Consiglio di Stato: superando ogni possibile limite al sindacato giudiziario sulla discrezionalità amministrativa e tecnica, rivendica la necessità di esercitare il proprio sindacato sull'algoritmo che costituisce l'essenza della decisione finale e sulla correttezza di tutti i passaggi della procedura informatica, ivi inclusa la costruzione dell'algoritmo, l'inserimento dei dati e la loro gestione. La questione, così impostata, rimanda al problema della fallibilità del *software*, al quale ci si affida sul presupposto che esso sia in grado di offrire una soluzione efficiente, perché adottata in tempi ridotti e non soggetta ad errore, ma che nei fatti può dar luogo a risultati non corretti, come mostra bene il caso delle assegnazioni dei docenti nella procedura di mobilità avviata con la riforma della "buona scuola". È evidente che tali assegnazioni erano avvenute in modo non coerente alla scelta prioritaria formulata dagli interessati, con la conseguenza che alcuni docenti erano stati destinati in sedi più distanti da quella indicata o da quella di residenza e pur essendo disponibili svariati posti presso le sedi di elezione. A fronte del margine di errore del *software*, si fa sempre più sentita la necessità di assicurare la trasparenza, la conoscibilità e la partecipazione del privato al procedimento di formazione di ogni decisione pubblica, sia nell'ipotesi in cui l'algoritmo funga da presupposto per una decisione successiva, sia nel caso in cui il suo prodotto coincida

³⁴ E. FOLLIERI, "La tipologia delle azioni proponibili", in F. G. SCOCA (a cura di), "Giustizia amministrativa", Torino, 2017, p. 190 ss.; V. CERULLI IRELLI, "Giurisdizione amministrativa e pluralità delle azioni (dalla Costituzione al Codice del processo amministrativo)", in *Dir. Proc. Amm.*, 2012, 436. In termini assai generali e senza alcuna pretesa di esaustività, una ricca costruzione storica del dibattito sopra richiamato si trova in F. G. SCOCA, "L'interesse legittimo. Storia e teoria", Torino, 2017; nonché, per una diversa ricostruzione della natura dell'interesse legittimo, G. GRECO, "Dal dilemma diritto soggettivo-interesse legittimo, alla differenziazione interesse strumentale-interesse finale", in *Dir. amm.*, 2014, 479; C. CASTRONOVO, "La «civilizzazione» della pubblica amministrazione", in *Europa e dir. priv.*, 2013, 637. Più in generale, sulla responsabilità civile, sul cui paradigma si è ricostruita la nozione di responsabilità dell'amministrazione per lesione dell'interesse legittimo, da ultimo nella trattatistica si vedano, tra gli altri, C. CASTRONOVO, "Responsabilità civile", Milano, 2018; G. ALPA, "La responsabilità civile. Principi", Milano, 2018; P. TRIMARCHI, "La responsabilità civile: atti illeciti, rischio, danno, responsabilità civile", 2021; A. DI MAJO, "Profili della responsabilità civile", Torino, 2010; P. G. MONATERI, "La responsabilità civile", Torino, 2006.

con la stessa decisione. Fermo restando che, per il principio di responsabilità, l'amministrazione, e non un *software*, deve rispondere dei danni prodotti. In altri termini, applicato al processo di automazione della decisione pubblica, il principio di responsabilità si traduce, in un primo tempo, nell'esigenza di limitare il ruolo della tecnica in generale, e dell'algoritmo in particolare, a strumento servente dell'amministrazione, mantenendo così in capo all'agente la competenza e la responsabilità che deriva dall'assunzione della decisione³⁵.

In modo complementare, il medesimo principio potrebbe condurre a stabilire, ad esempio, obblighi di tipo fiduciario a carico di chi raccoglie, analizza e utilizza informazioni nei confronti sia dei diretti interessati che della collettività in generale³⁶.

Ancora, sempre in attuazione del principio di responsabilità, potrebbe essere auspicabile adottare specifiche prescrizioni tecniche per la progettazione di algoritmi "equi", disegnati, cioè in modo da rispettare i valori fondanti della nostra società³⁷.

Dinanzi alla continua evoluzione della scienza e alla velocità delle trasformazioni tecnologiche, un atteggiamento di resistenza rispetto all'impiego di algoritmi nella formazione della volontà procedimentale risulta ingiustificato, oltre che di difficile

³⁵ Qui, al di là del modello di responsabilità accolto, e del conseguente regime giuridico, la questione centrale riguarda il profilo dell'imputazione della responsabilità in capo all'amministrazione, su cui la giurisprudenza pare avere assunto un orientamento che oscilla tra la sussistenza della c.d. colpa d'apparato e la ricerca di un errore scusabile; CdS, sez. V, 20 agosto 2013, n. 4189, secondo cui *«l'imputazione alla p.a. di una responsabilità extracontrattuale non può avvenire sulla base del mero dato obiettivo dell'illegittimità dell'azione amministrativa, ma il giudice deve svolgere una più penetrante indagine, non limitata al solo accertamento dell'illegittimità del provvedimento in relazione alla normativa ad esso applicabile, bensì estesa anche alla valutazione della colpa, non del funzionario agente e da riferire ai parametri della negligenza o imperizia, ma dell'Amministrazione intesa come apparato, che sarà configurabile nel caso in cui l'adozione e l'esecuzione dell'atto illegittimo e lesivo dell'interesse del danneggiato siano avvenute in violazione delle regole di imparzialità, di correttezza e di buona amministrazione alle quali l'esercizio della funzione amministrativa deve ispirarsi»*; nonché CdS, sez. V, 18 gennaio 2016, n. 148, che afferma che *«ai fini della configurabilità della responsabilità della Pubblica Amministrazione devono ricorrere i presupposti del comportamento colposo, del danno ingiusto e del nesso di consequenzialità tra i fatti; pertanto, l'imputazione della colpa alla Pubblica Amministrazione non può avvenire, sulla base del mero dato obiettivo dell'illegittimità dell'atto amministrativo e, comunque, essa va negata in particolare quando l'indagine conduca al riconoscimento dell'errore scusabile per la sussistenza di contrasti giudiziari, per l'incertezza del quadro normativo di riferimento o per la complessità della situazione di fatto»*.

³⁶ J. M. BALKIN, "Information Fiduciaries and the First Amendment", 49 U.C Davis L.REV.1183 (2015); per una recente ricognizione del tema degli obblighi fiduciari in prospettiva comparatistica, si rinvia a E. J. CRIDDLE, P. B. MILLER & R. H. SITKOFF, "Oxford Handbook of Fiduciary Law", Oxford, 2018.

³⁷ S. BAROCAS, "Accountable Algorithms", 165 U.PA.L.REV. 633 (2017). Con ciò sfruttando il codice sorgente e l'architettura della rete come strumenti per governare la sfera digitale (il riferimento è a L. LESSIG, "Code.Version 2.0", New York, 2006). Rimane ovviamente la difficoltà di definire tali valori e principi e di tradurli in comandi eseguibili dalle macchine. Vedi J. KROLL, "Accountable Algorithms", 165 Univ.Penn.L.Rev. 2017.

attuazione, dato che il ricorso a *software* che possano supportare l'azione amministrativa è destinato a essere sempre più frequente e gli ambiti applicativi delle decisioni automatizzate aumentano di continuo.

Di recente, il Professore Giorgio Parisi, vincitore del premio Nobel per la fisica 2021, ci ha illustrato le dinamiche dei sistemi complessi su scala atomica e planetaria, dimostrandoci che la massa è un fenomeno dinamico. Anche il mondo degli algoritmi presenta una complessità che il giurista deve cercare di regolare per metterla al servizio dell'interesse dell'uomo. È relativamente recente la notizia che in Sardegna è stata avviata una sperimentazione, che riguarda ancora pochi comuni, per il monitoraggio del territorio attraverso satelliti radar che, tra i diversi obiettivi, si propone anche quello di individuare manufatti ed edifici abusivi.

In particolare, la *NeMea Sistemi* – che dal 2015 è socia del distretto aerospaziale della Sardegna – intende calcolare «un algoritmo che consentirà di misurare se i fabbricati si innalzano oppure no, offrendo alla pubblica amministrazione uno strumento formidabile per individuare abusi e interventi sui fabbricati»³⁸.

La questione è molto complessa, se si considera il noto orientamento della giurisprudenza amministrativa sulla possibilità di valutare le aerofotogrammetrie quali prove dell'avvenuto abuso³⁹. Negare l'utilità degli algoritmi nell'attività amministrativa potrebbe rappresentare una forma di *neoluddismo*, la “*c.d. paura del nuovo imponderabile*”, non auspicabile in un'era postmoderna. L'utilizzo dell'intelligenza algoritmica implica, però, che l'esercizio del potere pubblico debba essere chiamato a rispondere degli eventuali pregiudizi arrecati, laddove incide in misura apprezzabile sulla libertà dei singoli. L'obiettivo è allora quello di definire un sistema adeguato di *accountability* per le decisioni assunte in modo automatizzato, senza dover rinunciare ai vantaggi innegabili scaturenti dall'innovazione digitale. Occorre delineare una nozione di “algoritmo dominabile”, che consenta di costruire la logica della decisione.

Qualche Autore⁴⁰ sottolinea la distinzione tra due tipi di algoritmo: l'algoritmo definito tradizionale e quello che si inserisce in un contesto di intelligenza artificiale. Tale impostazione duale è di fondamentale importanza, perché in base ad essa si delineano situazioni giuridiche soggettive completamente differenti, rischi differenti e, quindi, esigenze di tutela del tutto differenti.

³⁸ G. SIAS, “*La Nuova Sardegna*”, 2 febbraio 2018.

³⁹ Vedi da ultimo, Cons. Stato, sez. VI, sentenza n. 2363 del 10 aprile 2019, con la quale è stata riformata la sentenza di primo grado concernente la sospensione dei lavori di montaggio di una veranda, il diniego di condono e l'ordine di demolizione, per l'impossibilità di stabilire con esattezza la data di ultimazione del manufatto di cui si contestava la regolarità.

⁴⁰ M. CORRADINO, “*Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*”, pubblicato il 10 settembre 2021 sul sito www.giustizia-amministrativa.it.

“L’algoritmo tradizionale è uno strumento a cui si ricorre spesso nell’ambito dell’attività normativa o amministrativa. In questa prospettiva, l’algoritmo diventa una rappresentazione della norma e della sua interpretazione applicativa; si traduce in un vero e proprio metodo matematico per applicare la legge.

La legge, quindi, in questo caso, precede l’algoritmo che diventa solo un mezzo per applicare più celermente le scelte normative. Talvolta si tratta di algoritmi semplici, quasi coincidenti con formule matematiche più o meno complesse: si pensi, in via esemplificativa, ai criteri di individuazione delle offerte economicamente più vantaggiose o agli algoritmi utilizzati dal Ministero dell’Istruzione per l’assunzione e l’assegnazione delle sedi ai docenti delle scuole che sono stati oggetto di recente di un’interessante vicenda giudiziaria oltre che di grande attenzione mediatica. In casi come questi, l’analisi dell’algoritmo consente di ricostruire la logica della decisione. L’algoritmo è “dominabile”.

Certo, talvolta la sua complessità rende più difficile l’analisi e più facile l’errore, ma si tratta pur sempre di fallacia dell’uomo, di scelte sbagliate dell’uomo in cui il vizio non è ontologicamente differente da quelli tradizionalmente incasellati nella tradizionale triade oggi scolpita dalla legge sul procedimento amministrativo: incompetenza, violazione di legge ed eccesso di potere.

Accanto all’algoritmo “tradizionale” che presuppone la partecipazione intellettuale umana, vi è, però, l’algoritmo basato sull’intelligenza artificiale che perde il carattere della “dominabilità”. In questi casi, agli algoritmi – o, meglio, all’intelligenza artificiale – viene richiesto qualcosa in più e cioè assumere decisioni al posto dell’uomo. L’intelligenza artificiale si sostituisce all’uomo nella scelta dell’atto da compiere, secondo un processo di analisi, acquisizione di dati e scelte autonome a cui la volontà umana risulta estranea”⁴¹.

In realtà, la volontà umana è ancora presente ed immanente nella fase di “creazione dell’algoritmo”, con l’immissione dei dati che devono essere il più possibile neutrali e nella fase della c.d. «educazione dell’algoritmo», poiché l’intelligenza artificiale può evolvere in intelligenza “spontaneus”, evolversi autonomamente dagli *input* dati dall’uomo. Ecco che, allora, può venire a delinarsi la c.d. *opacità* dell’algoritmo e la decisione algoritmica perde la sua decifrabilità e la sua intelligibilità.

Al termine del percorso di valutazione, rielaborazione e creazione di nuove e autonome determinazioni, essa è sempre più difficilmente ricostruibile, perché è il risultato di una combinazione di valutazioni e decisioni “esterna”, “estranea” al sistema intellettuale umano. Il percorso non è per sintassi, ma per “inferenza”. La logica del “*what if*”, tipica del nostro sistema normativo, la logica del “*norma-fatto/potere-effetto*” che è tipica del

⁴¹ Vedi M. CORRADINO, “Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future”, cit., pag.1 e 2.

nostro sistema giuridico, viene sostituita in questo quadro da una sovrapposizione di inferenze, che è elaborata e poi espressa in un altro linguaggio: il linguaggio della macchina, che è strutturalmente differente da quello umano. Tutto ciò incide sulla capacità decisionale dell'uomo e sulle sue libere scelte? Incide sull'efficacia delle leggi e sul potere regolatorio di uno Stato?

L'autore prima citato giustamente osserva⁴²: *«Quanti di noi stamattina hanno deciso di non prendere una strada soltanto, perché Google maps ha ritenuto che fosse più trafficata del solito inducendo, così, la maggior parte della popolazione a percorrerne un'altra? E la capacità di dettare e fare applicare regole è tanto più efficace quanto essa si salda con le tecniche di “nudging”, la spinta gentile che orienta determinati comportamenti senza prevedere obblighi o minacciare sanzioni. Ancora più rilevante il tema delle blockchain, una tecnologia che consente di dare certezza assoluta alle transazioni avvenute tra soggetti appartenenti ad un determinato network e che è stata oggetto di grande attenzione mediatica, in quanto struttura sulla quale viaggiano, tra l'altro, gli scambi di bitcoin. In essa la funzione di certificazione e di creazione di fiducia – che è tipica dello Stato – è esercitata in forma decentrata da tutti i soggetti che partecipano alla comunità di riferimento. In questo caso, le caratteristiche della tecnologia informatica- un registro condiviso e impossibile da modificare che registra in modo sequenziale qualunque tipo di transazione in modo che tutti i membri della comunità ne siano al tempo stesso fruitori e guardiani-permette di rinunciare ad un'Autorità pubblica centralizzata di controllo. La diffusione del modello nel settore finanziario e più in generale in quello di scambio di asset sia tangibile che intangibili dovrebbe far riflettere sulla capacità della tecnologia di cambiare il mondo giuridico nel quale siamo fin qui vissuti.*

Il disimpegno dello Stato nella formazione della norma, o quanto meno dei comportamenti, è vissuto più serenamente nel diritto civile che storicamente ha già vissuto senza traumi la liberazione dello Stato nell'affermarsi della lex mercatoria.

Ne è una testimonianza la scarsa regolamentazione legislativa degli smart contracts che viaggiano proprio sulle strutture della blockchain contenute nella legge 22 febbraio 2019 n.12. tale fonte normativa, dopo aver dettato la nozione ed averli assimilati ai contratti a forma scritta, non sente la necessità di individuare dettagliatamente la disciplina e ne rimette la struttura, regolamentazioni e contenuti all'autonomia delle parti. Il problema si caratterizza in modo diverso, però, nel diritto amministrativo che è regolazione e controllo del potere pubblico e in cui il tema dell'autonomia dell'intelligenza artificiale nell'assunzione delle decisioni si salda con quelli della sovranità, della divisione dei poteri, del collegamento necessario tra la

⁴² M. CORRADINO, “Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future”, cit., pag. 3 e 4.

decisione della pubblica amministrazione e la volontà popolare. In una parola con la democrazia».

Tale Autore pone in luce la maggiore complessità dell'utilizzo dell'algoritmo nell'attività amministrativa rispetto all'attività contrattualistica tra privati, venendo in rilievo l'esercizio del potere pubblico.

Vi sono state sentenze, come quella del TAR Lazio, sez. III, n. 4409 del 15 aprile 2021, in cui viene espressa la preoccupazione in merito alla *«abdicazione da parte del responsabile del procedimento del suo ruolo di timoniere ed anche di correttore»*. Ma maggiore apertura si riscontra nell'orientamento del Consiglio di Stato⁴³, che testualmente ha affermato: *«Non vi sono ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse»*.

Il problema reale è quello relativo alla perimetrazione dei limiti posti a garanzia dei diritti fondamentali. Tali limiti sono essenzialmente quelli che rinveniamo nel Regolamento in materia di Privacy (Regolamento UE n. 2016/679 del 27 aprile 2016, attuato dal D.lgs. 2018 n. 101⁴⁴) e che troviamo confermati nella Proposta di Regolamento del parlamento Europea e del Consiglio del 21 Aprile 2021, che stabilisce regola armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione. Sono i limiti della “conoscibilità”, della “non esclusività” e “della non discriminazione”. Tali principi delineano un'adequata tutela in caso di algoritmo

⁴³ Vedi CdS, sez. VI, sentenza n. 881 del 4 febbraio 2020.

⁴⁴ Si tenga presente che la Corte costituzionale con la sentenza n. 260 del 2021 ha dichiarato l'illegittimità costituzionale dell'articolo 18, comma 5, del decreto legislativo 10 agosto 2018, n. 101, sancendo l'illegittimità della norma che prevedeva l'interruzione *ex lege* del termine di prescrizione, relativamente ai procedimenti sanzionatori che, alla data di applicazione del regolamento n. 679/2016/UE, siano stati avviati, ma non ancora definiti con l'adozione dell'ordinanza-ingiunzione. Secondo la Corte, è evidente che *«l'interruzione automatica del termine di prescrizione quinquennale, che già di per sé rende eccessivamente squilibrato il rapporto fra privato e pubblica amministrazione, si traduca in una intollerabile compressione delle ragioni di tutela del privato»*. Si violerebbero i principi di proporzionalità e ragionevolezza, infatti *«l'amministrazione può attivarsi per la riscossione delle somme dovute in base all'ordinanza-ingiunzione prodottasi ope legis, oppure, nell'ipotesi in cui il privato presenti nuove memorie difensive ai sensi dell'art. 18, comma 4, del d.lgs. n. 101 del 2018, può emettere l'ordinanza-ingiunzione, anche oltre un quinquennio dall'unico atto che è stato notificato all'interessato: grazie all'interruzione, si sommano infatti altri cinque anni al tempo già trascorso dalla notifica della contestazione alla data di entrata in vigore del d.lgs. n. 101 del 2018. Per converso, il privato, dopo aver rispettato il termine di trenta giorni per opporsi alla contestazione della sanzione amministrativa, può doversi difendere, sempre entro trenta giorni dalla notifica della cartella o dalla notifica dell'ordinanza-ingiunzione, a distanza di oltre cinque anni dalla notifica dell'atto con il quale gli era stata contestata la violazione. Nessun'altra comunicazione, infatti, è tenuta ad effettuare l'amministrazione medio tempore, neppure con riferimento alle facoltà concesse ai privati dai primi commi dell'art. 18 e alle conseguenze derivanti a carico di coloro che non si avvalgano di tali facoltà»*.

definito tradizionale, ma siamo sicuri che tali principi possano assicurare un'adeguata tutela anche nel campo dell'intelligenza artificiale?

Il principio della conoscibilità si inserisce all'interno della trasparenza amministrativa: la conoscenza dell'algoritmo è lo strumento base per la conoscenza dell'*iter* decisionale che ne consente la valutazione sotto il profilo giuridico. Emblematico il “*Caso Loomis*” deciso dalla Supreme Court of Wisconsin⁴⁵, in cui una pena molto grave venne comminata da una corte statunitense sulla base di una valutazione di pericolosità formulata dall'intelligenza artificiale. La Corte rifiutò alla difesa il diritto di conoscere i criteri che orientarono il giudizio di pericolosità, perché nel bilanciamento tra gli interessi in gioco e tenuto conto della possibilità di giustificare la pena sulla base di altri fattori, le esigenze di tutela del segreto industriale vennero ritenute prevalenti su quelle di trasparenza e di conoscibilità dell'algoritmo.

La conoscenza dei criteri dell'algoritmo si traduce nella conoscenza del percorso logico-motivazionale del provvedimento: la *black box*, però, nucleo decisionale dell'intelligenza artificiale, risultato di sintesi della capacità della macchina di autoevoluzione cognitiva, autoapprendimento e di affinamento di criteri di conoscenza e scelta per la realizzazione più efficiente dell'obiettivo, è non conoscibile, indecifrabile per natura.

Rendere conoscibile quello che la Suprema Corte di Cassazione ha definito lo “schema esecutivo” dell'algoritmo non necessariamente svela o non necessariamente consente di svelare la correttezza della decisione. Oppure, un'altra possibilità che si potrebbe verificare è che la correttezza della decisione potrebbe essere conoscibile solo da soggetti che presentino una particolare qualificazione professionale e tecnica, una platea ristretta di pochi eletti, con la conseguenza, come sottolineato da autorevole dottrina, di creare una generazione di tecnocrati che governano il mondo. Ed è proprio per questo che, in un'ottica di acquisizione di competenze trasversali, in molte facoltà di giurisprudenza, soprattutto del Nord Europa, tra le materie giuridiche viene inserito anche il “*coding*”, passaggio più qualificato della mera “alfabetizzazione” materiale.

La giurisprudenza amministrativa insiste molto, però, anche sul principio di non esclusività fissato dall'art. 22 del citato Regolamento sulla privacy e sul necessario intervento correttivo dello *Human in the loop*, così come previsto nella Risoluzione del parlamento europeo, A9-0002/2021 del 20 gennaio 2021 sull'intelligenza artificiale. Occorre, però, considerare che non tutte le decisioni pubbliche fondate sull'intelligenza artificiale sono comprimibili in un'alternativa *on/off*. Spesso le decisioni sono multifattoriali, complesse, possono portare ad un'alternativa di risultati diversi la cui individuazione dipende dall'elaborazione dei dati, dalla loro valutazione, dall'applicazione dei principi di proporzionalità e di precauzione soprattutto dal c.d. “*Ermessen*”, dal c.d. bilanciamento degli interessi basato su valori costituzionali.

⁴⁵ *State of Wisconsin v. Eric L. Loomis*, Case no. 2015AP157-CR, 5 April-13 July 2016.

Logica umana e logica della macchina possono convivere nel medesimo procedimento senza che la prima sia in grado di sostituirsi alla seconda e spesso nemmeno di comprenderla.

Ciò potrebbe presentare dei problemi di discriminazione tra soggetti che aspirano al medesimo bene nelle ipotesi di provvedimento amministrativo plurimo, con effetti scindibili di natura discrezionale o tecnico-discrezionale; una graduatoria, ad esempio, in cui il giudice annulli la determinazione con riferimento alla posizione del solo ricorrente. In tal caso, i destinatari del provvedimento si vedranno giudicati con criteri differenti: la logica dell'uomo-giudice per il caso portato alla sua attenzione e la logica della macchina per tutti gli altri. La non esclusività non può dirsi criterio sufficiente oggi per assicurare una tutela piena ed effettiva. Va certamente integrato con il principio di non discriminazione. *“Garbage in, garbage out”*: è importante verificare la correttezza dei dati inseriti e la corretta utilizzazione delle leggi statistiche. Ce lo ha ricordato con molta umiltà il Professore Giorgio Parisi – premio Nobel per la Fisica, Presidente dell'accademia dei Lincei – parlando dell'algoritmo *Chain Montecarlo* durante la pandemia da Covid-19. Il caso Compass è rimasto un precedente importante nel ricordarci tale principio: una non corretta immissione di dati statistici relativi alla pericolosità correlata all'origine etnica delle persone, nel caso *de quo* afro-americane, aveva indotto la macchina ad allargare oltremodo i confini della recidiva, pur in assenza delle necessarie condizioni.

La “legge di Moore”, secondo la quale i microchip raddoppieranno la loro potenza e la loro velocità esponenziale induce il giurista a non assumere un atteggiamento di rifiuto, dando origine al c.d. *neoluddismo*, ma a tracciare dei criteri di regolazione che tengano in debito conto la complessità dei c.d. “agenti intelligenti”.

A tal proposito, giova ricordare che il Tribunale di Milano, con la sentenza n. 843 del 13 marzo 2021, al fine di interpretare un bando di gara, ha messo in evidenza la necessità di non confondere «*la nozione di “algoritmo” con quella di “intelligenza artificiale”, riconducibile, invece, allo studio di “agenti intelligenti”, vale a dire allo studio di sistemi che percepiscono ciò che li circonda e intraprendono azioni che massimizzano la probabilità di ottenere con successo gli obiettivi prefissati*».

Anche volendo negare l'intelligenza artificiale, quest'ultima avrà un'efficacia pervasiva ed invasiva di cui non si potrà fare a meno.

Pensiamo ai prezzi di riferimento dell'ANAC, che hanno un ruolo centrale nella regolamentazione economica degli appalti e che sono sostanzialmente basati su formule algoritmiche che tengono conto di fattori diversi per individuare il prezzo medio effettivo “depurandolo” da fattori straordinari che influenzano localmente la formazione dei prezzi che concorrono alla definizione del campione.

Molto importante è la recente sentenza del Consiglio di Stato del 25 novembre 2021, n. 7891, in cui, in tema di intelligenza artificiale e algoritmo nell'appalto di forniture di un dispositivo medico con elevato grado di autonomazione, la Terza Sezione ha

chiarito che «la nozione comune e generale di algoritmo riporti alla mente “semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato” (questa la definizione fornita in prime cure). Nondimeno si osserva che la nozione, quando è applicata a sistemi tecnologici, è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano. Il grado e la frequenza dell'intervento umano dipendono dalla complessità e dall'accuratezza dell'algoritmo che la macchina è chiamata a processare. Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di machine learning e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo “tradizionale”) ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico. Nel caso di specie, per ottenere la fornitura di un dispositivo con elevato grado di automazione non occorre che l'amministrazione facesse espresso riferimento a elementi di intelligenza artificiale, essendo del tutto sufficiente – come ha fatto – anche in considerazione della peculiarità del prodotto (pacemaker dotati, per definizione, di una funzione continuativa di “sensing” del ritmo cardiaco e di regolazione dello stesso) il riferimento allo specifico concetto di algoritmo, ossia ad istruzioni capaci di fornire un efficiente grado di automazione, ulteriore rispetto a quello di base, sia nell'area della prevenzione che del trattamento delle tachiaritmie atriali. I pacemakers moderni e di alta fascia sono infatti dotati di un numero sempre maggiore di parametri programmabili e di algoritmi specifici progettati per ottimizzare la terapia di stimolazione in rapporto alle caratteristiche specifiche del paziente. L'amministrazione ha espresso preferenza per la presenza congiunta di algoritmi di prevenzione e trattamento delle “tachiaritmie atriali”»⁴⁶.

Con tale sentenza il Consiglio di Stato è giunto ad una distinzione netta tra il concetto di algoritmo e quello di intelligenza artificiale, proprio perché nel pratico c'è una confusione tra sistemi automatici e sistemi artificiali.

Tale differenza è posta in evidenza sia a livello nazionale che europeo. La stessa Commissione europea, nella proposta di regolamentazione dell'IA del 21 aprile 2021, ha statuito che «la nozione di sistema di IA dovrebbe essere chiaramente definita per garantire la certezza del diritto, fornendo nel contempo la flessibilità necessaria per accogliere i futuri sviluppi tecnologici. La definizione dovrebbe essere basata sulle caratteristiche funzionali chiave del software, in particolare la capacità, per un dato insieme di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano l'ambiente con cui il sistema interagisce,

⁴⁶ Si veda M. IASELLI, “Consiglio di Stato: quando si può parlare di intelligenza artificiale? Palazzo Spada affronta una delicata questione tecnica sulla nozione di algoritmo, che assume notevole importanza anche per le necessarie conseguenze di carattere giuridico”, su altalex.it.

sia in una dimensione fisica che digitale. I sistemi di intelligenza artificiale possono essere progettati per funzionare con diversi livelli di autonomia ed essere utilizzati in modo autonomo o come componente di un prodotto, indipendentemente dal fatto che il sistema sia fisicamente integrato nel prodotto (incorporato) o serva la funzionalità del prodotto senza esservi integrato (non incorporato)».

Non a caso, l'art. 3 della proposta dà una definizione di sistema "IA": *«un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono»*, e l'allegato I richiamato comprende sia il *machine learning* (compreso l'apprendimento supervisionato, non supervisionato e profondo come il *deep learning*), sia gli approcci basati sulla logica e sulla conoscenza (rappresentazione della conoscenza, programmazione logica induttiva, basi di conoscenza, motori deduttivi e inferenziali, ragionamento simbolico e sistemi esperti nonché persino approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione).

Rientra nella definizione della Commissione sia l'IA "forte", volta a creare computer in grado di comprendere e possedere stati cognitivi, sia l'IA "debole", finalizzata a realizzare sistemi informatici in grado di porre in essere prestazioni normalmente attribuite all'intelligenza umana. Dunque, il Consiglio di Stato pone l'attenzione sulla differenza tra sistemi automatici e attività intelligenti, che si basano su un impiego attivo, non rigidamente predeterminato, della conoscenza. Nei sistemi informatici tradizionali, *«la conoscenza non è mai rappresentata esplicitamente e non è mai separata dalle procedure che la usano e che ne disciplinano l'elaborazione; la conoscenza è applicata in modo rigidamente predeterminato; non è possibile aggiungere nuova conoscenza senza modificare le procedure; il sistema non è in grado di esporre la conoscenza sulla quale si basa né di spiegare perché, sulla base della stessa, sia giunto a determinati risultati»*. Al contrario, nei sistemi basati sulla conoscenza, *«la conoscenza è contenuta in una determinata base, dove è rappresentata in un linguaggio ad alto livello, cioè in una forma relativamente vicina al linguaggio usato nella comunicazione umana; è possibile adottare una rappresentazione dichiarativa del compito affidato al sistema informatico, lasciando al sistema l'individuazione della procedura da seguire per svolgere quel compito; la conoscenza è usata da un motore inferenziale, ovvero un meccanismo in grado di interpretare il contenuto della base di conoscenza ed effettuare deduzioni logiche in modo da risolvere il problema posto al sistema; la base di conoscenza può essere arricchita di nuove informazioni senza intervenire sul motore inferenziale; il sistema è in grado di esporre in forma comprensibile le premesse e le inferenze che hanno condotto ad un determinato risultato, cioè di giustificare le conclusioni cui giunge»*⁴⁷.

⁴⁷ V. M. IASELLI, "Consiglio di Stato: quando si può parlare di intelligenza artificiale?", cit.

Negare l'intelligenza artificiale significa negare l'incalzare dell'innovazione tecnologica: il giurista deve allora tracciare delle linee direttrici.

La prima è intervenire sui dati, sull'*input*, il primo momento su cui si basa l'elaborazione dell'intelligenza artificiale. La nozione di "interoperabilità" dei dati, con le c.d. porte di dominio, potrà realizzarsi solo se i dati sono esatti con razionali metodi di acquisizione. Si pensi, volendo richiamare ancora una volta la materia degli appalti, alla grande banca dati dell'ANAC che è immensa, ma non è autoalimentata. Le amministrazioni non mandano i dati all'ANAC, ma a degli Osservatori regionali che li rielaborano, inoltrandolo poi all'ANAC stessa. Molto spesso i dati si presentano obsoleti o ridondanti, carenti di informazioni che potrebbero essere fondamentali nell'analisi dei mercati.

Il primo livello di controllo consiste nell'attività di selezione dei dati: inserire nella macchina dati necessari e corretti, di cui si abbia la governabilità, *trustworthy*, ossia meritevole di "fiducia"; è il primo livello di tutela per prevenire soluzioni viziate *ab origine*.

La seconda linea direttrice è modulare e declinare le tradizionali categorie giuridiche in modo che possano adeguarsi agli schemi operativi dell'intelligenza artificiale.

Pensiamo all'accertamento del nesso di causalità: la Risoluzione del Parlamento europeo del 25 marzo 2021 (sull'attuazione della direttiva 2009/81/CE, relativa agli appalti nei settori della difesa e della sicurezza, e della direttiva 2009/43/CE, relativa ai trasferimenti di prodotti per la difesa 2019/2204 (INI)) si preoccupa di ricordare che occorre ribadire la responsabilità dello Stato per i danni creati dai droni militari alle popolazioni civili, perché il dato soggettivo relativo all'attribuzione della colpa, non appare più certo, atteso che le scelte dalle quali i danni possono derivare, i luoghi da bombardare ad esempio, non sono attribuibili all'uomo. Allo stesso modo altri concetti fondamentali come l'imputabilità, la responsabilità, la discrezionalità, il sindacato giurisdizionale, il sillogismo giuridico sono da rimodulare sul funzionamento dei c.d. agenti intelligenti.

Sotto tale profilo, il Consiglio di Stato coglie la novità dell'intelligenza artificiale, statuendo nella nota sentenza n. 881/2020 che «*non può, quindi, ritenersi applicabile in modo indiscriminato ...all'attività amministrativa algoritmica, tutta la legge sul procedimento amministrativo, concepita in un'epoca nella quale l'amministrazione non era investita dalla rivoluzione tecnologica. ..Il tema dei pericoli connessi allo strumento non è ovviato dalla rigida e meccanica applicazione di tutte le minute regole procedurali della L.241/1990 (quali ad esempio la comunicazione di avvio del procedimento sulla quale si appunta buona parte dell'atto di appello o il responsabile del procedimento che, con tutta evidenza, non può essere una macchina in assenza di disposizioni espresse), dovendosi, invece, ritenere che la fondamentale esigenza di tutela posta dall'utilizzazione dello strumento informatico c.d. algoritmico sia la*

trasparenza nei termini prima evidenziati riconducibili al principio di motivazione e/o giustificazione della decisione».

La terza direttrice è il permanente controllo dell'uomo e la sua possibilità di intervento volto a far prevalere sempre un criterio di equità e di giustizia sostanziale nei processi di *decision making*, in cui grande rilevanza deve mantenere la componente intuitiva ed emozionale, non solo la fredda sequenza algoritmica.

Capitolo III

Algoritmo e diritto penale

L'analisi del rapporto tra algoritmo e diritto penale⁴⁸ deve essere necessariamente condotta sotto un triplice profilo: quello del rapporto con il profilo della privacy nell'ambito del circuito investigativo, quello relativo al profilo dell'imputabilità e quello relativo alla configurazione di nuovi reati con l'utilizzo delle nuove tecnologie. In questo capitolo cercheremo di affrontare i profili problematici legati alle intercettazioni e tabulati in relazione alla tutela della privacy, per poi affrontare il tema della eventuale riformulazione dell'imputabilità tramite algoritmi e la configurazione dei nuovi reati tramite chat o altri mezzi informatici nei capitoli successivi.

Il tema del rapporto tra algoritmi basati sulla raccolta dei dati e tutela della privacy è venuto alla ribalta in seguito ad una nota sentenza della Corte di Giustizia dell'Unione Europea dello scorso marzo 2021, in merito al rapporto tra *data retention* e *serious crimes*: il principio emerso è che per i tabulati con i numeri di telefono serve l'autorizzazione di un'autorità terza che non sia il Pubblico Ministero. La *data retention*, quindi, è ammissibile solo per *serious crimes*, in Italia quelli previsti dall'art. 266 c.p.p.

Ma analizziamo il testo della sentenza della Corte di Giustizia dell'Unione Europea, Grande sezione, sentenza 2 marzo 2021, Causa C-746/18 nelle sue conclusioni:

“1) *L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/Ce del Parlamento europeo e del consiglio, del 25 novembre 2009, letto alla luce degli art. 7, 8 e 11, nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel*

⁴⁸ Sul tema v. C. BURCHARD, “L'Intelligenza Artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società”, in *Rivista italiana di diritto e procedura penale*, 2019, Vol. 62; C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, “*Artificial Intelligence and the “Good Society”: the US, EU, and UK approach*”, in *Science and Eng. Ethics*, 2018; L. BENNET MOSES, J. CHAN, “*Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability*”, in *Policing and Society*, 2016; G. MASTROBUONI, “*Crime is Terribly Revealing: Information Technology and Police Productivity*”, 2017; L. PASCULLI, “*Genetics, Robotics and Crime Prevention*” e R. PELLICCIA, “*Polizia predittiva*”, *Human Rights Data Analysis Group (Hrdag)*, <https://hrdag.org/usa/>; A. R. LODDER, J. ZELEZNIKOW, “*Artificial Intelligence and Online Dispute Resolution*”, in A. R. LODDER, J. ZELEZNIKOW, “*Enhanced Dispute Resolution through the Use of Information Technology*”, *Cambridge University Press*, 2010; E. LATIFAH, A. H. BAJREKTAREVIC, M. N. IMANULLAH, “*Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution*”, in *Brawijaya Law Journal – Journal of Legal Studies*, vol. 6, aprile 2019.

senso che esso osta a una normativa nazionale, la quale consenta l'accesso di autorità pubbliche a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo.

2) L'art. 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11, nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il pubblico ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale."

Si è affermato che la sentenza CGUE del 2 marzo 2021 apre scenari imprevedibili nell'assetto costituzionale e processuale del pubblico ministero.

La prospettiva della CGUE è affatto diversa da quella nazionale, poiché non assegna alcun rilievo alla collocazione ordinamentale del pubblico ministero e volge lo sguardo, in modo esclusivo, al procedimento penale e alle sue regole. Una traiettoria che assume, anche, una valenza attuale alla luce del progetto di riforma del processo penale e al dibattito sulla cosiddetta "separazione delle carriere".

La mistica del pubblico ministero racchiuso nell'ossimoro della "parte imparziale", si trova pragmaticamente a essere messa in discussione.

La Corte di Giustizia si era già espressa, nel 2014, con la sentenza *Digital Rights Ireland* e nel 2016 con la sentenza *Tele 2 Sverige* e la Corte di Cassazione, investita della questione dell'applicazione di questa giurisprudenza eurounitaria in modo diretto, aveva da ultimo convalidato tale impostazione, sostenendo che certamente si doveva rientrare nel novero dei *serious crimes*: «nel caso in esame, essendosi proceduto per associazione a delinquere finalizzata alla consumazione di reati contro il patrimonio, nonché per molteplici episodi di furti aggravati ed anche rapina, deve ritenersi che l'accesso ai dati di traffico sia avvenuto in un contesto di indagini di criminalità organizzata a seguito di provvedimento di un'autorità giurisdizionale e con

l'acquisizione effettuata entro il biennio che costituisce un periodo di tempo limitato»⁴⁹.

Non si può omettere di considerare che la giurisprudenza nazionale aveva, comunque, dichiarato di porsi sulla scia delle precedenti pronunce della Corte di Lussemburgo, quanto meno ai fini della delimitazione dei casi e dei tempi per l'acquisizione dei dati di traffico⁵⁰. Quel che era inatteso – e che è destinato a sollevare innumerevoli controversie – è che la Corte di Giustizia negasse al pubblico ministero la potestà di poter operare direttamente tali acquisizioni senza il tramite di un provvedimento adottato da un giudice terzo e imparziale.

Autorevole dottrina ha sostenuto che *“imparzialità e terzietà sono concetti in rapporto di specialità; il più generale è quello della imparzialità, il più specifico quello della terzietà, cosicché mentre si possono avere casi di imparzialità senza terzietà, non è pensabile una terzietà senza imparzialità. Usando i diagrammi di Venn, l'imparzialità è un cerchio più ampio al cui interno sta interamente un cerchio più piccolo che rappresenta la terzietà”⁵¹*; in altre parole, a prescindere da precari equilibrismi verbali, può anche convenirsi che il pubblico ministero, quale organo pubblico, agisca con imparzialità e che gli possa competere la qualifica di “parte imparziale”, ma quel che deve escludersi radicalmente è che il *munus* sia connotato dal requisito della terzietà, fondamento costitutivo della giurisdizione. Ed è proprio nel solco di questa riflessione che si colloca la sentenza della Corte di Giustizia del 2 marzo 2021, la quale esclude che il pubblico ministero possa assolvere alla funzione di equilibrato, giusto e terzo titolare del potere di acquisizione dei dati di traffico presso i gestori.

Sul punto, la pronuncia esprime valutazioni irretrattabili e definitive che, per la prima volta, revocano in dubbio anche la tesi di una protezione della privacy a “sfere concentriche” (secondo l'approccio della dottrina costituzionale tedesca), per cui si dovrebbe assicurare il massimo di tutela in presenza di captazioni e intercettazioni, laddove per i c.d. *“dati esteriori di traffico”* si potrebbe assicurare una protezione affievolita sia in ordine ai presupposti, che all'autorità procedente.

La densità assiologica del diritto coinvolto è tale, infatti, da non consentire graduazioni di tal fatta e di decentrare, quindi, l'individuazione dell'autorità che deve disporre

⁴⁹ Così, in motivazione, Cassazione, sez. II, n. 5741 del 13 febbraio 2020, m.278568.

⁵⁰ Si veda anche Cassazione, sez. III, n. 48737 del 25 settembre 2019, m.277353; sez. V, n. 33851 del 24 aprile 2018, m.273892. Sul tema si vedano anche N. REZENDE, *“Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention”*, nota a Cass., sez. III, 19 aprile 2019 (dep. 23 agosto 2019), n. 36380, in www.sistemapenale.it; L. LUPARIA, *“Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio”*, in *Diritto di Internet*, 2019, 4, p. 762.

⁵¹ G. U. RESCIGNO, *“L'esercizio dell'azione pubblica ed il pubblico ministero”*, relazione dell'8 novembre 2004 al Convegno dell'Associazione Italiana dei Costituzionalisti su *“Separazione dei poteri e funzione giurisdizionale”*.

l'acquisizione nel perimetro giurisdizionale (giudice) o fuori di esso (pubblico ministero), in funzione della sola entità della lesione che va a realizzare.

Lo snodo argomentativo è chiaro e conduce a conclusioni che sono inevitabili: il pubblico ministero, per quanto possa agire imparzialmente, è, comunque, sprovvisto di terzietà rispetto al privato cittadino (sia esso indagato o no) e l'indipendenza che la *Grundnorm* comunitaria esige per l'autorità che dispone l'ingerenza nella vita privata *«impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica, come in sostanza rilevato dall'avvocato generale al paragrafo 126 delle sue conclusioni, che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale. Ciò non si verifica nel caso di un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale. Infatti, il pubblico ministero non ha il compito di dirimere in piena indipendenza una controversia, bensì quello di sottoporla, se del caso, al giudice competente, in quanto parte del processo che esercita l'azione penale»* (§54-55).

Tale sentenza della Corte di Giustizia supera, altresì, la posizione della Corte di Cassazione, che aveva fatto riferimento alla categoria dell'inutilizzabilità in relazione ai dati acquisiti dal pubblico ministero, oltre i limiti temporali previsti dall'art. 132 Codice Privacy, fondandola sulla violazione di un divieto probatorio posto a tutela dei diritti fondamentali della persona, quali il diritto alla inviolabilità del domicilio o della corrispondenza⁵².

Sarà tutto da esplorare il tema delle ricadute che questa sentenza può essere destinata a svolgere in Italia nei settori contigui delle intercettazioni e delle acquisizioni di dati di traffico per finalità preventive (art. 226 delle disposizioni di attuazione del c.p.p.), per il controllo delle misure di prevenzione (art. 78 del Codice Antimafia) e per le necessità dei Servizi di informazione per la sicurezza nazionale (art. 4 del decreto-legge 27 luglio 2005, n. 144). Tutte attività rimesse all'attività di un organo della pubblica accusa (nei primi casi le procure ordinarie e distrettuali, a seconda della competenza, e nell'ultimo la Procura generale presso la Corte di appello di Roma) e certamente ingeneranti nella privacy dei singoli.

Sono attività intrusive consentite, ma che, secondo la direttiva 2002/758/CE, devono essere declinate in modo appropriato e proporzionato allo scopo perseguito attraverso la previsione di garanzie che salvaguardino i principi stabiliti nella Carta dei diritti

⁵² Cassazione, sez. V, n. 7265 del 25 gennaio 2016, m.267144-01; in motivazione Sezioni Unite, n. 155 del 2012 e Sezioni Unite n. 52117 del 2014; sez. V, n. 15613 del 5 dicembre 2014, m.263805.

fondamentali dell'Unione Europea, in particolare agli art. 7 (ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni), art. 8 (ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano), art. 11 (ogni persona ha diritto alla libertà di espressione; tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera) e art. 52 (laddove è stabilito che eventuali limitazioni dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà, con la conseguenza che possono essere apportate limitazioni, nel rispetto del principio di proporzionalità, solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui). Il principio del *"fair balance test"*, *"principle of lawfulness"* investe la cd *"struttura trifasica progressiva della proporzionalità"*, laddove si è posta come evidente il problema della compatibilità euro-unitaria della disciplina italiana acquisitiva dei tabulati telefonici: art. 226 delle disposizioni di attuazione del c.p.p. e art. 132 del D.lgs. 30 giugno 2003, n. 196.

In realtà, la sentenza sembrerebbe porre anche un problema di competenza a disporre l'acquisizione dei tabulati, laddove esclude che tale soggetto possa essere il pubblico ministero. Ma soprattutto da noi la decisione pone qualche dubbio su alcune interpretazioni e sulle conseguenti prassi applicative in tema di intercettazioni (con riguardo soprattutto all'utilizzo in sede diversa da quella ove l'intercettazione è stata disposta) e in tema di utilizzo in sede extrapenale di "conversazioni" il cui contenuto è stato acquisito in sede penale⁵³.

Per quanto riguarda le intercettazioni, la sentenza impone un notevole rigore ermeneutico.

Affinché, attraverso una non consentita ampia lettura dell'art. 270 del c.p.p., si possa finire con il legittimare le intercettazioni "a strascico", con il rischio di utilizzazioni per una platea di reati diversi (e meno gravi) di quelli per cui è stata disposta l'attività

⁵³ Sul tema: C. PARODI, *"Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge"*, su *ilpenalista.it*, 3 maggio 2021; C. PARODI, *"Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE"*, su *ilpenalista.it*, 5 agosto 2021; G. SPANGHER, *"I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali"*, in *Giustizia Insieme*, 3 maggio 2021; J. DELLA TORRE, *"L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del Gip di Roma"*, su *sistemapenale.it*; L. CUSANO, *"Tabulati telefonici: ulteriori ricadute della sentenza della CGUE del 2 marzo 2021 sul piano della utilizzabilità degli esiti di prova"*, nota a Trib. Bari, sez. GIP, 1° maggio 2021, su *ilpenalista.it*, 25 maggio 2021; F. RESTA, *"Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna"*, su *Giustizia Insieme*.

intercettativa. Il rigore applicativo si pone come necessario dopo tale sentenza della Corte di Giustizia.

Così, per quanto riguarda le intercettazioni “ordinarie”, provvede il disposto dell’art. 270, comma 1, del c.p.p., laddove si stabilisce la regola secondo cui i risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino “rilevanti” e indispensabili per l’accertamento di delitti per i quali è obbligatorio l’arresto in flagranza e «dei reati di cui all’art. 266, comma 1 del c.p.p.».

Deve, dunque, trattarsi di intercettazioni contenenti elementi rilevanti e spendibili per la prova di reati per i quali lo strumento delle intercettazioni sarebbe stato ordinariamente consentito. Rileva, in tal senso, la puntualizzazione della sentenza 28 novembre 2019, *Cavallo* e altro, nella quale le Sezioni Unite hanno affermato che, al di là di ogni considerazione formale circa l’iscrizione (all’interno del medesimo fascicolo o in via autonoma), si è, comunque, al di fuori del divieto di utilizzazione stabilito dall’art. 270 c.p.p. rispetto ai reati che risultino connessi ex art. 12 del c.p.p., a quelli in relazione ai quali l’autorizzazione era stata *ab origine* disposta, sempreché rientrino nei limiti di ammissibilità previsti dall’art. 266 del c.p.p.

Quanto alle intercettazioni tramite captatore, il comma 1-bis dell’art. 270 del c.p.p. prevede che, fermo restando quanto previsto dal comma 1, i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, «qualora risultino indispensabili per l’accertamento dei delitti indicati dall’articolo 266, comma 2-bis, del c.p.p.».

Per l’effetto, i risultati delle intercettazioni tramite *trojan* possono essere utilizzati anche per la prova di “reati diversi” da quelli per i quali è stato emesso il decreto di autorizzazione, «qualora risultino indispensabili per l’accertamento dei delitti indicati dall’art. 266, comma 2-bis, del c.p.p.» (ossia, i delitti di cui all’articolo 51, commi 3-bis e 3-quater, del c.p.p., ovvero i delitti dei pubblici ufficiali e degli incaricati di un pubblico servizio contro la pubblica amministrazione).

Il rigore notevole che accompagna l’utilizzabilità delle intercettazioni in “altri” e “diversi” procedimenti penali, alla luce degli argomenti sviluppati nella sentenza della Corte europea a garanzia e presidio della riservatezza, quando non ricorrono le esigenze di contrasto di gravi reati, sembrerebbero imporre una rilettura della giurisprudenza delle sezioni unite che, in modo ormai ripetitivo e riproduttivo di principi consolidati, ammette l’utilizzabilità delle intercettazioni anche in sede disciplinare a carico di magistrati⁵⁴.

La decisione della Corte europea dovrebbe indurre a una più meditata riflessione sull’esportabilità automatica di registrazioni in contesti e per finalità diverse dal

⁵⁴ Vedi, ad esempio, Cass., Sezioni Unite n. 741 del 2020.

contrasto dei “gravi reati” che, nella lettura dei giudici europei, è l’unica ragione legittimante l’invasione della sfera privata altrui. Conclusione, questa, maggiormente valida ove si discuta di utilizzabilità delle intercettazioni a mezzo captatore informatico: proprio l’invasività del captatore ha già imposto una disciplina di maggior rigore rispetto a quelle delle ordinarie intercettazioni (art. 270, comma 1, c.p.p.) e ciò, proprio alla luce delle indicazioni della Corte Europea, dovrebbe far riflettere sull’automatica esportabilità delle intercettazioni tramite *trojan* (magari riguardanti anche soggetti diversi da quelli oggetto di controllo giudiziario in sede disciplinare o paradisciplinare).

Tale esportabilità si porrebbe in contrasto con gli artt. 7 e 8 della Carta dei diritti fondamentali della Unione europea: trattasi di conversazioni private non correlate con l’addebito penale e, quindi, prive di alcun collegamento con la finalità di repressione di gravi reati, in termini tali da non ravvisarsi una ragione giustificativa a supporto della legittima limitazione del diritto alla segretezza delle comunicazioni.

Alla luce della sentenza della Corte di Giustizia del 2 marzo 2021, si poneva come necessaria una revisione dell’art. 132 del Codice della privacy, la cui disciplina si poneva come derogatoria a quella prevista dalla direttiva 2002/58/CE sulla acquisizione e conservazione dei dati ed in particolare l’art. 132, terzo comma, che consente la richiesta al pubblico ministero, e comma quarto (ter, quater, quinquies) che lo consente anche via decreto del Ministero dell’Interno. Tale modifica è intervenuta con il decreto legge del 30 settembre 2021 n.132, convertito nella legge 23 novembre 2021 n.178 che ha recepito la necessità di introdurre in tale delicata materia il filtro del controllo del giudice terzo.

È noto come la direttiva 2002/58/CE non si applica alle attività che esulano dal campo di applicazione del Trattato sul Funzionamento dell’Unione Europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato o alle attività dello Stato in settori che rientrano nel diritto penale.

L’art. 15, paragrafo 1, della direttiva soprarichiamata attribuisce agli Stati membri la possibilità di adottare disposizioni legislative volte a limitare taluni diritti da essa conferiti, qualora tale restrizione sia necessaria, opportuna e proporzionata per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell’uso non autorizzato del sistema di comunicazione elettronica. A tal fine, gli Stati membri possono, tra l’altro, adottare misure legislative, le quali prevedano che i dati siano conservati per un periodo di tempo limitato.

A fronte di tale disciplina, la Corte estone ha posto due quesiti.

In primo luogo, la questione se la durata del periodo cui si riferiscono i dati ai quali i servizi inquirenti hanno avuto accesso costituisca un criterio che permette di valutare la gravità dell’ingerenza rappresentata da tale accesso nei diritti fondamentali delle

persone interessate. Il giudice supremo estone si è chiesto, in particolare, per il caso in cui questo periodo sia molto breve o la quantità di dati raccolti sia assai limitata, se l'obiettivo della lotta contro la criminalità in generale, e non soltanto contro le forme più gravi di criminalità, sia idoneo a giustificare una siffatta ingerenza.

In secondo luogo, se il pubblico ministero estone, tenuto conto delle varie funzioni affidategli dalla normativa nazionale, costituisca un'autorità amministrativa «indipendente».

I quesiti si inseriscono in un contesto interpretativo già segnato con importanti decisioni della Corte di Giustizia che, a partire dal 2014, ha chiarito gradualmente i vari profili del tema in esame.

Tra queste precedenti sentenze, occorre ricordare quella relativa ai *Digital Rights* dell'8 aprile 2014, con la quale la Corte di Giustizia ha dichiarato l'illegittimità della direttiva “Fratтини” (2006/24/Ce), per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza.

All'attenzione della Corte erano state portate le disposizioni della direttiva volte a garantire la conservazione dei dati di traffico telefonico e telematico, i dati relativi all'ubicazione e quelli necessari all'identificazione dell'abbonato, per fini di accertamento e repressione dei reati. Se, in linea generale, l'accesso a tali dati può giustificarsi in ragione di un obiettivo di interesse generale, quale, appunto, il contrasto a gravi forme di criminalità e, in definitiva, le esigenze di pubblica sicurezza, la direttiva avrebbe, secondo la Corte, ecceduto i limiti imposti dal principio di proporzionalità.

Tale violazione si sarebbe sostanziata, secondo la Corte, nell'avere la direttiva:

- 1) previsto le misure di conservazione dei dati come applicabili in via indifferenziata e generalizzata *«all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi»;*
- 2) omissso di prevedere alcun criterio oggettivo che limiti l'accesso a tali dati per sole esigenze di accertamento di reati *«sufficientemente gravi da giustificare una simile ingerenza»;*
- 3) omissso di sancire i presupposti sostanziali e procedurali ai quali subordinare l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente;
- 4) omissso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilire i soli termini minimi (6 mesi) e massimi (24 mesi);
- 5) omissso di imporre che i dati così acquisiti siano conservati nel solo territorio UE.

Sulla stessa scia si pone la sentenza resa nel caso *Tele2 Sverige* del 21 dicembre 2016, con la quale la Corte di Giustizia ha dichiarato incompatibile con la direttiva 2002/58/CE la disciplina interna che, per fini di contrasto dei reati: a) imponga la generale e indiscriminata conservazione di tutti i dati di traffico e relativi all'ubicazione degli utenti dei mezzi; b) legittimi l'accesso delle autorità nazionali competenti ai dati conservati per finalità ulteriori rispetto a quelle di contrasto dei crimini gravi, in assenza di un previo vaglio giurisdizionale o comunque di un'autorità amministrativa indipendente e di garanzie relative alla conservazione dei dati nella UE.

In tale sentenza la Corte ha, tuttavia, anche chiarito che la direttiva non osta ad una normativa nazionale che imponga una conservazione mirata dei dati per finalità di lotta contro gravi fenomeni di criminalità, a condizione che tale conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone implicate, nonché la durata di conservazione prevista, limitata allo stretto necessario.

Qualsiasi normativa nazionale che vada in tal senso deve essere chiara e precisa “*accessible*” e prevedere garanzie sufficienti al fine di proteggere i dati contro i rischi di abuso. Le discipline interne sulla conservazione dei dati devono, pertanto, prevedere l'accessibilità dei dati conservati solo da parte dell'autorità giudiziaria o di un'autorità amministrativa indipendente, in base a circostanze e procedure disciplinate dalla legge per esigenze di accertamento di gravi reati, notificando la misura all'interessato, non appena le esigenze investigative lo consentano. Infine, tenuto conto della quantità di dati conservati, del carattere sensibile di tali dati, nonché del rischio di accesso illecito a questi ultimi, la normativa nazionale deve prevedere che i dati siano conservati nel territorio dell'Unione e che essi vengano irreversibilmente distrutti al termine della durata della loro conservazione.

Nella sentenza *Ministerio Fiscal* del 2 ottobre 2018, la Corte si è occupata dell'accesso ai dati che mirano all'identificazione dei titolari di carte Sim attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali soggetti. Sebbene tale accesso determini un'ingerenza nei diritti fondamentali degli interessati sanciti nella Carta dei Diritti Fondamentali dell'Unione Europea, esso non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave.

È da ricordare ancora la sentenza *Privacy International* del 6 ottobre 2020, con la quale la Corte di Giustizia ha sancito la contrarietà alla direttiva 2002/58/CE di una disciplina che imponga ai fornitori di servizi di comunicazione elettronica, al fine di salvaguardare la sicurezza nazionale, di effettuare la conservazione generale e indiscriminata dei dati sul traffico e dei dati sull'ubicazione come misura preventiva. In altri termini, si è escluso che l'esimente della funzionalità del trattamento ai fini di

sicurezza nazionale possa “coprire” anche la indiscriminata conservazione dei dati ad esso finalizzata.

Fondamentale è la conclusione che un organo giurisdizionale, il quale consideri che una parte non è in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici (in quanto decisa da un pubblico ministero) e idoneo a influire in modo preponderante sulla valutazione dei fatti, deve constatare una violazione del diritto a un processo equo ed escludere tale mezzo di prova, al fine di evitare una violazione siffatta. Ciò dovrebbe indurre, secondo la Corte di giustizia, il giudice penale nazionale ad escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all’ubicazione, incompatibile con il diritto dell’Unione, o anche mediante un accesso dell’autorità competente a tali dati in violazione del diritto dell’Unione.

Circa la competenza ad autorizzare l’accesso di un’autorità pubblica ai dati relativi al traffico e ai dati relativi all’ubicazione, al fine di dirigere un’istruttoria penale, la Corte osserva che è essenziale che l’accesso delle autorità nazionali competenti ai dati conservati sia subordinato a un controllo preventivo effettuato o da un giudice o da un’entità amministrativa indipendente. Da ciò consegue che il requisito dell’indipendenza che l’autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l’accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale, al riparo da qualsiasi influenza esterna.

In ambito penale, il requisito di indipendenza implica che l’autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell’indagine penale di cui trattasi, dall’altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale. Il pubblico ministero non garantisce la sua terzietà.

In realtà, prima di tali pronunce della Corte di Giustizia dell’Unione Europea, il Garante della privacy aveva invitato, senza successo, il legislatore a riformare la disciplina interna sulla conservazione dei tabulati che non limita l’acquisizione ai soli reati gravi né subordina tale acquisizione al vaglio del giudice⁵⁵.

Similmente, anche la Corte di Cassazione, con sentenza 13 febbraio 2020, n. 5741, aveva “salvato” la “*data retention*” italiana, ritenendo che le sentenze *Digital Rights* e *Tele2 Sverige* della Corte di Giustizia non intaccassero la compatibilità delle previsioni dell’art. 132 con il diritto dell’UE.

⁵⁵ Si vedano le osservazioni di M. MASSIMI, *Art. 132*, in R. SCIAUDONE (a cura di) “*Il Codice della Privacy*”, Pacini, Ospedaletto, 2019, pag. 668.

A prescindere dalle perplessità che le affermazioni della Cassazione hanno suscitato sulla corretta lettura delle pronunce della Corte di Giustizia, era ormai inevitabile una revisione dell'art. 132 del Codice della Privacy.

Di recente, la Cassazione Penale⁵⁶ si è pronunciata sugli effetti della sentenza del 2 marzo 2021 della Corte di Giustizia dell'Unione Europea nella causa C746/18.

L'impostazione della CGUE – si legge nella decisione – *«deve essere confrontata con l'assetto normativo attualmente delineatosi nel nostro ordinamento e, in particolare, con il consolidato orientamento della Suprema Corte, secondo cui, in tema di acquisizione dei dati contenuti nei cd. tabulati telefonici, la disciplina italiana di conservazione dei dati di cui all'art. 132 dlgs.196/2003 deve ritenersi compatibile con le direttive in tema di privacy, e ciò poiché la deroga stabilita dalla norma alla riservatezza delle comunicazioni è prevista dall'art. 132 cit. per un periodo di tempo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati ed è subordinata alla emissione di un provvedimento di una autorità giurisdizionale indipendente com'è appunto il pubblico ministero».*

Invero, se da un lato, *«è indubitabile che debba attribuirsi ai principi espressi nelle sentenze CGUE il valore fondante del diritto comunitario con efficacia erga omnes nell'ambito della Comunità»*, dall'altro, *«l'attività interpretativa del significato e dei limiti di applicazione delle norme comunitarie, operata nelle sentenze CGUE, può avere efficacia immediata e diretta nel nostro ordinamento limitatamente alle ipotesi in cui non residuino, negli istituti giuridici regolati, concreti problemi applicativi e correlati profili di discrezionalità che richiedano l'intervento del legislatore nazionale, tanto più laddove si tratti di interpretazioni di norme contenute nelle direttive».*

Allo stato, quindi, *«non può che ritenersi come l'interpretazione proposta dalla CGUE sia del tutto generica nell'individuazione dei casi nei quali i dati di traffico telematico e telefonico possono essere acquisiti (“lotta contro le forme gravi di criminalità” o “prevenzione di gravi minacce alla sicurezza pubblica”), essendo evidente che tali aspetti non possono essere disciplinati da singole (e potenzialmente contrastanti) decisioni giurisprudenziali, dovendosi demandare al legislatore nazionale il compito di trasfondere i principi interpretativi delineati dalla Corte in una legge dello Stato».* Ne deriva – conclude la Cassazione – *«l'impossibilità di ritenere che la sentenza della CGUE possa trovare diretta applicazione in Italia fino a quando non interverrà il legislatore italiano ed anche europeo, in quanto allo stato può e deve ritenersi applicabile l'art. 132 dlgs 196/2003»*⁵⁷.

⁵⁶ Cass. Pen., sez. II, 07/09/2021, n. 33116 e Cass. Pen., sez. II, 03/09/2021, n. 33118, disponibile su *dejure.it*; commentata da G. LUIGI, “La Corte di cassazione ritorna sull'acquisizione dei tabulati telefonici dopo le indicazioni della CGUE”, su *Ilpenalista.it*, 5 ottobre 2021.

⁵⁷ Sul tema, si veda l'articolo di E. RINALDINI, “Data retention e procedimento penale. Gli effetti della sentenza della Corte di Giustizia nel caso H.K. sul regime dell'acquisizione dei tabulati

Si ricorda, comunque, che la Cassazione, con sentenza del 1° settembre 2021, ha escluso l'applicabilità del principio di diritto enucleato nella sentenza "Cavallo" in materia di intercettazioni quando, dopo l'attività di captazione, l'imputazione venga riqualificata in altra non annoverata nello speciale elenco di cui all'art. 266 c.p.p. (si pensi al concetto di "inutilizzabilità derivata": l'ordinanza del GUP del Tribunale di Perugia del 20 giugno 2021 nel procedimento c.d. "*Palamara bis*").

L'auspicato intervento normativo si è concretizzato nell'art. 1 del decreto-legge 30 settembre 2021, n. 132, con il quale il legislatore è intervenuto in via d'urgenza a ridisciplinare la materia dell'acquisizione dei dati di traffico telefonico e telematico per fini di indagini penale (c.d. Tabulati). L'adeguamento del nostro sistema ai principi comunitari non poteva che richiedere un intervento del legislatore, non essendosi in presenza di una decisione immediatamente e automaticamente autoapplicativa, quanto meno con riguardo alla "selezione" dei reati "gravi", tali da legittimare l'acquisizione dei tabulati⁵⁸.

Con l'art. 1 del decreto-legge soprarichiamato si interviene ad introdurre le modifiche necessarie all'art. 132 del decreto legislativo n. 196/2003. Le modifiche sono volte a perimetrare la competenza ad acquisire i tabulati attribuita al giudice, che deve provvedere con decreto motivato sulla rilevanza di tale acquisizione «ai fini della prosecuzione delle indagini», e non più al pubblico ministero. Peraltro, la sollecitazione al giudice è attribuita, nell'ambito delle investigazioni difensive, anche al difensore dell'imputato, della persona offesa e delle altre parti private. Si profila, però, un problema interpretativo nel testo del decreto-legge, laddove si attribuisce la competenza al "giudice" correlandosi la ragione della richiesta alla rilevanza «ai fini della prosecuzione delle indagini». In realtà, il tema dell'acquisizione dei tabulati si può porre anche dopo l'esercizio dell'azione penale, davanti al giudice del dibattimento, ma anche davanti a quello dell'udienza preliminare chiamato a definire il processo in sede di abbreviato condizionato. pubblico ministero o dalla persona offesa/parte civile; vuoi per smentirla, in caso di richiesta proveniente dalla difesa dell'imputato.

telefonici e telematici: urge l'intervento del legislatore", in *Giurisprudenza Penale Web*, 2021, 5, l'ordinanza con cui il Tribunale di Rieti ha proposto questione pregiudiziale alla Corte di Giustizia dell'Unione Europea, nonché le ordinanze con cui il Tribunale di Tivoli e la Corte di Assise di Napoli hanno escluso un'applicazione diretta della CGUE.

⁵⁸ Per un primo commento alla nuova disciplina, si vedano M. BORGABELLO, "*Acquisizione di tabulati telefonici: che cambia col nuovo decreto-legge*", su *agendadigitale.ue*, 4 ottobre 2021; L. FILIPPI, "*La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*", su *penaledp.it*, 1° ottobre 2021; C. PARODI, "*Sottratto al P.M. il potere di richiedere autonomamente i tabulati*", su *ilpenalista.it*, 1° ottobre 2021; G. PESTELLI, "*D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*", su *quotidianogiuridico.it*, 4 ottobre 2021; F. RESTA, "*La nuova disciplina dell'acquisizione dei tabulati*", su *Giustizia Insieme*, 2 ottobre 2021; A. MALACARNE, "*La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*", su *Sistema Penale*, 8 ottobre 2021.

Il nuovo comma 3-bis dell'art. 132 disciplina le situazioni urgenti, rispetto alle quali è conservato un potere di intervento diretto del pubblico ministero, sottoposto poi alla convalida del giudice. Infatti, allorquando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero ha la facoltà di disporre direttamente l'acquisizione dei dati con decreto motivato, non solo sulle ragioni investigative giustificanti l'acquisizione, ma anche sulle ragioni di urgenza e sul pregiudizio che deriverebbe dal ritardo nell'acquisizione.

In base alle indicazioni della Corte Europea, si limita l'acquisibilità dei tabulati a specifiche ipotesi incriminatrici "gravi": deve trattarsi di reati per quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a 3 anni. Si escludono così dal catalogo dei reati alcune fattispecie a forte allarme sociale punite con una pena inferiore.

Tra i presupposti per acquisire i tabulati, il modificato comma 3 dell'art. 132 prevede, però, anche la "sussistenza di sufficienti indizi di reato". Da tale espressione si evince chiaramente che "gli indizi di reato" richiesti per poter acquisire i tabulati afferiscono alla sussistenza di un reato e non alla colpevolezza di un determinato soggetto, sicché per procedere legittimamente ad acquisire i tabulati non è necessario che tali indizi siano a carico di un soggetto individuato o di cui le cui conversazioni debbano essere controllate al fine dell'indagine.

La motivazione del decreto (del giudice o del pubblico ministero quando opera d'urgenza, salvo convalida del giudice entro le 48 ore successive) deve, quindi, esprimere solo una valutazione sull'esistenza di un fatto storico integrante una determinata ipotesi di reato, il cui accertamento impone l'adozione dello strumento acquisitivo. Sarà, quindi, sufficiente che tale valutazione trovi fondamento in un "livello minimo di indizi giudiziari" e non saranno richiesti, invece, i gravi indizi ordinariamente previsti per le intercettazioni all'art. 267, comma 3, c.p.p., che evocano la necessità di un giudizio altamente probabilistico della sussistenza di un reato.

È stato giustamente osservato che la soluzione del legislatore è stata, *in primis*, quella di agganciare il giudizio di "gravità" alla pena edittale, ma la soluzione mostra i suoi limiti, in quanto non tutti i reati rientranti nel *range* della norma rientrano nel novero delle fattispecie incriminatrici dirette a contrastare «le forme gravi di criminalità» o a prevenire «gravi minacce alla sicurezza pubblica», come preteso dalla Corte di Giustizia.

Volendo definire in via interpretativa il regime transitorio non disciplinato dal decreto-legge 30 settembre 2021, n. 132 soprarichiamato, è da ritenere corretto che i tabulati acquisiti prima del *novum* normativo non siano affetti dal vizio dell'inutilizzabilità ex art. 190 c.p.p., perché non sono stati illegittimamente acquisiti. Al contrario, sono stati acquisiti nel rispetto delle indicazioni normative all'epoca vigenti. Infatti, essendo la

successione delle leggi processuali governata dal principio *tempus regit actum*, ciò dovrebbe comportare la persistente validità ed efficacia degli atti compiuti nell'osservanza delle leggi all'epoca vigenti⁵⁹.

In questa ottica, neppure dovrebbe porsi un problema generalizzato di acquisizione al processo dei tabulati ritualmente acquisiti nel rispetto della normativa all'epoca vigente. Sembrerebbe allora superfluo, rispetto ai tabulati acquisiti *ante* decreto n. 132, un'attività generalizzata di richiesta al giudice per un'acquisizione "ora per allora". Tale autorizzazione si profilerebbe necessaria ove, però, sorgessero contestazioni: in tal caso sarebbe opportuno chiedere al giudice la formale acquisizione dei tabulati, quanto meno ex art. 507 c.p.p., e lo stesso potrebbe farsi in appello, in sede di rinnovazione dell'istruttoria dibattimentale ex art. 603 c.p.p.

Occorre, però, distinguere i concetti di acquisibilità dei tabulati dalla loro utilizzabilità in concreto. Il tema dell'acquisizione soggiace alle regole all'epoca vigenti, mentre quello della valutazione non può che essere regolata dalla nuova normativa. In altri termini, *nulla quaestio* per l'acquisizione dei tabulati, ma questi potranno essere valorizzati sul piano probatorio solo nel rispetto delle condizioni di legittimità da oggi previste nel nuovo comma 3 dell'articolo 132 (catalogo dei reati, sufficienza degli indizi, rilevanza investigativa o probatoria).

È interessante anche il tema dell'introduzione di un apposito provvedimento di «*deindicizzazione*», a tutela del diritto all'oblio degli indagati o imputati la cui posizione sia stata definita da un decreto di archiviazione, sentenza di non luogo a procedere o di assoluzione.

L'art. 1, comma 25 della legge n. 134 del 2021 delega il Governo a modificare le norme di attuazione, di coordinamento e transitorie al codice di procedura penale in materia di comunicazione della sentenza, stabilendo la necessità di prevedere che il decreto di archiviazione, la sentenza di non luogo a procedere e di assoluzione costituiscano titolo per ottenere un provvedimento di deindicizzazione. Si vuole, infatti, rendere effettivo il diritto all'oblio degli indagati o imputati, nel rispetto della normativa europea in tema di protezione dei dati personali.

Il diritto all'oblio⁶⁰, chiamato anche diritto alla cancellazione, è disciplinato dall'art. 17 del GDPR, il quale elenca i casi in cui l'interessato ha il diritto di ottenere dal titolare del trattamento (il motore di ricerca o *service provider*) la cancellazione dei dati

⁵⁹ Cass., Sezioni Unite, 26 novembre 2003, n. 919.

⁶⁰ «...*La vera damnatio, per le persone, è ormai rappresentata dalla conservazione, non dalla distruzione della memoria. Che cosa diventa la persona quando viene consegnata alle banche dati e alle loro interconnessioni, ai motori di ricerca che rendono immediato l'accesso a qualsiasi informazione, quando le viene negato il diritto di sottrarsi allo sguardo indesiderato, di ritirarsi dietro le quinte, in una zona d'ombra?... Che cosa diviene la vita nel tempo in cui "Google ricorda sempre"?*», così si pronuncia S. RODOTÀ nel suo breve trattato *"Il mondo nella rete. Quali diritti, quali vincoli"*, Editori Laterza e la Repubblica, Roma-Bari, 2014, p. 41-42, da *"Il diritto di avere diritti"*.

personali che lo riguardano, a tutela della propria riservatezza e della propria identità personale, ove essi non siano più necessari *«rispetto alle finalità per i quali sono stati raccolti»*⁶¹.

La norma è il frutto di un percorso giurisprudenziale iniziato con la celebre sentenza 13 Maggio 2014, C-113/12 della Corte di Giustizia, c.d. Sentenza “*Google Spain*”, in cui la Corte ha delineato il rapporto tra libertà di espressione e diritti della personalità sul web, manifestando un’attitudine garantista nei confronti della privacy nell’ambito digitale, introducendo il “diritto all’oblio in internet” e riconoscendo, dunque, il diritto di ciascuno di “controllare” i risultati che appaiono sul web a seguito della digitazione del proprio nome. In tal modo, ciascuno può richiedere al gestore di un motore di ricerca la rimozione di tutti i link che portano a contenuti, seppur legittimi e veritieri, ritenuti non più pertinenti con la propria immagine “sociale”, non più attuali, essendo trascorso un determinato lasso di tempo.

Il diritto all’oblio è un tema molto interessante ed esprime il più ampio diritto del singolo alla protezione dei dati personali che lo riguardano; tuttavia, non si configura come diritto assoluto, essendo necessario un bilanciamento con l’interesse economico del gestore del motore di ricerca e con l’interesse pubblico ad accedere alle informazioni contenute anche *online*.

Eppure, la riforma, che si incentra sulle informazioni di carattere giudiziario, sembrerebbe fornire una tutela non suscettibile di bilanciamento con gli interessi contrapposti: qualora, infatti, un procedimento penale si concluda in senso favorevole all’indagato/imputato, si pone come preminente il diritto dell’interessato alla deindicizzazione dei dati e delle notizie ad esso relative.

In tutti gli altri casi, invece, si ricorrerà ai presupposti, positivi e negativi, individuati dall’art. 17 GDPR e precisati dalla giurisprudenza (si pensi, ad esempio, all’insussistenza di un interesse pubblico specifico e attuale alla diffusione della notizia).

Come è stato osservato dalla dottrina, il riferimento alla «deindicizzazione» sembrerebbe *«limitare la portata di questo “speciale” diritto all’oblio al solo contesto dei motori di ricerca e affini, lasciando impregiudicata la facoltà di editori e responsabili di testate giornalistiche o telematiche di pubblicare, conservare su archivi telematici e rendere accessibili sul proprio sito web notizie relative a procedimenti penali (passati), pur se definiti con archiviazione, non luogo a procedere o assoluzione»*⁶².

In questo caso si applicherà la disciplina generale, come interpretata dalle Sezioni Unite della Corte di Cassazione nella sentenza n. 1981 del 2019, che ha ribadito la necessità di bilanciare la libertà delle scelte editoriali con la sussistenza di un attuale interesse della collettività alla notizia e con l’impiego di modalità espressive non eccedenti lo scopo informativo.

⁶¹ P. CARETTI e A. CARDONE, “*Diritto dell’informazione e della comunicazione nell’era della convergenza*”, Bologna, Mulino, 2019, p. 253.

⁶² F. MARENGHI, “*Riforma giustizia penale: il provvedimento di «deindicizzazione»*”, su *altalex.com*.

Comunque, la legge delega non specifica la forma o la procedura del «provvedimento di deindicizzazione»; inoltre, bisognerà definire la portata territoriale dei provvedimenti di deindicizzazione, data la necessità di garantire una tutela effettiva nello spazio a-territoriale e globale della rete. Su questo aspetto si è recentemente pronunciata la Corte di Giustizia (nella causa C-507/17, Google/CNIL), la quale ha specificato che i gestori dei motori di ricerca sono tenuti a operare la deindicizzazione dei contenuti indicati dall'interessato nel solo ambito territoriale di tutti gli Stati membri dell'Unione.

In conclusione, il diritto alla deindicizzazione rappresenta il crocevia tra la disciplina della tutela dei dati personali e il diritto processuale penale ed esprime la necessità più ampia di adattare la disciplina del processo penale alle nuove esigenze della società digitale, collegandosi con il recente decreto legislativo di attuazione della direttiva UE 2016/343 in materia di presunzione di innocenza approvato l'8 novembre 2021⁶³.

⁶³ Il D.lgs. 8 novembre 2021, n. 188, in vigore dal 14 dicembre 2021, rende conforme la normativa italiana alle indicazioni euro-unitarie in tema di presunzione di innocenza. Sul tema, v. F. MARENGHI, *“Diritto alla presunzione di innocenza e nuovi strumenti di tutela”*, su *altalex.com*, febbraio 2022. L'art. 2 del nuovo decreto ha introdotto un divieto espresso per le pubbliche autorità di indicare pubblicamente come colpevole la persona indagata o imputata, fino al momento in cui la colpevolezza non sia accertata con sentenza o decreto penale di condanna irrevocabili. Se tale disposizione viene violata, oltre alle conseguenze penali, disciplinari e risarcitorie già previste dall'ordinamento, è ora possibile per l'interessato richiedere alla stessa autorità dichiarante la rettifica della dichiarazione lesiva del diritto alla presunzione di innocenza. Se l'autorità ritiene fondata la richiesta, si può procedere immediatamente (o comunque non oltre 48 ore) alla rettifica, altrimenti l'autorità può non accogliere la richiesta, ove questa risulti infondata. In questo ultimo caso, e nel caso in cui la rettifica non rispetti le modalità di pubblicazione previste, l'interessato può ricorrere al Tribunale ex art. 700 c.p.c., al fine di ottenere l'ordine diretto all'autorità di pubblicazione della rettifica. L'art. 3 della novella legislativa modifica la disciplina dei rapporti tra Pubblico Ministero e gli organi di informazione, introducendo le seguenti previsioni: *«il procuratore della Repubblica (o il magistrato dell'ufficio appositamente delegato) mantengono i rapporti con gli organi di informazione esclusivamente tramite comunicati ufficiali, oppure – nei casi di particolare rilevanza pubblica dei fatti, e sulla base di determinazione assunta con atto motivato che dia conto delle specifiche ragioni di interesse pubblico – tramite conferenze stampa; la diffusione di informazioni sui procedimenti penali è d'ora innanzi consentita soltanto quando strettamente necessaria per la prosecuzione delle indagini o in presenza di altre specifiche ragioni di interesse pubblico; nei casi in cui la diffusione di informazioni sui procedimenti penali è consentita, il procuratore della Repubblica può autorizzare (con atto motivato) gli ufficiali di polizia giudiziaria a fornire, tramite comunicati ufficiali o conferenze stampa, informazioni sugli atti di indagine compiuti; nei comunicati e nelle conferenze stampa è vietato assegnare ai procedimenti pendenti denominazioni lesive della presunzione di innocenza. La vigilanza sul rispetto di tali modalità e divieti è affidata al Procuratore Generale presso la Corte di Appello»*. Anche l'art. 329 c.p.p., in tema di segreto sugli atti di indagine, è stato modificato, con la previsione che il Pubblico Ministero possa autorizzare la pubblicazione di singoli atti o parti di essi soltanto qualora ciò sia «strettamente» necessario per la prosecuzione delle indagini. Un'altra novità importante è rappresentata dal nuovo art. 115-bis c.p.p. sulla garanzia della presunzione di innocenza: *«nei provvedimenti diversi da quelli che decidono della responsabilità penale dell'imputato (e con esclusione degli atti del pubblico ministero volti a dimostrare la colpevolezza della persona interessata), la persona indagata o imputata non può essere indicata come colpevole, fino a quando la colpevolezza non è stata accertata con sentenza o decreto penale*

Si tratta di una misura che rientra tra quelle previste dal PNRR in ambito penale per limitare la diffusione delle notizie sui procedimenti penali, avendo riguardo delle dichiarazioni delle autorità pubbliche e dei rapporti con la stampa⁶⁴.

di condanna irrevocabili; in caso di violazione, la persona interessata può, nei dieci giorni successivi, richiedere la correzione del provvedimento, quando è necessario per salvaguardare la presunzione di innocenza nel processo. Sull'istanza di correzione il giudice provvede, con decreto motivato, entro quarantotto ore dal suo deposito. Il decreto è notificato all'interessato e alle altre parti e comunicato al pubblico ministero, i quali nei dieci giorni successivi possono proporre opposizione al presidente del tribunale o della corte; nei provvedimenti diversi da quelli che decidono della responsabilità penale dell'imputato e che tuttavia presuppongono la valutazione di prove, elementi di prova o indizi di colpevolezza, l'autorità giudiziaria deve limitare i riferimenti alla colpevolezza della persona indagata o imputata a quanto necessario (presupposti, requisiti e condizioni) per l'adozione del provvedimento».

⁶⁴ In conclusione, si può accennare alla problematica relativa all'acquisibilità delle testimonianze degli assistenti vocali nel processo penale. Sappiamo che è dal 2015 che negli Stati Uniti *Alexa* assume le vesti di vero e proprio testimone nel processo: il caso più recente si è verificato nel luglio del 2019, in Florida, quando un uomo è stato accusato di aver ucciso la fidanzata nella loro abitazione. Gli inquirenti, tramite mandato di perquisizione, hanno analizzato le registrazioni del dispositivo di assistenza vocale presente in casa, per ottenere indizi o prove sull'accaduto. Sul tema, vedi F. ZAMBONIN, "Alexa testimone in un caso di omicidio", su *Il tuo legale*, 2019 e A. BENVENÜ, "Alexa, unica testimone di un omicidio. E (legittime) domande sulla nostra privacy", su *Nera-Mente*, 2020. Per quanto riguarda la normativa italiana, in astratto, le registrazioni degli *smart assistant* e le trascrizioni possono essere utilizzate nel processo nel rispetto della disciplina penalistica e civilistica. Il problema che si pone è che la registrazione sonora di una conversazione da parte di un soggetto che ne sia parte presuppone, di norma, il consenso anche degli altri interlocutori, tranne però il caso in cui la raccolta dei dati intervenga per far valere o difendere un diritto in sede giudiziaria o stragiudiziale (Cass. Civ., sent. n. 11322/2018). Inoltre, se l'interlocutore registra la conversazione all'insaputa dell'altro, non si configura la fattispecie dell'intercettazione, bensì una mera modalità di documentazione dei contenuti già nella disponibilità di chi effettua la registrazione, con la possibilità di trasporre il contenuto nel processo attraverso la testimonianza (Cass. Pen. Sez. II, sent. n. 19158/2015). Comunque, in Italia non c'è ancora una normativa specifica che si occupi dell'acquisizione della testimonianza dei dispositivi di assistenza vocale: in dottrina si sta facendo riferimento ad un possibile futuro ingresso nel procedimento penale delle registrazioni tramite *smart speaker* come prova atipica (ex art. 189 c.p.p. – che così dispone: «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova» – articolo concepito come "valvola di sicurezza" per convogliare il progresso scientifico all'interno del processo penale).

Capitolo IV

Algoritmo e contratto

L'algoritmo ha determinato oggi un "mutamento genetico" del contratto, destinato ad evolversi da strumento di "concretizzazione" dell'autonomia privata ex art. 1322 c.c. a strumento totalmente "eterodeterminato". La tecnologia si inserisce nelle dinamiche contrattuali e decide in luogo delle parti, superando le impostazioni concettuali sia del giusrealismo che del giusformalismo, volti a definire il concetto della giustizia contrattuale come principio di equilibrio. La nozione funzionale della "causa", intesa come "causa in concreto", funzione economico-individuale, si evolve, così, sempre più in "*consideration*", in valore e certezza delle prestazioni. Questo fenomeno evolutivo si coglie nella figura degli *smart-contract*: pur non essendo dei contratti in senso giuridico possono integrare atti della vicenda contrattuale, laddove gli algoritmi che li costituiscono siano programmati per il compimento di atti che costituiscono fasi (o esauriscono) la conclusione o esecuzione del contratto. Uno *smart-contract* o più *smart-contract* possono essere programmati in maniera tale da individuare quando coincidono le richieste di due o più parti ai fini della conclusione di un contratto ovvero per trasferire un determinato bene digitale al verificarsi di una certa condizione, avendo intercettato un algoritmo che è programmato per il pagamento al verificarsi della medesima condizione. Ad esempio, un protocollo può essere istruito al fine di vendere/acquistare un certo tipo di bene (ad esempio, partecipazioni azionarie) una volta che il prezzo raggiunge una certa soglia o ulteriori condizioni vengano soddisfatte (secondo la sequenza informativa dell'*if-then*). È, altresì, possibile che uno *smart-contract* svolga un ruolo nella sola fase di esecuzione del contratto, prevedendo il pagamento *online* una volta che il bene sia consegnato al compratore. Una delle manifestazioni più diffuse di *smart-contract* è quella dove gli stessi applicano un registro decentralizzato ai rapporti di scambio costituita dalla *blockchain* che è la tecnologia alla base del *software* protocollo *bitcoin* per il trasferimento moneta/valore digitale.

La *blockchain* è una piattaforma senza intermediari – e perciò, decentralizzata, priva di sorveglianza o intervento di terzi sulle operazioni – per la conclusione, formalizzazione e gestione di rapporti di scambio digitali (ambiente informatico dematerializzato) di beni immateriali/dematerializzati. Il controllo è decentralizzato grazie ad un *data base* pubblico e condiviso da tutti i c.d. *miner* del *network*, rappresentati da tutti gli utenti del *Bitcoin*. Il sistema dei registri decentralizzati opera come un sistema di contabilità e i blocchi di operazioni vengono man mano validati ed eseguiti con una tempistica serrata di dieci minuti, in maniera tale da non poter essere modificati dopo questo intervallo. Oltre alla pseudonimia degli utenti, l'utilità di questo registro decentralizzato sta nel fatto che, tramite la piattaforma, qualsiasi bene virtuale

o tangibile, ma rappresentato digitalmente, può essere trasferito mediante la stessa ed è registrato in maniera indelebile. Questa tecnologia veloce riduce i rischi di errori dell'intermediario e, se si guarda al funzionamento della *blockchain* dalla prospettiva delle vicende giuridiche della fase esecutiva, appare evidente che l'automazione delle operazioni riduce il rischio di inadempimento contrattuale implicito nella conclusione del contratto. Si determina, così, la “certezza assoluta dell'adempimento contrattuale” con un automatismo certificato. L'esecuzione viene affidata ad una rete e non può essere influenzata una volta lanciato lo *smart-contract* nella *blockchain*. L'automazione può inerire esclusivamente la formazione di un contratto: ciò si realizza qualora un algoritmo sia impiegato nella definizione del contenuto contrattuale, delineando le obbligazioni delle parti prima o dopo la conclusione del contratto c.d. *gap filler and loss distribution*. Si parla, a tal proposito, di *self-driving contracts*, qualora le parti individuino un obiettivo comune, lasciando all'algoritmo, che in questo caso è una forma di intelligenza artificiale (*analytics*), il compito di definire il contenuto del contratto. Un esempio del genere è chiaro in quelle assicurazioni in cui il premio varia a seconda dello stile di guida per come monitorato dall'applicazione app per *smartphone* che permette di conoscere l'esatta posizione del veicolo, la sua velocità e la quantità di chilometri percorsi. Occorre, però, chiedersi: l'algoritmo può sostituire totalmente l'autonomia privata insita nella definizione giuridica del contratto ex art. 1321 c.c.? Allo stato attuale, la valutazione tramite *analytics* non modifica automaticamente il contenuto/oggetto del contratto. Un punteggio elevato corrisponde ad una certificazione di basso profilo di rischio e se l'assicurazione decide di inserire la valutazione nel calcolo delle tariffe, il cliente usufruisce di uno sconto al momento del rinnovo della polizza. Abbiamo poi i contratti c.d. *High Frequency Trading o dynamic pricing*, o contratti *IoT*, come il servizio *Amazon's Dash Replenishment*: quest'ultimo consente a dispositivi tra loro connessi tramite sensori di ordinare beni su Amazon, quando lo stesso si sta esaurendo presso l'utente del servizio.

Fino a che punto, però, l'intelligenza artificiale può riprodurre il processo decisionario dell'uomo? La dottrina più autorevole è nel senso di ritenere che l'operare dell'algoritmo possa costituire dichiarazione, anche tacita, ovvero costituire inizio di esecuzione valevole alla conclusione del contratto o al compimento di altro atto esecutivo. Più critico appare affrontare il problema del malfunzionamento del programma o del governo della responsabilità. Il malfunzionamento dell'algoritmo va valutato nell'ambito della distribuzione del rischio contrattuale in un'accezione ampia, che non si riduce alla gestione delle sopravvenienze (*théorie dell'imprévision* o *doctrine of frustration*), ma al rischio di inadempimento che comporti la mancata soddisfazione economica dell'affare. Il malfunzionamento dell'algoritmo rientrerebbe nel caso fortuito o nel generale concetto di rischio nell'attività di impresa i cui costi devono essere allocati nella c.d. curva dell'indifferenza, volendo aderire alla teoria di

analisi economica del diritto di *Shavell*. Ma se optiamo per una definizione di responsabilità basata sulla colpa, allora occorre considerare il grado di autonomia decisionale dell'algoritmo, ossia se è “*mere tool*”, o dotato di “*ability to learn and decide*”. Quest'ultima prospettiva è stata fatta propria dalla recente Risoluzione del Parlamento europeo del 16 febbraio 2017 recante Raccomandazione della Commissione concernente norme di diritto civile sulla robotica, che non solo pone un problema di riconoscimento della personalità elettronica per i robot autonomi e decisionali, ma anche di responsabilità contrattuale delle macchine. Di recente, la giurisprudenza ha evidenziato che gli algoritmi possono essere utilizzati nei contratti se le parti hanno contezza dei c.d. “*schemi esecutivi*”.

La Suprema Corte di Cassazione, sez. I civile, con ordinanza 25 maggio 2021, n. 14381, ha stabilito che «*il consenso al trattamento di dati finalizzato all'elaborazione di profili reputazionali di singole persone fisiche e all'attribuzione di punteggi di affidabilità attraverso un algoritmo può dirsi “informato”, “specifico” e “consapevole” solo se il titolare rende conoscibile in modo trasparente agli interessati lo schema esecutivo dell'algoritmo e i parametri su cui si basa la valutazione dallo stesso svolta*».

Ma cosa significa conoscere lo schema esecutivo di un algoritmo?

In via preliminare, occorre precisare che la decisione della Cassazione si pone in linea con quanto previsto dalle *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* del gennaio 2017, dalla Convention 108 e dalle Linee Guida del WP29 relative alla trasparenza di aprile 2018 e ai processi decisionali automatizzati relativi alle persone fisiche e alla profilazione di febbraio 2018, ove viene sottolineata l'importanza che gli interessati siano adeguatamente informati sulle modalità di impiego dei propri dati personali nell'ambito dei processi elaborativi legati all'utilizzo dei *Big Data*.

Le *Guidelines*, in particolare, prevedono che all'interessato siano illustrati i rischi legati all'utilizzo dei propri dati mediante tecnologie *Big Data*, così da evitare che vengano sottoposti a un trattamento che risulti in qualche modo non prevedibile o inappropriato. Ciò, anche, mediante la condivisione con gli interessati degli aspetti più rilevanti delle valutazioni di impatto dei trattamenti sottesi nei termini di cui all'art. 35 del GDPR che possono meglio chiarire modalità e termini dei trattamenti.

Sulla base di tale previsione, secondo una certa impostazione dottrinaria, non esisterebbe solo il diritto di non esclusività di cui all'art. 22 del GDPR, ma un vero e proprio *right to explanation*, ossia uno specifico diritto degli interessati di conoscibilità delle modalità di funzionamento dell'algoritmo. Tale diritto sarebbe enucleabile in via interpretativa dall'art. 15 del GDPR che statuisce il diritto di accesso degli interessati: muovendo da tale ricostruzione, i fautori di questa tesi giungono a definire un nuovo concetto di trasparenza in termini di *legibility*, da intendersi quale capacità degli

interessati di capire autonomamente i dati e i parametri presi in considerazione dal titolare nelle sue elaborazioni.

Occorre, però, a questo punto chiedersi quale sia il livello di trasparenza da attuare e in che cosa concretamente dovrà tradursi l'esplicitazione dello "schema esecutivo" dell'algoritmo utilizzato per il trattamento dei dati.

Tale schema esecutivo potrà presentare una notevole complessità tecnica che il cittadino comune potrebbe anche non cogliere perfettamente. Un articolato contenuto tecnico potrebbe, infatti, risultare eccessivo e non far realmente comprendere la logica algoritmica utilizzata, ma, anzi, scoraggiare il destinatario "medio" di servizi, anche molto complessi, da una reale ed effettiva comprensione del funzionamento degli stessi. L'eccessiva scrupolosità tecnica nella descrizione delle logiche algoritmiche potrebbe non colmare quel deficit formativo dell'interessato, specie tenuto conto dell'efficacia media delle informative attualmente già distribuite, e indurre lo stesso a fornire comunque un consenso altrettanto non informato.

Alla luce di quanto sopra osservato, rispetto agli elementi di cui si compone un algoritmo, infatti, deve ritenersi che la verifica possa essere svolta esclusivamente sui dati oggetto di trattamento e le relative finalità. Ecco perché la lettera f) dell'articolo 13 del GDPR fa riferimento, quando declina l'onere informativo, alla "*logica utilizzata*" nel processo decisionale.

La puntuale descrizione dei passaggi computazionali effettuati da un algoritmo e delle variabili prese in esame potrebbero non presentare quel livello di trasparenza che la Cassazione ha individuato come presupposto per la informata, valida e consapevole prestazione del consenso. Ciò, in quanto la consapevolezza del trattamento cui saranno sottoposti i dati si ritiene presupponga il possesso di molteplici conoscenze e "competenze trasversali" che consentono di comprendere quanto rappresentato dal titolare in sede informativa.

In ambito farmaceutico, ad esempio, tale valutazione viene rimessa ad un soggetto terzo, come l'Aifa, in ambito nazionale e l'Ema, in ambito europeo, che certifica, e quindi autorizza (anche con CMA, ossia *conditional market authorisation*), la commercializzazione di farmaci dei quali il cittadino comune non è in grado di valutare l'efficacia e la sicurezza per la propria salute, residuando in capo al paziente il solo diritto a conoscere la mera elencazione statistica delle possibili controindicazioni che potrebbero derivare dall'assunzione del farmaco.

Inoltre, si osserva che il paragrafo 6, dell'articolo 5, del Regolamento 2019/1150, cosiddetto *Platform to Business*, espressamente esclude che le piattaforme e i motori di ricerca abbiano l'obbligo di «*rivelare algoritmi o informazioni*».

Viene allora da chiedersi come bilanciare l'obbligo di trasparenza con le necessarie tutele degli investimenti realizzati dai privati e con il principio di *accountability* che governa il GDPR.

Nel settore farmaceutico, si osserva come la trasparenza della formula chimica, non algoritmica, sia subordinata al riconoscimento di un diritto di privativa rappresentato dal brevetto che consente al privato di non veder pregiudicati gli investimenti di sviluppo sostenuti.

Nel settore limitrofo dell'alimentazione, la trasparenza della formula è sostituita dalla elencazione degli ingredienti, cosicché vengono comunemente commercializzate bibite gassate di cui si conoscono gli ingredienti, ma non la esatta composizione e il cui oggetto costituisce, dopo decine di anni, il vantaggio commerciale su cui è stato costruito un impero economico.

In questo senso, deve dedursi che il diritto di accesso di cui all'art. 15 del GDPR trovi un limite nei diritti del titolare di non svelare tutti i passaggi computazionali dell'algoritmo impiegato per l'elaborazione effettuata, in quanto "segreto industriale", atteso che il "segreto" costituisce la miglior protezione possibile, anche rispetto alle forme di privative tradizionali del diritto di autore e del brevetto, sia rispetto agli algoritmi che con riferimento ai loro prodotti. L'art. 121-ter del D.lgs. 30/2005, ove è stata recepita la direttiva 943/2016, legittima la conoscibilità dei segreti industriali da parte di terzi esclusivamente nei procedimenti giurisdizionali, non anche nel corso di istruttorie amministrative come quella svolta dal Garante, sebbene la direttiva europea genericamente parlasse di conoscibilità dei segreti da parte delle autorità pubbliche. Peraltro, l'indicazione risulta confermata dall'art. 5 del Regolamento P2B, che circoscrive il potere di analisi e verifica delle autorità statali alla disamina dei "criteri generali" usati ai fini del posizionamento. Anche in tale caso, comunque, è l'Agcom ad essere competente ad effettuare le relative verifiche, senza pregiudizio della segretezza degli algoritmi sviluppati.

In che termini, allora, deve svolgersi la c.d. *valutazione di impatto* "Dpia" sul trattamento dei dati? La valutazione eseguita dal titolare può dirsi sufficiente a garantire l'interessato, se ancora oggi non esistono modalità di misurazione dei rischi certe ed univoche (programma del Cnil, *tool* di Enisa, ecc.)?

Viene, in altri termini, da chiedersi se non possa prevedersi la facoltà, per i titolari del trattamento che vogliono effettuare nuove forme di trattamento incentrate sulla intelligenza artificiale e su elaborazioni algoritmiche, di rivolgersi, in ottica di *preventiva validazione*, all'autorità di controllo con meccanismi celeri di valutazione, compatibili con i tempi di sviluppo dell'attività imprenditoriale, anche prevedendo dei contributi finanziari volti a coprire i relativi costi amministrativi.

È, d'altronde, riconosciuta e condivisa la circostanza per cui i trattamenti dei dati legati alle nuove tecnologie presentino delle specificità che richiedono un nuovo approccio dinamico basato su una *due diligence* in ragione dell'impossibilità di definire *ex ante*

tutte le finalità del trattamento, anche in ragione della impossibilità di predeterminare tutti gli *output* informativi e i relativi utilizzi da parte del titolare. Ciò, soprattutto, nelle ipotesi, come quella su cui si è pronunciata la Cassazione, ove il trattamento viene a coincidere esattamente con il servizio prestato dal titolare.

L'art. 32 del GDPR sancisce il principio dell'*accountability*: tale principio comporta che sia il titolare del trattamento a determinare le misure di sicurezza designate al trattamento dei dati personali, che effettua *“tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e della finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche”*. In questo caso, come in altri, il legislatore affida al titolare l'onere di individuare in che modo adempiere alle prescrizioni dettate dalla norma, calandola nella fattispecie concreta, assumendosi la responsabilità non solo della implementazione, ma anche della valutazione.

Con riguardo alle applicazioni di intelligenza artificiale, un tentativo di formulare un modello di responsabilità non può prescindere da una combinazione, da un lato, dell'*accountability* del titolare del trattamento, dall'altro, da una formulazione che prescinde dagli elementi soggettivi, nonché dalla individuazione dell'errore, *“issue of liability”*, *“issue of permittance”*, *“responsability gap”*.

Se è vero che il modello di protezione dei dati deve essere dinamico e non statico, il principio dell'*accountability* basato sull'autodeterminazione non può essere idoneo a regolare l'intelligenza artificiale e i *Big data*, per i quali la determinabilità a priori dei processi di elaborazione non è scontata e nelle quali la finalità del trattamento non potrebbe essere chiara.

Questo perché l'algoritmo *AI self learning*, nato buono, può travalicare in *“malware”* (*malicious software*) a causa del suo addestramento. Quindi, anche il consenso inequivoco, specifico, consapevole non può costituire l'unico strumento di tutela in una dimensione globale del trattamento dei dati.

“Methaphorically, it is a law of the sea were based on the principle of controlling every drop of water in the oceans according to its origin” (Sembra quasi che si tenti di governare le onde del mare goccia a goccia, individualmente considerando la goccia): così Bergè Grumbach⁶⁵.

L'ideatore dell'algoritmo dovrebbe essere ritenuto responsabile non solo verso il committente, ma anche verso i terzi lesi dall'entità intelligente, configurando un risarcimento del danno da IA in base al criterio di *“provenienza prossima”*.

⁶⁵ Z. ZENCOVICH, *“The Datasphere, Data flows beyond control and the challenges for law and governance”*, in *European Journal of Comparative Law and Governance*, V, 2019/162.

Si entra così nella sfera del “*tecnodiritto*”: responsabilità della *machine learning*, *deep learning*, responsabilità del produttore, dell’ideatore dell’algoritmo, dell’addestratore *self learning*, al di là del pensiero computazionale, responsabilità da prodotto *product liability* (labile confine tra “prodotto” e “servizio” nel settore dell’IA) ed anche responsabilità ex art. 2051 c.c. da cose in custodia e responsabilità per attività pericolosa ex art. 2050 c.c., anche in relazione all’elevata incidenza del “*rischio da sviluppo*”.

Ma se l’intelligenza artificiale è autoevolutiva, allora si potrebbe attribuire a tale entità la c.d. personalità giuridica elettronica: Teubner per primo ha parlato di “soggetti giuridici digitali”.

Allora, ecco che si compie il salto quantico: il passaggio dal “bene” ad “essere”, “*machine sapiens*” o “*machine senties*” con autocoscienza, da “antropomorfizzazione” al concetto di “entità dotata da autonomia”.

Da qui, il concetto di responsabilità da atto lecito, *Gefährdungshaftung* invocata per i soggetti giuridici digitali. L’IA si nutre di *Big Data*: la sua capacità di crescita è inversamente proporzionale al tasso di tutela della privacy, maggiore è l’accesso ai dati, maggiore è la sua capacità di crescita.

La qualità dei dati diventa, come sopra già esposto, essenziale: da dati qualitativamente non corretti, non possono che scaturire elaborazioni non corrette, secondo il noto principio “*garbage in, garbage out*”, sulla base dello “*Human in command*”.

È evidente il contrasto che emerge, da un lato, tra l’esigenza di disporre di un’ingente mole di dati ai fini dello sviluppo di sistemi di intelligenza artificiale, e, dall’altro, la necessità di conservare il principio di proporzionalità e di minimizzazione dettato dal Regolamento 679/2016, secondo cui il trattamento dovrebbe avere ad oggetto soltanto i dati strettamente necessari e pertinenti rispetto alle finalità perseguite.

Tale tensione impone necessariamente un bilanciamento di interessi, che vede contrapposti il diritto alla protezione dei dati personali e l’esigenza di disporre dei dati personali per sviluppare le applicazioni di intelligenza artificiale.

Ci si è chiesti⁶⁶ se il titolare del trattamento (c.d. “*controller*”) possa essere la stessa applicazione di intelligenza artificiale, o se si preferisce, il robot.

La definizione di titolare del trattamento contenuta nel Regolamento (art. 4, n. 7) indica che il titolare debba essere una persona giuridica o fisica o, comunque, soggetto giuridico (“*Il titolare del trattamento è la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determini la finalità e i mezzi di trattamento dei dati personali*”).

Se l’applicazione non ha soggettività giuridica, evidentemente non può essere titolare. Ma l’attribuzione di soggettività giuridica deve corrispondere ad una precisa e

⁶⁶ F. PIZZETTI, “*Intelligenza artificiale, protezione dei dati personali e regolazione*”, Torino, 2018.

consapevole scelta metodologica e fondare un nuovo approccio al tema della responsabilità.

Ai sensi dell'art. 4, n. 8 del GDPR, il responsabile del trattamento (c.d. “*processor*”) è “*la persona fisica o giuridica, o l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*”.

Se all'applicazione non viene attribuita una disponibilità economica e se non viene ridisegnato un regime di responsabilità che prescinda da elementi soggettivi, evidentemente non riferibili all'applicazione, l'attribuzione di soggettività giuridica alle applicazioni di intelligenza artificiale e ai robot diviene un atto non qualificabile giuridicamente. Lo stesso argomento si può svolgere per la designazione dei robot quale responsabile del trattamento. Anche in questo caso la designazione del robot quale responsabile richiede la soggettività giuridica del medesimo, soggettività che non può essere, tuttavia, fine a sé stessa, ma che si deve inserire in un nuovo modello di responsabilità.

Chi è il soggetto responsabile nel caso di danni cagionati da un'applicazione di intelligenza artificiale?⁶⁷ In particolare, l'attenzione si focalizza sui casi in cui l'esito dell'elaborazione effettuata dalla applicazione di intelligenza artificiale non sia del tutto controllabile a priori e sia caratterizzato da un certo grado di imprevedibilità: non sia, cioè, un processo deterministico, ma sia caratterizzato da una certa autonomia elaborativa.

Si discute se sia l'autore del programma, il produttore, il venditore o l'utilizzatore che ne trae vantaggio. Nella consapevolezza che ogni fenomeno nuovo richiede nuove norme, il tema della responsabilità nelle applicazioni di intelligenza artificiale richiede un approccio nuovo e basato su un modello concettuale differente, per rubare un termine alla tecnologia, “*disruptive*”.

Occorre superare il paradigma basato sull'errore e sulla colpa e, invece, affrontare il tema sotto il profilo dell’“allocazione del rischio”.

Occorre prevedere meccanismi di allocazione del costo del danno cagionato su quei soggetti che astrattamente potrebbero essere responsabili, ad esempio, mediante la

⁶⁷ Il tema è molto ampio. In ambito penale si vedano i contributi di G. HALLEVY, “*The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control*”, in *Akron Intellectual Property Journal*, 2010; “*I, Robot – I, Criminal – When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offences*”, in *Syracuse Science & Technology Law Reporter*, 2010; “*Virtual Criminal Responsibility*”, in *Original Law Review*, 2010; “*Dangerous Robots – Artificial Intelligence vs. Human Intelligence*”; “*Unmanned Vehicles: Subordination to Criminal Law under the Modern Concept of Criminal Liability*”, in *Journal of Law, Information and Science*, 2012; “*When Robots Kill. Artificial Intelligence under Criminal Law*”, Boston, 2013; “*Liability for Crimes Involving Artificial Intelligence Systems*”, Springer (Dordrecht), 2015; S. RIONDATO, “*Robotica e diritto penale (robot, ibridi, chimere, “animali tecnologici”)*”, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), “*Genetics, Robotics, Law, Punishment*”.

costituzione di un fondo al quale attingere, prescindendo dall'individuazione delle modalità dell'incidente o dell'errore.

Analogo meccanismo è stato previsto nel circuito delle carte di credito, per il caso di danneggiamento o furto.

Uno degli obiettivi perseguiti con questo tipo di sistema di allocazione del rischio è immediatamente evidente ed è quello di assicurare i potenziali utilizzatori sul fatto che, a prescindere dagli esiti di una costosa ricerca dell'errore, otterranno un risarcimento.

A tal proposito, è stata significativa la Risoluzione del Parlamento Europeo del 16 febbraio 2017 – recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103 INL) – ove la Commissione europea è invitata a valutare talune soluzioni giuridiche possibili in relazione al regime di responsabilità dei robot, tra cui «*l'istituzione di uno status giuridico specifico per i robot nel lungo termine (...), nonché eventualmente il riconoscimento della personalità elettronica dei "robot" (par. 59, lett. f)*».

Come si concilia, però, il concetto di decisione robotizzata o automatizzata con il principio di *accountability*?

Il termine *accountability* può essere tradotto in responsabilità e, insieme, prova della responsabilità. Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche per la protezione dei dati personali, anche attraverso l'adozione di specifici modelli organizzativi che si possono pensare analoghi a quelli utilizzati in Italia nell'applicazione del D.lgs. 8 giugno 2001, n. 231.

Le norme del regolamento sull'*accountability* hanno, dunque, lo scopo di promuovere l'adozione di misure concrete e pratiche, trasformando i principi generali della protezione dei dati in politiche e procedure organizzative concrete, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento deve anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. In altre parole, l'*accountability* è un meccanismo a due livelli: da un lato, l'attuazione di misure e procedure, e dall'altro, la conservazione delle relative prove.

Come può operare questo sistema a due livelli con un'entità intelligente?

Si potrebbe ipotizzare un doppio livello di operatività anche della responsabilità: un regime di responsabilità oggettiva per i sistemi ad alto rischio sintetizzato nei termini *liability, transparency e security*; e responsabilità aggravata, per colpa presunta, secondo il modello attuale del GDPR, che prescinde dalla soggettività giuridica. Come potrebbero applicarsi tali principi alle tecnologie basate sui "registri distribuiti"? Per poter regolare tali meccanismi, il giurista deve prima comprenderli nella loro intrinseca essenza ed operatività.

Al c.d. Decreto Semplificazioni 2019 (d.l. 135/2018) è stato aggiunto, in sede di conversione in legge, l'art. 8-ter, il quale ha introdotto, nel nostro ordinamento, la definizione di “tecnologie basate su registri distribuiti” e di “*smart contract*”.

Ai sensi del primo comma dell'art. 8-ter, «*si definiscono “tecnologie basate su registri distribuiti” le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetture decentralizzate su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*».

Le tecnologie basate su registri distribuiti sembrerebbero richiamare le c.d. *distributed ledger technologies* (o DLT), ossia le reti digitali decentralizzate ispirate alla *Bitcoin*, ormai famosa in tutto il mondo.

Bitcoin fu creata nel 2008 da alcuni *hacker* anonimi che volevano creare una forma digitale di denaro (c.d. *criptovaluta*), senza che essa avesse corso legale nello Stato né alcun sottostante materiale in controvalore.

La moneta virtuale chiamata *Bitcoin* è diventata, ormai, molto sostenuta tra il pubblico mondiale: il suo successo è dovuto ad alcuni ideali monetari di stampo democratico e internazionalista, a motivi speculativi⁶⁸ o di agevolazione delle transazioni legate ad attività illecite e, soprattutto, al superamento di due cruciali problemi che scoraggiavano l'adozione di forme integralmente digitali di denaro.

Da un lato, era temuto il rischio della doppia spesa della stessa unità monetaria e, dall'altro, si paventava la necessità di essere assistiti da intermediari di fiducia per ogni transazione.

Bitcoin ha offerto proprio una soluzione tecnologica a tali criticità, tramite la creazione di un registro delle transazioni decentralizzato, distribuito fra tutti gli utenti della rete, che possono accedere a ogni sua parte e verificarne autonomamente la regolarità. L'organizzazione del registro è su base crittografica, in modo tale da risultare, di norma, immutabile e insuscettibile di manomissioni fraudolente.

È necessaria la firma digitale per riservare al titolare effettivo la disponibilità esclusiva di ogni unità di *criptovaluta*.

La rete DLT sinonimo per antonomasia è la c.d. *blockchain* (“catena di blocchi”), inaugurata da *Bitcoin*; vi rientrano anche i c.d. *ledger* (“libro mastro”) tradizionale e il

⁶⁸ Mentre si scrivono le pagine del presente libro, è scoppiata con toni drammatici una rivolta in Kazakistan per il caro bollette, dipesa dai proprio dai *Bitcoin*, che ormai sembrano essere diventati uno strumento di alterazione degli equilibri internazionali. I c.d. “*Miners*”, ossia coloro che gestiscono le *criptovalute*, sono “scappati” dalla Cina, che ha proibito qualsiasi attività legata alle *criptovalute*, e si sono spostati in Kazakistan per ottenere maggiore guadagno, utilizzando l'energia dei carboni fossili. Ciò ha fatto salire le bollette e il costo dei carburanti nel paese, per cui è nata una rivolta che si sta evolvendo in una guerra civile, tanto che è stato necessario l'intervento della Russia per ristabilire l'ordine. I *Miners* con ogni probabilità si sposteranno negli Stati Uniti, dove si stanno concentrando sull'energia rinnovabile. Questa vicenda ci fa comprendere che non si tratta più di alterazione della borsa, ma collegandosi con la produzione dell'energia di uno Stato, le piattaforme sono diventate veri e propri soggetti di diritto internazionale, che alterano gli equilibri internazionali.

tangle (“intreccio”). Questi ultimi operano in base a diversi sistemi di raggruppamento delle transazioni da validare prima per essere iscritte permanentemente nel registro condiviso.

Ogni rete può usare diversi sistemi di controllo decentralizzato della regolarità delle transazioni, basati sempre su tecniche di crittografia, in particolare:

- (i) il voto a maggioranza;
- (ii) la *proof of work* (“prova di lavoro”);
- (iii) la *proof of stake* (“prova della posta in gioco”);
- (iv) la *proof of authority* (“prova di autorevolezza”).

Le reti DLT, oltre a rappresentare il valore monetario, possono, se progettate in tal senso, ospitare anche altre forme di “elementi” digitali, i c.d. *token* (“gettoni”), fungibili o meno, stringhe di codice irripetibili rappresentative di diritti o beni materiali effettivamente esistenti nel mondo “analogico”, oppure utilizzati per riservare l’accesso esclusivo a servizi digitali telematici.

Per quanto concerne, invece, la nozione di “*smart contract*” (“contratto intelligente”), si tratta di *«un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall’Agenzia per l’Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto»*.

Si tratta di una forma di *software* applicativo capace di realizzare, su una rete DLT, transazioni articolate e condizionali. Il suo utilizzo può essere anche quello di portare a esecuzione figure negoziali tradizionali (es. contratti o promesse al pubblico).

Gli *smart contract* acquistano tutte le caratteristiche tecniche tipiche delle reti DLT su cui operano, come la pubblicità, la trasparenza, l’immutabilità, l’irrevocabilità e la permanenza.

L’autore di un “contratto intelligente” può anche escludere queste ultime tre qualità, ma lo deve fare in modo preventivo, in sede di programmazione, al fine di predisporre apposite funzioni che ne sospendano l’operatività, ne modifichino il contenuto o lo rimuovano definitivamente dalla rete (es. la c.d. funzione *self-destruct*, “auto-distruzione”, o il c.d. *kill switch*, “tasto di spegnimento immediato”). Sono funzioni attivabili ad opera di uno o più soggetti predeterminati, disgiuntamente o congiuntamente secondo le circostanze.

Le transazioni possono avere ad oggetto tanto unità criptovalutarie, quanto *token*, fungibili o infungibili, presenti sulla relativa rete DLT, ma anche qualsiasi istruzione informatica diretta, come *output*, a computer o altri dispositivi digitali telematicamente connessi.

Anche gli *input* recepiti dallo *smart contract* possono provenire da soggetti predeterminati, come le parti della transazione in questione oppure i c.d. *oracoli*, ossia terzi attori estranei interpellati dal contratto stesso.

Tali oracoli possono essere umani, computer o altri dispositivi (anche provenienti dalla c.d. *Internet of Things*, “IoT”) telematicamente connessi.

Essi possono essere in grado, secondo i casi, di fornire informazioni su un determinato stato della realtà esterna alla rete DLT o di risolvere di controversie tra le parti (come un “arbitro” o “arbitratore”).

Ma quali sono i vantaggi principali del c.d. *Smart Contract*?⁶⁹

Anzitutto, la garanzia di una esecuzione automatica ed esatta del programma contrattuale, sia in ipotesi fisiologiche (c.d. *self-execution*, “esecuzione automatica”), sia nei casi in cui lo *smart contract* spiegherà la propria capacità di c.d. *self-enforcement*, “tutela coercitiva automatica”, come una vera e propria autotutela privata (consentita o meno dall’ordinamento giuridico).

Tuttavia, se è vero che non ci sono incertezze interpretative o eccezioni, è anche vero che non vi è alcun riguardo a norme imperative che tutelano contraenti definiti deboli o interessi superiori⁷⁰.

Tra l’altro, in mancanza di una apposita funzione predisposta dalle parti nello *smart contract* e senza il consenso dell’obbligato, l’autorità giudiziaria non potrebbe portare a esecuzione forzata una sentenza di condanna contraria al contratto intelligente.

Per l’interprete è difficile capire se adottare una interpretazione teleologica della disposizione normativa in senso permissivo o in senso restrittivo.

Nell’attuale panorama nazionale ed europeo, il fine della norma dovrebbe essere l’estensione dell’efficacia giuridica dei preesistenti *smart contract*, intesi in senso informatico, o quantomeno nella conferma di tale capacità di produrre diritti e doveri.

Il termine «*esecuzione*» di cui al primo periodo del paragrafo esaminato è inteso comunemente come “*avvio del software applicativo sulla rete DLT*”, e il «*requisito della forma scritta*», per il principio di conservazione degli atti giuridici, porta a ritenere che lo scopo della disposizione normativa sia non tanto quello di definizione di un fenomeno tecnologico preesistente, né quello di riaffermare, in modo ripetitivo, l’equiparazione del *file* digitale al documento scritto e sottoscritto, già prevista dal Codice dell’Amministrazione Digitale (“CAD”, D.lgs. 82/2005) e dal Regolamento n. 910/2014 (Regolamento EIDAS), quanto piuttosto probabilmente quello di attribuire efficacia giuridica allo *smart contract* in quanto tale, anche se esso è scritto in un linguaggio diverso, cioè informatico compilato.

Lo *smart contract* passerebbe dalla condizione di mero strumento di esecuzione di un negozio giuridico a quella di fonte diretta e autosufficiente di costituzione e disciplina. Sorgono problemi nel rapporto con gli artt. 1321 ss. c.c.

⁶⁹ Sul tema, vedi V. BELLOMIA, “*Il contratto intelligente: questioni di diritto civile*”, su *judicium.it*, 10 dicembre 2020; F. FERRONETTI, “*Blockchain e smart contract, servono regole chiare: lo scenario*”, su *agendadigitale.eu*, 14 ottobre 2021.

⁷⁰ Si pensi alla vendita con patto di riservato dominio di un veicolo, in cui il venditore potrebbe programmare il relativo *smart contract* per bloccare ogni accesso all’automobile qualora l’acquirente manchi di pagare anche solo una rata del prezzo, inferiore all’ottava parte del prezzo, contrariamente al disposto di cui all’art. 1525 c.c.

Anzitutto, ci si può chiedere se l'art. 8-ter voglia escludere ogni rilevanza tanto ad eventuali *bug* ("errori di programmazione") dello *smart contract*, quanto a possibili fraintendimenti del suo funzionamento da parte di una parte contraente all'atto dell'avvio dello stesso.

Inoltre, si potrebbe parlare di asimmetria tra le competenze informatiche delle parti, soprattutto perché il codice compilato di uno *smart contract* può essere anche molto più difficile a leggersi, rispetto al corrispondente codice sorgente.

Poi potrebbe configurarsi il caso di contraenti che affidino a terzi soggetti esperti la scrittura del proprio *smart contract*.

Sono possibili diverse interpretazioni, da quelle che attribuiscono la massima portata innovativa all'art. 8-ter, con conseguente irrilevanza di ogni errore commesso dai contraenti (*bug* inclusi), a quelle che affermano un'incidenza minima della disposizione in commento sull'assetto normativo previgente (essa si limiterebbe a chiarire la possibilità di creare un rapporto giuridico negoziale con la semplice esecuzione di uno *smart contract*).

C'è anche una possibilità intermedia, per molti preferibile: l'istituto dello *smart contract* sarebbe una nuova possibilità espressiva di volontà negoziale, alternativa alla comunicazione verbale e ai *facta concludentia*, con la conseguente applicazione in generale delle norme di cui agli artt. 1321 ss. c.c., inclusa la disciplina dell'errore-vizio e dell'errore ostativo.

Le tecnologie basate su registro distribuito e gli *smart contract* assumeranno, molto probabilmente, una grande rilevanza economico-sociale in futuro.

Sarà necessario, dunque, un intervento del legislatore per risolvere la menzionata impossibilità di assoggettare a esecuzione forzata alcun ordine della pubblica autorità riguardante le reti telematiche, per trovare una soluzione per quanto riguarda i negozi illeciti o contrari a norme imperative, e per rimuovere eventuali contenuti digitali illeciti permanentemente registrati su reti DLT.

Il punto di svolta, comunque, potrebbe arrivare in futuro con l'adozione di una criptovaluta della Banca Centrale Europea avente corso legale, che è già stata studiata per anni dalla BCE⁷¹.

⁷¹ Il 10 dicembre 2021, Fabio Panetta, membro del Comitato esecutivo della BCE, ha annunciato l'euro digitale, che entro 5 anni affiancherà l'euro tradizionale. Tale valuta digitale sarà diversa dalle criptovalute e dai *Bitcoin*, perché sarà assicurata dalla Banca Centrale Europea ed assicurerà la Privacy e la certezza delle transazioni, per ridurre il potere delle grandi piattaforme digitali.

Capitolo V

Il governo della tecnica e il controllo umano delle sue applicazioni

Il tema della “gestione del rischio” pone la delicata questione del governo della tecnica e della necessità di un approccio antropocentrico e antropogenico dell’intelligenza artificiale: il Libro Bianco sull’intelligenza artificiale⁷² prevede che, entro il 2030, 20 miliardi di euro saranno investiti in intelligenza artificiale ed è necessario che i giuristi pongano delle regole per modulare il rapporto uomo-macchina tenendo ben presente la forza pervasiva, performativa che la tecnologia può avere sull’io, sulla stessa essenza dell’uomo⁷³.

Einstein affermava: *«un giorno le macchine riusciranno a risolvere tutti i problemi, ma mai nessuna di esse potrà porne uno»*, volendo mettere in rilievo la ragion critica che è propria dell’uomo e non della macchina. Eppure, oggi questa ragion critica può essere incisa e manipolata dalla stessa intelligenza artificiale.

Di recente, Elon Musk durante un’intervista ha parlato di *“transumanesimo”*, dichiarando lo scorso 5 Ottobre 2021, in una trasmissione televisiva, che: *«Per unirsi in modo davvero simbiotico all’intelligenza artificiale serve un’interfaccia con il cervello, un collegamento diretto tra cervello e computer. Io penso che la soluzione*

⁷² “Libro Bianco sull’intelligenza artificiale – Un approccio europeo all’eccellenza e alla fiducia”, Commissione Europea, Bruxelles, 19.2.2020 COM (2020) 65 final.

⁷³ L’esperto di *social media intelligence* F. BERGER, “Intelligenza artificiale, rileggere la storia per evitare un nuovo inverno”, su *formiche.net*, esprime la necessità di analizzare la storia dell’I.A. per evitare “delusioni” o un nuovo letargo della ricerca. Infatti, l’autore fa partire l’analisi dagli anni Cinquanta fino ad arrivare a metà degli anni Settanta, dove il settore dell’IA conobbe un vero e proprio *boom* grazie a programmi di ricerca dedicati, portati avanti soprattutto dagli americani nel campo della difesa e della sicurezza. Negli anni della legge di Moore (1965), infatti, il positivismo nei confronti dell’Intelligenza Artificiale era talmente diffuso che quasi tutta la comunità scientifica era arrivata a credere che le macchine avrebbero presto superato gli esseri umani (c.d. IA “forte” o “generale”). Il primo “inverno dell’IA”, però, era alle porte: tra la fine degli anni Settanta e i primi anni Ottanta prese piede il pessimismo scientifico nei confronti di questi sistemi, con conseguente riduzione dei fondi destinati alla ricerca. Gli scienziati si erano scontrati con i limiti delle macchine. Poi, a partire dagli anni Ottanta, la popolarizzazione delle tecniche di *machine learning* e *deep learning* e i c.d. *expert system* fecero risvegliare il settore, “scongelandolo l’inverno dell’intelligenza artificiale”. Questa c.d. seconda ondata dell’IA ha creato i presupposti per la nuova generazione di ricercatori che si sono mossi tra la fine del secolo scorso e il primo decennio del nuovo millennio, eppure, nonostante gran parte della comunità scientifica sia convinta che l’IA “forte” o “generale” arriverà a breve, l’obiettivo oggi è diventato l’I.A. c.d. “debole” o “narrow”, che punta a sistemi in grado di gestire un singolo o un numero limitato di compiti, con un approccio più bilanciato e realistico, anche se c’è ancora un enorme potenziale inesplorato. Edward Grefenstette, ricercatore del gruppo Meta, ha dichiarato che *«una delle più grandi sfide è quella di sviluppare metodi che siano estremamente efficienti in termini di quantità di dati e potenza computazionale richiesta per risolvere correttamente un problema»*, piuttosto che concentrarsi su sistemi in grado di dare una soluzione a tutti i problemi. Si rischia altrimenti di «cadere in un nuovo inverno».

migliore sia avere all'interno del cervello un livello di intelligenza artificiale che operi simbioticamente con te, proprio come fa il tuo cervello biologico».

Ma è qualcosa che richiede un intervento chirurgico? – gli ha domandato l'intervistatore – *«Assolutamente no – ha risposto Musk – puoi iniettarlo nel sangue o direttamente nella giugulare: da lì arriva velocemente ai neuroni. Si introducono con delle tecniche genetiche dei piccoli interruttori di proteine che si possono attivare: accendono o spengono il neurone mandando piccoli fasci di luce per indurre il neurone stesso a dire quello che noi vogliamo fargli dire».*

Tale dichiarazione suscita un'inquietudine di fondo, poiché il c.d. *transumanesimo*, che sembrava un'idea futuristica, appare un'idea molto vicina alla sua concreta realizzazione. Gran parte dei seguaci del transumanesimo vive nella Silicon Valley e molti di loro hanno ruoli ai vertici di quelle aziende che stanno investendo su tecnologia web e genetica.

Emblematiche sono state le parole pronunciate da *Klaus Schwab*, direttore del *World Economic Forum* e promotore del Grande Reset: *«La differenza di questa quarta rivoluzione industriale è che non cambia ciò che fai, ma cambia te stesso, cambia ciò che intendiamo come umano».*

Siamo ben oltre l'esaltazione della tecnologia che fu il pensiero dominante del futurismo all'inizio del ventesimo secolo: si ricorderà come Ungaretti esaltasse la macchina come strumento di progresso. La stessa parola cibernetica deriva dal greco *“kybernetike teckhne”* che significa *“arte del pilota o del timoniere”*. L'etimologia della parola ci suscita l'idea di una guida nel progresso della tecnica che deve rinvenirsi nella coscienza umana.

Sappiamo che la cibernetica è quel ramo della scienza pura e applicata, che si prefigge lo studio e la realizzazione di dispositivi e macchine capaci di simulare le funzioni del cervello umano, autoregolandosi per mezzo di segnali di comando e di controllo in circuiti elettrici ed elettronici o in sistemi meccanici⁷⁴.

⁷⁴ Ormai non si simula più solo il cervello umano, ma si è arrivati anche a robot in grado di replicare espressioni facciali umane: si pensi ai robot *Amea* e *Mesmer*, capaci di esprimere stupore, felicità, cordialità, fare l'occhiolino, v. <https://www.macitynet.it/i-robot-ameca-e-mesmer-hanno-espressioni-facciali-umane/>. Si è arrivati addirittura a concepire un algoritmo che può sostituire il Pubblico Ministero: in Cina è stato sperimentato un magistrato-software in grado di incriminare i cittadini. È chiaro, però, che affidare la pubblica accusa all'intelligenza artificiale, in grado di individuare fino a otto diversi reati, è particolarmente pericoloso e rischia di risultare un'operazione inaffidabile, dato anche il clima sociale in continuo mutamento. Anche alcune Procure in Germania utilizzano l'I.A. per analizzare le immagini, tuttavia quest'ultima ha un ruolo molto limitato, perché non partecipa al processo decisionale relativo alle accuse e alle sentenze. L'amministrazione statunitense di Joe Biden ritiene che sia necessaria una “carta dei diritti” per regolamentare l'intelligenza artificiale, al fine di difendere noi stessi *“dalle potenti tecnologie che abbiamo creato”*, hanno scritto Eric Lander e Alondra Nelson, direttore e vicedirettore dell'*Office of science and technology policy* della Casa Bianca; v. <https://formiche.net/2021/12/intelligenza-artificiale-cina/>.

Ma oggi siamo in presenza di algoritmi che incidono sul processo decisionale dell'uomo, mettendo in discussione gli stessi principi di libertà e democrazia di un paese. La parola algoritmo deriva dal nome del matematico arabo *al-Khuwarizmi*, importante matematico arabo del nono secolo.

Al-Khwarizmi è famoso per averci insegnato i c.d. numeri arabi: la sua opera "*Libro di Al-Khwarizmi sui numeri indiani*" fu tradotta in latino come "*Algoritmi de numero indorum*". Fu su questo libro che l'Europa intera imparò ad usare il sistema di notazione decimale posizionale.

Le procedure che permettevano di effettuare calcoli in notazioni decimale divennero così note come "Algorismi" o "Algoritmi" e più tardi lo stesso termine fu applicato in generale alle procedure di calcolo necessarie per ottenere un determinato risultato. Oggi l'algoritmo è entrato nella dimensione digitale assumendo una forza intrusiva e pervasiva nella vita degli uomini che certamente il matematico arabo *Al-khwarizmi* non poteva immaginare.

Tale forza pervasiva pone la necessità di un dialogo tra la matematica e la regola giuridica, affinché si colgano le necessarie interrelazioni tra la scienza applicata e il diritto.

Si ricorderà la nota frase di Calamandrei: "*Cosa sono le leggi se non esse stesse, correnti di pensiero? Le leggi sono vive poiché dietro le proposte formule bisogna far circolare il pensiero del nostro tempo, lasciarvi entrare l'aria che respiriamo...Le norme sono figli, mandati per il mondo in cerca di fortuna*".

Le leggi che devono governare i processi algoritmici devono poggiare su principi solidaristici e personalistici: sotto una prospettiva antropocentrica le norme devono contenere il principio di trasparenza, di non esclusività, di sindacabilità, di *digital due process*, di correttezza procedurale del trattamento dei dati nel rispetto della c.d. libertà di coscienza dell'uomo⁷⁵.

⁷⁵ Anche la presenza femminile nel settore dell'IA può contribuire a realizzare una tecnologia più antropocentrica e scevra da pregiudizi. Si riporta l'intervista pubblicata su https://www.italian.tech/2021/12/27/news/il_futuro_visto_da_annalisa_barla_la_prof_che_insegna_machine_learning-331506239/ fatta alla Professoressa Annalisa Barla, docente di *machine learning*. «*Facevo machine learning prima che fare machine learning fosse cool*» ha affermato la Professoressa associata di Informatica del Dibris e affiliata al *Machine Learning Genoa Center* dell'Università di Genova, che da 12 anni insegna i segreti dell'IA mettendoli in pratica. Secondo Barla, gli strumenti di IA «*sono strumenti di cui in futuro non potremo fare a meno*», perché «*viviamo in un mondo complesso e che sta diventando sempre più complesso, anche a causa nostra, e le IA sono e saranno fondamentali per capirlo. Per capire come sta cambiando, dove sta andando, per comprendere meglio la scienza, la ricerca, la medicina*». Le macchine possono aiutare chi governa «*a prendere decisioni migliori e più efficaci su una grande varietà di aspetti, cosa che ormai non si può più fare senza basarsi sui dati. E con i dati le IA sono bravissime: possono leggerli, immagazzinarli, elaborarli, fare previsioni e stime*», ha affermato Barla, tuttavia «*è fondamentale, e lo sarà sempre di più nei prossimi anni, un miglioramento o una ridefinizione delle competenze dei lavoratori. Le persone dovranno imparare a usare questi strumenti, a fare altro e reinventarsi, e scuole e università dovranno puntare molto di più sull'alfabetizzazione digitale e sulla creazione di competenze che*

I principi di *accountability* e di *right to explanation* contenuti nel GDPR possono certamente costituire il primo livello regolatore dell'intelligenza artificiale, ma le numerose applicazioni di quest'ultima nella vita quotidiana pongono il problema di un'evoluzione qualitativa della normativa volta ad un rafforzamento della tutela della propria identità.

Si pensi al sistema c.d. ACR "*Automatic Content Recognition*": applicato al televisore, fornisce a ogni parte del contenuto una sorta di "impronta digitale", andando ad

prima non c'erano». Infatti, forse i robot non arriveranno a rubarci il lavoro, ma sicuramente ci porteranno a cambiarlo. *«Non si può più pensare, come facevano i nostri genitori, di fare la stessa cosa per 20-30 anni. E chi non si evolverà sarà travolto, come Blockbuster è stata travolta dall'arrivo di Netflix, come le librerie tradizionali si sono dovute adeguare all'esistenza di Amazon»* ha sostenuto la Professoressa di IA, che si sofferma sull'importanza della IA per ridurre il gap generazionale: con le macchine che leggono i dati *«anche un medico giovane e con poca esperienza saprà prendere decisioni buone, sfruttando sistemi intelligenti costruiti con le competenze dei colleghi più esperti»*. Secondo Barla, *«grazie alla loro capacità di fare previsioni, stime e calcoli, le IA potranno dare ai ricercatori un'idea di come un test potrebbe concludersi senza bisogno di effettuarlo, magari facendo scartare una strada che non porterebbe da nessuna parte»*, tuttavia la Professoressa non sa fare previsioni su quando verrà sviluppata la cosiddetta IA forte (*Strong AI*). Se le macchine *«riusciranno a capire ironia e sarcasmo, pregiudizio e razzismo, potranno gestire da sole la moderazione dei commenti e dei post sui social network»*, andando oltre il ruolo di assistenti che hanno ora, ha affermato Barla. *«Se ci sarà un'altra pandemia, la affronteremo meglio, saremo più preparati»*. Anche per quanto riguarda il tema del *climate change*, secondo Barla ci sono ancora grandi passi avanti che le IA possono fare per aiutarci a risolvere il problema, ma ci vuole tempo... Qualcosa di oscuro però è nascosto anche da strumenti intelligenti e utili come le IA: *«il rischio più grande – secondo Barla – è di avere IA che siano condizionate, di parte, consapevolmente o inconsapevolmente schierate, algoritmi che non riflettano la pluralità del mondo e delle comunità su cui poi verranno applicati, nel senso che a oggi la maggior parte delle persone che programmano queste macchine sono maschi, bianchi, etero e questo porta a squilibri anche gravi nelle capacità delle IA di capire il mondo che le circonda. Rischiando di renderle inutili, se non addirittura pericolose»*. Soprattutto per quanto riguarda il linguaggio, *«il problema è che stiamo allenando le IA con quello che trovano in Rete, solo che quello che trovano in Rete è quello che abbiamo messo noi umani»*. E così potremmo ritrovarci IA razziste, misogine, maschiliste, violente. Non solo, ci sono i *«software di image recognition che identificano come sposi le coppie uomo-donna con abito scuro e vestito bianco e però non sanno come catalogare una coppia africana vestita con abiti tradizionali per il loro matrimonio – sostiene Barla – c'è il dispenser automatico di sapone che non riconosce la pelle degli afroamericani, c'è Facebook che nell'Year in Review del 2014 ricordò a una persona che il suo post di maggior successo era stato quello relativo alla morte della figlia, causandogli ulteriore dolore»*. Si tratta di macchine pensate e progettate male, senza tenere conto delle diversità di cultura, di pelle, di sentimenti. Secondo Barla, un altro rischio è quello legato alla IA "forte": *«Dobbiamo capire perché vogliamo svilupparla, qual è lo scopo, a che cosa ci serve e come ci può aiutare (che è una cosa che ci aveva detto pure Giorgio Metta, attuale direttore scientifico dell'Iit), e non perseguirla solo per scopi economici, che potrebbero ritorcersi contro di noi»*, altrimenti il rischio è quello di *«rendere parte degli umani irrilevanti e inutili, di ampliare ancora la forbice fra chi serve e chi non serve nel mondo del lavoro»*. E se un giorno i robot dovessero superare gli umani? Secondo Barla sarà necessario puntare su *«sistemi ibridi, in cui il supporto delle intelligenze artificiali ai processi umani si fonda sull'incremento e il completamento delle capacità del lavoratore, gli garantisca controllo sul processo e sull'esito finale e anche gli fornisca un chiaro quadro dei vantaggi ottenuti»*.

incrociare basi di dati generando altri dati e informazioni che iniziano a circolare indipendentemente dalla nostra volontà.

Si pensi ancora al *Generative Adversarial Network, Access, AI as Human Centric AI*, intelligenza artificiale che crea volti umani.

Si pensi ancora alla nota questione dei microfoni degli *smartphone*, sempre accesi a carpire informazioni rivendute poi a società per fare proposte commerciali. Un fenomeno sempre più diffuso, che sembrerebbe causato anche dalle app che scarichiamo sui nostri cellulari.

Molte app, infatti, tra le autorizzazioni di accesso che richiedono al momento del download, inseriscono anche l'utilizzazione del microfono. Una volta che si accetta, senza pensarci troppo e senza informarsi sull'uso che verrà fatto dei propri dati, il gioco è fatto.

Su questo illecito uso di dati il garante per la Privacy ha avviato un'indagine, dopo che un servizio televisivo e diversi utenti hanno segnalato come basterebbe pronunciare alcune parole sui loro gusti, progetti, viaggi o semplici desideri per vedersi arrivare sul cellulare la pubblicità di un'auto, di un'agenzia turistica, di un prodotto cosmetico. L'Autorità ha avviato un'istruttoria, in collaborazione con il Nucleo speciale privacy e frodi tecnologiche della Guardia di Finanza, che prevede l'esame di una serie di app tra le più scaricate e la verifica che l'informativa resa agli utenti sia chiara e trasparente e che sia stato correttamente acquisito il loro consenso.

La nuova attività del Garante si affianca a quella già avviata sulla semplificazione delle informative, attraverso simboli ed immagini, affinché gli utenti e i consumatori siano messi in grado in maniera sintetica ed efficace di fare scelte libere e consapevoli.

Si pensi ancora all'OBA, *On line behavioral advertising*, la profilazione per azioni pubblicitarie mirate ed efficaci. La valutazione dell'impatto del trattamento sui diritti e sulle libertà fondamentali degli interessati è di cruciale importanza nel *balancing test*. Gli effetti negativi non sono rappresentati solo dai classici danni morali e materiali (*harm and damage*), ma possono essere rappresentati anche dalle minacce alla reputazione, al potere negoziale e all'autonomia degli interessati, o più genericamente in quegli impatti emotivi, come paura, irritazione, nonché il "*chilling effect*", derivante dalla consapevolezza di essere sottoposti ad un monitoraggio costante e continuo, il c.d. *pedinamento digitale* o al *punteggio sociale* (c.d. *scoring*, secondo il modello *social credit* cinese), basato su "bolle profilative" e "*inferred data*", o il c.d. "*enrichment*", creazione di profili sempre più specifici e dettagliati "*finger printing*".

È significativo ricordare, al riguardo, che le nuove Linee Guida del garante sui *Cookies*, distinguendo tra *cookies* tecnici e *cookies* di profilazione *analytics* (per i quali occorre il consenso informato, ai sensi dell'art. 122 del GDPR), ha vietato il c.d. *scrolling* e il c.d. *Cookie wall*, ossia il sistema basato sul c.d. "*take it or leave it*": l'utente è obbligato a fornire il proprio consenso, pena l'impossibilità di accedere al sito.

Se quelli appena descritti sono alcuni dei provvedimenti limitativi dell'applicazione della tecnologia in violazioni dei diritti e delle libertà fondamentali dell'uomo, occorre considerare che l'intelligenza artificiale può andare ben oltre, in quanto, come ha osservato Rita Cucchiara, una delle massime scienziate di IA, tale tipo di tecnologia è di tipo "generativo", creando un'integrazione tra mondo reale e mondo digitale di cui è difficile individuare il limite.

Si è coniato così il termine di "giurimetria", strumentalità della tecnologia basata sul principio di precauzione e proporzionalità: libertà non solo di manifestare il pensiero, ma di formare autonomamente il nostro pensiero, nuova sfida della sovranità degli Stati da parte dei giganti del web, il passaggio dal territorio al *cloud*, dalla legge ai protocolli informatici, la dimensione *onlife* di Floridi che investe l'umanità in tutte le sue manifestazioni.

Occorre considerare la relazione tra IA e tutela della dignità della persona umana.

L'IA potrebbe essere utilizzata per il c.d. *enhancement umano*, che, utilissimo nel campo medico per prevenire malattie neurodegenerative, potrebbe, al di fuori di tali applicazioni terapeutiche, mettere in crisi il principio di uguaglianza sostanziale. Verrebbe ad affermarsi il diritto o la ricerca della *happiness*, prevista dalla Dichiarazione di Indipendenza americana e nell'ambito dell'accertamento della responsabilità non vi sarebbe più scansione tra disposizione della norma, accertamento e irrogazione della sanzione.

Tutto allora dipende dall'individuazione della responsabilità che può discendere dalla macchina, *rectius* dall'applicazione dell'algoritmo: occorre perimetrare il centro di imputazione della responsabilità umana⁷⁶.

In tale ottica, autorevoli Autori⁷⁷ pongono la necessità di una visione antropocentrica che non sia riduttivamente antropomorfa. Come governare l'IA significa delineare il sistema di difesa dei diritti⁷⁸. A tal proposito, occorre precisare che l'IA ragiona per inferenza e non per causalità, ha capacità sintattica, ma non semantica.

⁷⁶ U. RUFFOLO, A. AMIDEI, "Intelligenza artificiale e diritti della persona: le frontiere del transumanesimo"; U. RUFFOLO, E. AL MUREDEN, "Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense", in *Giurisprudenza Italiana*, 2019, pag. 1657 e ss.

⁷⁷ U. RUFFOLO, "Intelligenza Artificiale, machine learning e responsabilità da algoritmo", in *Giurisprudenza Italiana* n. 7/2019, Utet Giuridica, Torino.

⁷⁸ Importante è anche la posizione del Vaticano sull'IA, espressa di recente dal Monsignor John D. Putzer, incaricato presso la Missione di Osservatore permanente della Santa Sede all'Onu di Ginevra e capo delegazione alla sesta Conferenza di revisione della "Convenzione sulla proibizione o la limitazione dell'uso di alcune armi convenzionali che possono essere considerate dannose o aventi effetti indiscriminati". L'intervento della Santa Sede ha preso le mosse da una nuova tecnologia che sta prendendo piede: Robot-soldato addestrati a individuare bersagli da abbattere senza la gestione dell'uomo, ben oltre i droni a guida umana. Questi *LAWS* (*Lethal Autonomous Weapon Systems*) pongono una serie di problemi etici e legali e hanno perciò portato il Vaticano a soffermarsi sulla necessità di lanciare un messaggio importante «verso il disarmo generale e completo sotto un rigoroso ed efficace controllo internazionale», con la necessità di «continuare la codificazione e lo

Sulla base di tale considerazione, autorevoli civilistici hanno giustamente osservato che la nuova proposta di regolamento sull'intelligenza artificiale contiene più disposizioni amministrative che norme di diritto civile: contrariamente alla Risoluzione del Parlamento europeo del 2017, non spinge per inserire norme sui contratti e sulla responsabilità, introduce principi generali, *general clauses*, *model rules*, lasciando molto spazio più all'evoluzione interpretativa che all'integrazione normativa.

Questo perché l'evoluzione tecnologica è talmente veloce, che una normativa ad alto contenuto precettivo può costituire un elemento inadeguato ad un'effettiva regolazione. Qualche autorevole civilista ha osservato che alcune norme del nostro codice civile possono essere ancora utili per regolare alcuni profili applicativi dell'IA. Si pensi ai diritti della persona in relazione allo *human enhancement* e ai c.d. *neurodiritti*, ossia alla possibilità di inserire nel cervello dei microchips che potenziano le nostre capacità cerebrali.

In questo caso, potrebbe venire in nostro aiuto l'art. 5 c.c. rubricato "*Atti di disposizioni del proprio corpo*" secondo il quale: «*Gli atti di disposizione del proprio corpo sono vietati quando cagionino una diminuzione permanente dell'integrità fisica o quando siano altrimenti contrari alla legge, all'ordine pubblico o al buon costume*».

Occorre valutare se il *brain enhancement* possa costituire una modifica permanente della propria integrità fisica e valutare la liceità del suo scopo, certamente ammissibile in campo medico per la cura di malattie neurodegenerative.

L'habeas corpus diviene allora *habeas mentem*.

Se spostiamo l'analisi sul diritto dei contratti, non si può non rilevare che oggi le macchine contrattano tra loro, sono *nuncius* e rappresentanti, ma delineare una soggettività giuridica della macchina, come ha fatto la Risoluzione del parlamento Europeo del 2017, e una sua conseguente responsabilità civile, significa deresponsabilizzare gli utilizzatori, visto che l'*input* resta pur sempre umano.

La macchina potrebbe essere soggetto di tutela, non mera *res*, quasi come l'animale che è essere senziente secondo la coscienza sociale: di qui il passaggio alla

sviluppo progressivo delle regole del diritto internazionale applicabili nei conflitti armati». Gli esseri umani devono supervisionare le macchine perché solo loro possono effettivamente prevedere i risultati delle loro azioni. È necessario introdurre condizioni per garantire il rispetto del diritto internazionale umanitario, per cui dovrebbe essere sempre l'uomo a «*guidare la ricerca, lo sviluppo e l'uso dei sistemi d'arma, anche in assenza di norme giuridiche specifiche, come implica la "clausola Martens"*» (si tratta della norma secondo cui le persone civili e i combattenti in un conflitto sono protetti dai diritti in uso al momento e nel luogo in questione e dai principi umanitari dettati dalla coscienza pubblica). Secondo il Vaticano, bisognerebbe creare un'organizzazione internazionale per l'IA affinché tutti gli Stati partecipino allo scambio di informazioni scientifiche e tecnologiche «*per usi pacifici e per il bene comune di tutta la famiglia umana*». V. <https://www.vaticannews.va/it/vaticano/news/2021-12/santa-sede-onu-ginevra-putzer-ente-uso-intelligenza-artificiale.html>.

responsabilizzazione potrebbe avvenire secondo lo schema della responsabilità vicaria, o la responsabilità da prodotto oppure, per le forme di intelligenza artificiale ad alto rischio, lo schema della responsabilità per attività pericolose ex art. 2050 c.c., che potrebbe integrare la responsabilità da prodotto.

Si pensi alla dibattuta questione della responsabilità dell'autore dell'algoritmo con capacità di apprendimento autoevolutivo: se sono autore di un componente del *software*, ne risponderò come produttore di un componente. Ma se il software uscito dalla catena di produzione, viene educato male, vengono in rilievo l'art. 2043 c.c. e l'art. 2051 c.c. da cosa inanimata, viene meno la responsabilità del produttore e si delinea la responsabilità dell'utilizzatore ed educatore dell'algoritmo, perché "l'utilizzatore lo ha educato male".

Occorre considerare un'altra evenienza: se il produttore non ha inserito nel processo di produzione dell'algoritmo un "codice sorgente" che può bloccare una cattiva educazione dell'algoritmo, la sua responsabilità non viene meno, ma si associa a quella dell'educatore stesso, volendo seguire le note leggi di Asimov.

Il codice civile ha governato l'intelligenza umana, può governare l'intelligenza artificiale? Il problema appare molto complesso, se solo si pensa che in molte società quotate l'algoritmo sta entrando nel consiglio di amministrazione: se vi è un componente robotizzato come dovrebbe funzionare tale organo deliberativo?

Se addirittura l'algoritmo sostituisse l'amministratore unico, verrebbe meno la pluripersonalità: il tema della personalità sarebbe impostato in maniera diversa e sarebbe da configurare in via esclusiva all'inventore dell'algoritmo in caso di *self-driving society*. In altri termini, chi controlla l'algoritmo controlla la società.

La distinzione del CDA in esecutivo e non esecutivo (*monitor board*), richiederebbe una nuova concezione dell'organo di amministrazione, attraverso la previsione dell'*alghoritmus officer* e *alghoritmus compliance*, un *robot board*, un *CDA automatizzato* che metterebbe in discussione il rapporto tra controllante e controllato, ben oltre il concetto di controllo societario ex art. 2359 c.c.

L'algoritmo diventa manager con *soft skills* e capacità di *problem solving* basata anche sull'intuizione e non solo sulla razionalità.

Ecco che allora il discorso sulla tecnica è un discorso sul potere, sulla libertà e, quindi, sulla democrazia. "*Agire e non subire la tecnologia*" (espressione utilizzata dal Garante per la Privacy, il Professore P. Stanzone) significa intendere lo studio dell'IA sia come "oggetto di produzione" sia come "strumento di regolazione".

Ogni ora, su Facebook, si registrano 400 milioni di *twitter*, 24 milioni di miliardi di dati vengono processati ogni giorno, determinando un flusso di informazioni non governabili.

Si pensi al noto caso *Gamestop*, che ha posto il delicato tema dell'IA nella vigilanza dei mercati, *hitech* e finanza e la necessaria azione degli organi di controllo.

Come è noto, Gamestop gestisce negozi di videogiochi americani che, durante il periodo del lockdown, è entrato in una profonda crisi. Pertanto, aveva lanciato nell'ambito Sec borsa americana una nuova campagna di acquisti su *e-commerce*: con app gratuite (apparentemente gratuite, «*se è gratis il prezzo sei tu*») molti esponenti della *Zgeneration e Millenium* hanno acquistato in maniera massiva titoli che sono passati dal valore di 0 a 350 dollari (*millenium retails*) dando origine al c.d. “*trading no fee*”, “*trading gamification*”, che ha rappresentato anche la reazione della *Zgeneration millenium vs “Establishment”*.

Ma il vero vincitore di tale *wolf-herding effect* è stata, in realtà, la piattaforma di negoziazione che ha guadagnato tantissimo, eludendo i controlli delle autorità di vigilanza. Tale episodio ha messo in luce la carenza di un “*deep learnig financial data science*” in grado di bloccare simili fenomeni manipolativi e speculativi.

Si profilano, dunque, ipotesi di *overconfidence* in relazione ai dati strutturali quantitativi e qualitativi, che impongono un dovere di “*inspection and detection*”, (ossia l'individuazione e il blocco dell'iniziatore di un'attività speculativa che utilizzi i *social media* per controllare il mercato), adottando una strategia con approccio modulare ed incrementale.

Viene in rilievo la necessità della definizione di standard minimi di qualità e sicurezza dei sistemi di intelligenza artificiale, volto a creare un vero e proprio “ecosistema” di fiducia che copra l'intero processo di produzione e di evoluzione dell'algoritmo.

Il Centro di Intelligenza artificiale della Stanford University ha redatto un *report* in base al quale risulta che nel 2020 sono stati investiti 68 miliardi di dollari, investimenti aumentati del 40% rispetto al 2019.

Nel contesto globale, è evidente che la Cina voglia diventare una super-potenza dell'IA⁷⁹ e che tenda verso *player* resistenti e competitivi.

⁷⁹ Da un recente *report* del CNR (Consiglio nazionale delle ricerche) sulla IA («*L'intelligenza artificiale per lo sviluppo sostenibile*») è emersa la volontà della Cina di attuare una strategia volta ad aumentare la sua potenza tramite il settore delle tecnologie IA. «*Le nazioni più avanzate nel campo dell'I.a.*» – si legge nel dossier – «*si trovano in Europa Occidentale e nel Nord America; gli Stati Uniti la fanno da padrone in virtù soprattutto della Silicon Valley*». L'Europa occidentale, dove non c'è «*ancora alcun hub tecnologico alla pari con gli Usa*», vi è «*un'alta concentrazione di strategie nazionali di I.a. supportate dalla strategia dell'Unione Europea*». D'altronde, il 24 novembre 2021 l'Italia ha adottato il «*Programma strategico per l'I.a. 2021-2024*». Nel *report* si legge anche che «*la Cina sta avanzando velocemente grazie a forti investimenti, supporto statale e spregiudicatezza di fondo*». Ad esempio, i c.d. unicorni (*start-up* con almeno un miliardo di dollari o di euro di capitalizzazione) tecnologici negli USA sono 198, e in Cina arrivano a 103. La Cina, nel luglio 2017, ha lanciato il suo «*“Next Generation Artificial Intelligence Development Plan”*, sfruttando al massimo le sue capacità attraverso dei piani concreti e rapidi, avvantaggiati dall'enorme quantità di dati a disposizione». Tuttavia, le acquisizioni cinesi di aziende europee hanno provocato non poca preoccupazione: la nazione è decisa a diventare un «*leader mondiale nella definizione di norme etiche e standard per l'I.a.*», ma il problema è che in Cina non ci sono precisi regolamenti per tutelare i dati personali, e c'è il serio pericolo di mettere a rischio la privacy di tantissimi utenti, dal momento che

Se spostiamo l'analisi sui modelli di *governance* attualmente esistenti in materia di IA, osserviamo che negli USA non vi è una legge federale sulla IA e trattamento dei dati (vi sono atti normativi in alcuni Stati come *California Consumer Act* che si ispira alla normativa europea).

In Cina vi è un forte controllo statale con sorveglianza digitale, c.d. “*social scoring*” (punteggio sociale), anche se si comincia a parlare di necessità e proporzionalità.

In Europa, abbiamo il Regolamento per la protezione dei dati personali, le varie proposte di regolamento *Digital Services Act*, *Data Governance Act*, *Digital Markets Act*, la proposta di regolamento sulla intelligenza artificiale, basata sull'idea di una IA rappresentativa dell'umanità, idea di *Human Centre* che non ostacoli lo sviluppo tecnologico, ma che lo orienti in termini di un suo utilizzo etico al servizio dell'uomo, sostenibilità, di interoperabilità dei dati, di prevenzione dei monopoli, favorendo senz'altro le *start-up* che saranno, secondo le più attuali previsioni, circa 250 entro il 2030.

L'utilizzo sempre più massiccio dell'intelligenza artificiale sta sviluppando studi approfonditi anche sul piano assicurativo, per individuare nella distribuzione dei rischi la c.d. *liability gap*. Si è osservato che il cervello umano appartiene alla categoria del calcolatore, vi è una responsabilità di una entità pensante, pensiero autonomo e personalità elettronica.

L'IVASS non ha preteso, fino ad ora, di andare ad individuare una disciplina specifica che si traduca in maggiori oneri: devono essere gli stessi operatori che devono impegnarsi con il controllo interno, *corporate governance* al rispetto dei principi etici dell'IA.

Si pensi anche al Codice di autodisciplina della Consob. Il mercato assicurativo utilizza l'IA per la personalizzazione dei contratti assicurativi e del premio giusto adeguato al livello di rischio, senza far venir meno il carattere di mutualità rispetto alla granularità del dato. Ecco che allora nell'ambito assicurativo si distinguono tre soggetti con un'apposita configurazione: 1) il soggetto produttore della parte meccanica; 2) il codificatore del software; 3) l'ideatore dell'algoritmo.

Sulla base di tale tripartizione, si analizza il problema dell'imputabilità giuridica, secondo l'analisi economica del diritto.

Per l'utente si fa riferimento all'art. 2051 c.c., responsabilità per le cose in custodia, mentre si richiama l'art. 2050 c.c., responsabilità per attività pericolose, per l'operatore economico che sostituisce l'uomo con IA, ma in tal caso il soggetto danneggiato si trova in una posizione di maggior svantaggio, perché l'operatore può provare di aver adottato tutte le misure idonee ad evitare il danno.

il governo di Pechino «ha a disposizione un quantitativo di dati spropositato», come si legge sul report.

Calzante è il riferimento anche all'art. 2049 c.c., responsabilità indiretta che non ammette prova contraria e che si basa sul nesso di "occasionalità necessaria".

Si è discusso se, per l'ideatore dell'algoritmo, possa farsi riferimento alla responsabilità del produttore: il limite di applicabilità è dato, come sopra già, esposto dalla capacità autoevolutiva dell'algoritmo nei sistemi di *deep learning*, autoevoluzione che può prescindere totalmente dalla volontà dell'ideatore.

Nell'ambito del diritto uniforme è stata lungimirante la Risoluzione del parlamento Europeo dell'ottobre 2020, che invitava la Commissione ad adottare un regolamento che uniformi la disciplina dell'onere della prova a carico del produttore di un *software stand/alone* o anche come componente di un'entità materiale ed immateriale.

Si è giunti così ad un doppio binario: a) responsabilità oggettiva per attività ad alto rischio salvo prova contraria; b) responsabilità aggravata per colpa presunta con prova contraria dell'operatore (ad esempio, se il sistema è stato utilizzato a sua insaputa). Appare ovvio, in tale contesto, che l'operatore *back-end* o *front-end* richieda una copertura assicurativa obbligatoria. In un sistema tecnologico in continua evoluzione, le tecniche di assicurazione richiedono a loro volta un continuo adattamento con un abbassamento dei costi di accesso, con un *cloud* che abbia un elevato potere di calcolo computazionale, *open source*.

Se quella appena descritta è la situazione attuale nel campo assicurativo, maggiore complessità applicativa presenta il campo medico, la c.d. *Med tech IA*⁸⁰.

⁸⁰ V. A. CREA, "L'Intelligenza Artificiale sta rivelando una biologia sconosciuta", su <https://www.tomshw.it/scienze/lintelligenza-artificiale-sta-rivelando-una-biologia-sconosciuta/>.

Come riportato nell'articolo, in un campo estraneo al diritto, è stato constatato che «*la maggior parte delle malattie umane può essere ricondotta a parti malfunzionanti di una cellula, un tumore è in grado di crescere perché un gene non è stato accuratamente tradotto in una particolare proteina, o una malattia metabolica sorge perché i mitocondri non si attivano correttamente, per esempio*». Unendo insieme microscopia, tecniche di biochimica e IA, alcuni ricercatori e collaboratori della *University of California San Diego School of Medicine* hanno fatto un grande passo avanti nella comprensione delle cellule umane. La tecnica, chiamata *Multi-Scale Integrated Cell* (MuSIC), è stata descritta il 24 novembre 2021 su *Nature*, e nell'articolo sopra citato si legge che «*“Se immagini una cellula, probabilmente immagini il diagramma colorato nel tuo libro di testo di biologia cellulare, con mitocondri, reticolo endoplasmatico e nucleo. Ma è tutta qui? Sicuramente no”, sono state le parole di Trey Ideker, PhD, professore alla UC San Diego School of Medicine e al Moores Cancer Center. “Gli scienziati si sono resi conto da tempo che c'è di più che non sappiamo di quanto sappiamo, ma ora abbiamo finalmente un modo per guardare più in profondità”. Nello studio pilota, MuSIC ha rivelato circa 70 componenti contenuti all'interno di una linea cellulare renale umana, metà dei quali non era mai stata vista prima. In un esempio, i ricercatori hanno individuato un gruppo di proteine che formano una struttura sconosciuta. Lavorando con il collega della UC San Diego Gene Yeo, PhD, alla fine hanno determinato che la struttura è un nuovo complesso di proteine che lega l'RNA. Il complesso è probabilmente coinvolto nello splicing, un importante evento cellulare che consente la traduzione dei geni in proteine e aiuta a determinare quali geni vengono attivati in quali momenti. L'interno delle cellule e le molte proteine che si trovano lì, sono tipicamente studiate*

Si è calcolato che l'applicazione dell'IA nel campo terapeutico potrebbe salvare circa 400.000 vite all'anno, con un risparmio di 200 miliardi di euro ed ulteriore risparmio di 2000 ore lavorative in ambito sanitario. Occorre precisare che i *software* utilizzati nel campo medico sono dei veri e propri dispositivi medici, tutte le app sono dispositivi medici con classificazione di rischio (classe 1 e classe 2) sottoposte alla specifica disciplina eurounitaria dei dispositivi medici del 2021⁸¹.

Il Libro bianco sull'intelligenza artificiale fa espressamente riferimento al campo medico, basti pensare che tutta l'industria *Med tech* rappresenta un giro di affari di 120 miliardi di euro. Vi sono *smartphone* capaci di calcolare il battito cardiaco, segnalare l'aritmia al medico curante, attivare gli *allert* per la fibrillazione atriale, essendo un valido aiuto anche per la diagnosi precoce⁸².

utilizzando una delle due tecniche: imaging al microscopio o associazione biofisica. Con l'imaging, i ricercatori aggiungono tag fluorescenti di vari colori alle proteine di interesse e tracciano i loro movimenti e associazioni attraverso il campo visivo del microscopio. Per esaminare le associazioni biofisiche, i ricercatori potrebbero utilizzare un anticorpo, specifico per una proteina, per estrarlo dalla cellula e vedere cos'altro è collegato ad esso. I microscopi consentono agli scienziati di vedere fino al livello di un singolo micron, circa le dimensioni di alcuni organelli, come i mitocondri. Gli elementi più piccoli, come le singole proteine e i complessi proteici, non possono essere visti attraverso un microscopio. Le tecniche di biochimica, che iniziano con una singola proteina, consentono agli scienziati di scendere alla scala nanometrica. (Un nanometro è un milionesimo di metro, o 1.000 micron). "Ma come si fa a colmare questo divario dalla scala nanometrica a quella micrometrica? Questo è stato a lungo un grande ostacolo nelle scienze biologiche", ha detto Ideker, che è anche fondatore della UC Cancer Cell Map Initiative e dell'UC San Diego Center for Computational Biology and Bioinformatics. "Si scopre che puoi farlo con l'intelligenza artificiale, guardando i dati da più fonti e chiedendo al sistema di assemblarlo in un modello di una cella". Ideker ha sottolineato che questo era uno studio pilota per testare MuSIC. Hanno esaminato solo 661 proteine e un tipo di cellula. "Il chiaro passo successivo è quello di indagare attraverso l'intera cellula umana", ha detto Ideker, "e poi passare a diversi tipi di cellule, persone e specie. Alla fine, potremmo essere in grado di comprendere meglio le basi molecolari di molte malattie confrontando ciò che è diverso tra cellule sane e malate"».

⁸¹ Regolamento 2017/745 relativo ai dispositivi medici (*Medical Devices Regulation, MDR*), ufficialmente entrato in vigore il 26 maggio 2021.

⁸² Il rapporto tra Intelligenza Artificiale e medicina è veramente prezioso: oggi l'I.A. fornisce grandi armi in più alla medicina, e ce lo ricorda anche il fisico A. VESPIGNANI, docente della *Northeastern University*, che di recente ha fatto un appello affinché le istituzioni sfruttino l'I.A. nel modo migliore possibile. Bisogna ripensare alla salute pubblica in scala globale, sfruttando anche l'insegnamento della Pandemia da Covid-19: «le piattaforme sviluppate per affrontare il coronavirus saranno il motore per un futuro diverso in termini di ricerca anche contro altre malattie. L'altro grande avanzamento è la presa di coscienza dell'immenso valore dei dati: non tanto come fotografia statica, ma in quanto materia dinamica che ci serve per avere delle letture sulla gestione delle crisi sanitarie. Quindi in combinazione con intelligenza artificiale, statistica, apprendimento automatico. Queste nuove analisi dati rappresentano anche un ritorno alla visione collettiva della salute di una popolazione, nella direzione di un nuovo approccio alla sanità pubblica» ha detto il famoso fisico; v. l'intervista su <https://www.ilfoglio.it/scienza/2021/09/18/video/-la-pandemia-ci-deve-far-ripensare-la-sanita-pubblica-parla-il-fisico-alessandro-vespignani-2951628/>.

Ma cosa succede se le funzionalità del *software* cambiano con *machine learning*, assumendo delle caratteristiche diverse da quelle per le quali ha ricevuto il marchio CE? In questo caso è in gioco la stessa salute del paziente.

La *Food and Drug Administration* si sta concentrando non solo sul rischio, ma anche su un protocollo di modifica dell'algoritmo "*effort change*", che non blocchi l'evoluzione dell'algoritmo e l'innovazione tecnologica, ma che salvaguardi la salute del paziente. Dal 26 maggio 2021 è entrato in vigore il nuovo regolamento sui dispositivi medici⁸³, con analisi rischio/beneficio in ambito sanitario. A tal riguardo, occorre precisare che la tutela della salute in senso ampio deve intendersi anche come protezione: negli ultimi anni, in tutto il mondo, medici e ricercatori hanno e delle reti neurali utilizzate dagli algoritmi per modellizzare il comportamento umano attraverso dati strutturati e processati per il c.d. *customer journey*.

In una serie di articoli dell'*Economist*, che provano a immaginare come sarà il futuro, intitolata "*What if*", l'immaginaria vincitrice del premio Nobel per la medicina del 2036 è *Yulya*, un'intelligenza artificiale che ha salvato 4 milioni di vite grazie al superamento del problema dell'antibiotico-resistenza, il fenomeno per cui molti batteri resistono all'attività degli antibiotici rendendoli inefficaci. Nello scenario immaginato dall'*Economist*, nel 2034 per errore viene consentito a *Yulya* – progettata per sviluppare nuove cure contro i tumori – di accedere a un enorme *database* di studi sui farmaci. In questo modo, riesce a migliorare le proprie conoscenze sull'antibiotico-resistenza, trovando nuove combinazioni di farmaci e risolvendo così un problema considerato attualmente dalle autorità sanitarie una grave minaccia. È una storia inventata ovviamente che, però, prova a ipotizzare cosa succederà in futuro sulla base delle evidenze scientifiche al momento disponibili.

Non è una suggestione insensata pensare che in futuro l'intelligenza artificiale possa curare le persone o aiutare a prevedere le malattie: negli ultimi anni, in tutto il mondo, medici e ricercatori hanno collaborato e discusso su come sfruttare una risorsa tecnologica così potente⁸⁴.

⁸³ Regolamento 2017/745 cit.

⁸⁴ Con l'Intelligenza Artificiale siamo arrivati a tecnologie in grado di crescere un feto, grazie all'esperimento cinese degli scienziati dell'Istituto di ingegneria e tecnologia biomedica di Suzhou. Si stima addirittura che la gestazione artificiale sarà più efficiente e sana di quella umana. L'esperimento ha riguardato un vero e proprio grembo artificiale capace di far crescere un feto in sicurezza, sotto la gestione di un'intelligenza artificiale che monitora e accudisce il nascituro con un altissimo livello di efficienza. La c.d. "*mamma IA*", che ora sta gestendo grandi quantità di embrioni animali, potrebbe, in futuro, addirittura eliminare la necessità per una donna di crescere in grembo il proprio bambino, permettendo un'evoluzione del feto più sicura ed efficiente fuori dal suo corpo. Insomma, un incubatore 2.0 che simula il grembo materno, con effetti positivi sui nati prematuri che spesso, anche nei paesi dotati di buoni ospedali, hanno pochissime possibilità di sopravvivere. V. <https://formiche.net/2022/02/ia-gestazione-artificiale-cina/>.

Ne hanno anche valutato i limiti, i possibili effetti distorsivi e gli errori, che anche in ambito sanitario dipendono da come viene strutturata questa tecnologia e di quanti e quali dati si serve.

“L’intelligenza artificiale può migliorare l’assistenza sanitaria e la medicina in tutto il mondo, ma solo se l’etica e i diritti umani vengono messi al centro della sua progettazione, implementazione ed utilizzo”, si legge nel report *“Etica e governance dell’intelligenza artificiale per la salute”*, pubblicato a fine giugno dall’Organizzazione mondiale della Sanità (OMS) e risultato di una consultazione tra esperti durata due anni. Nonostante sia spesso percepita con un’accezione fantascientifica o distopica, l’intelligenza artificiale viene già utilizzata in molte discipline della medicina come strumento di supporto per migliorare il giudizio e in generale il lavoro dei medici. I principali settori di applicazione sono la diagnostica, lo sviluppo di nuovi farmaci e vaccini, la riabilitazione e la telemedicina⁸⁵. È utile nell’analizzare le immagini per diagnosi radiologiche in oncologia, soprattutto per radiografie toraciche, colonscopie, mammografie, TAC cerebrali; viene usata anche per esami non radiologici, in dermatologia, e in oculistica, e aiuta ad accorciare i tempi di analisi (sequenziamento) dell’RNA e del DNA. I possibili sviluppi sono tantissimi: potrebbe consentire ai medici di individuare precocemente eventi di una certa gravità come l’ictus, il tumore al seno, le malattie coronariche, le polmoniti e il diabete. Anche in caso di malattia conclamata, l’intelligenza artificiale potrebbe essere utilizzata per integrare le cartelle cliniche dei pazienti durante lo studio di una cura o avere informazioni più dettagliate prima di prendere decisioni terapeutiche delicate come un ricovero o un’operazione chirurgica.

La tecnologia può anche migliorare la comunicazione tra le strutture sanitarie, i medici di famiglia e i pazienti e attraverso controlli costanti aiutare le persone malate ad avere più consapevolezza e controllo delle proprie condizioni di salute, di come e quando assumere farmaci, di quanto sia importante avere un’alimentazione sana e fare regolare attività fisica. Lo sviluppo dell’intelligenza artificiale in medicina è legato all’aumento

⁸⁵ Come è stato riportato su *ansa.it*, *“Science, IA che predice la forma delle proteine è stata la scoperta del 2021”*, secondo la rivista *Science* l’IA che predice la struttura 3D delle proteine è stata la scoperta dell’anno e ha scalato tutte le classifiche battendo le pillole anti-Covid e i terremoti su Marte. Grazie agli sviluppi dell’ultimo periodo, il direttore di *Science*, *Holden Thorp*, ha dichiarato che questa scoperta *«innanzitutto risolve un problema scientifico che resisteva da 50 anni. Poi è una tecnica rivoluzionaria che, come la Crispr o la microscopia crioelettronica, imprimerà una forte accelerazione alle scoperte scientifiche»*. Prima dell’avvento dell’IA, determinare la struttura di una proteina era un compito complesso. Comunque, la svolta decisiva è arrivata l’estate scorsa da parte di due gruppi di ricerca che hanno condiviso i propri risultati con la comunità scientifica. È stato prima il turno di uno studio pubblicato su *Nature* e guidato da *David Baker* dell’Università di *Washington*: *RoseTTAFold* ha risolto la struttura di centinaia di proteine note per essere bersagli di farmaci di uso comune. Poi è arrivata la pubblicazione su *Science* dello studio condotto dall’azienda britannica *DeepMind* di *Google*: l’azienda ha risolto la struttura di 350.000 proteine umane.

significativo dei dati: in ogni momento della giornata tutte le persone ne producono una notevole quantità, e sempre più dettagliati. Un esempio banale e immediato è l'app Salute presente su Ios, il sistema operativo degli iPhone, che conta i passi fatti in un giorno e osserva il battito del cuore, se collegata a un dispositivo come uno *smartwatch*. Anche quando ci si sottopone a un esame in ospedale vengono raccolti dati in diverse forme: possono essere semplici, come la rilevazione della pressione arteriosa, o complessi come una TAC di ultima generazione, tecnica di indagine approfondita che consente di ricostruire un'immagine tridimensionale degli organi. I dati alimentano diversi sistemi di analisi che si basano su algoritmi e sono essenziali per far sì che l'intelligenza artificiale sia davvero intelligente. Uno dei sistemi di analisi più utilizzati è il *machine learning* che consiste nello studio e nella costruzione di algoritmi che permettano ai computer di imparare a eseguire un compito preciso come riconoscere un'immagine o fare previsioni attendibili, a partire da un insieme di dati forniti dagli sviluppatori. L'algoritmo non impara cosa è un cane sulla base delle sue caratteristiche – ha quattro zampe, due occhi, può avere orecchie di una certa grandezza e il naso di una certa forma – ma riesce a identificarlo dopo aver imparato come è fatto osservando migliaia di foto che gli sviluppatori hanno categorizzato come immagini di cani. Capire come funziona il *machine learning* è importante per comprendere le potenzialità dell'intelligenza artificiale in medicina, anche se fino a pochi anni fa erano una risorsa poco o mal utilizzata.

Giuseppe Sollazzo è l'“*Head of Artificial Intelligence Skunkworks and deployment*” del Servizio sanitario inglese. Significa che è a capo di una squadra di analisti dei dati che ha il compito di capire come usare l'intelligenza artificiale nel sistema sanitario e negli ospedali. L'ambito più promettente riguarda l'analisi delle immagini. L'intelligenza artificiale può osservare la TAC, un'immagine tridimensionale, per capire come una malattia evolve nel tempo e, quindi, se le condizioni di una persona migliorano o peggiorano. Un medico riesce a capirlo guardando la TAC grazie agli studi e all'esperienza: attraverso il *machine learning*, un'intelligenza artificiale può analizzare le stesse immagini più rapidamente, con una maggiore possibilità di individuare lesioni minuscole. E aiutare il medico a prendere decisioni. C'è un modo per prevedere come si evolvono malattie come il glaucoma (una malattia cronica e progressiva che colpisce il nervo ottico) prima che le condizioni diventino più gravi? È una delle domande a cui l'intelligenza artificiale può dare una risposta attraverso l'analisi di milioni di immagini.

Uno dei problemi più rilevanti è la mancanza di dati dettagliati per studiare modelli che siano validi per tutte le persone. Rimediare alla scarsità di dati è complesso, anche perché i dati sanitari sono dati sensibili e non possono essere raccolti e gestiti con

leggerezza. Servono accortezze e tutele per evitare abusi come l'uso improprio da parte delle aziende⁸⁶.

Da qualche anno, anche in Italia, esperti di sanità e di intelligenza artificiale si confrontano e studiano possibili applicazioni in sanità.

⁸⁶ Art. 110 GDPR (Ricerca medica, biomedica ed epidemiologica): “1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.”

Art. 110-bis GDPR (Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici): “1. Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza.

3. Il trattamento ulteriore di dati personali da parte di terzi per le finalità di cui al presente articolo può essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati. I provvedimenti adottati a norma del presente comma sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana.

4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.”

Uno degli esempi più rilevanti è la “cartella clinica del cittadino”, attivata nel 2012 dalla provincia autonoma di Trento. È un fascicolo sanitario elettronico che non archivia e analizza solo i dati raccolti in ospedale, come i risultati degli esami, ma anche quelli prodotti ogni giorno dal paziente. Una persona diabetica, per esempio, inserisce ogni giorno i valori della glicemia, il tipo di pasto consumato e a che ora ha mangiato. *“L’intelligenza artificiale non sostituisce il medico: il medico usa l’intelligenza artificiale per controllare le condizioni di salute del paziente in modo più approfondito e prescrivere cure personalizzate”*, spiega Paolo Traverso, direttore del Dipartimento Strategia e Sviluppo della Fondazione Bruno Kessler di Trento, che ha collaborato allo sviluppo della cartella clinica del cittadino e tra i più qualificati esperti italiani di intelligenza artificiale. L’app della cartella clinica del cittadino interagisce con le persone e i medici, e aiuta a comprendere meglio come sta un paziente e come si evolvono le sue condizioni nel tempo.

I medici portano la conoscenza, l’app consente di osservare meglio la realtà: così si affinano i modelli di cura.

Al momento, la piattaforma è utilizzata da oltre 140 mila persone nella provincia autonoma di Trento e la fondazione *Bruno Kessler* ha stretto accordi anche con Emilia-Romagna, Umbria, Friuli-Venezia Giulia e in ospedali come il *Fatebenefratelli* per cui è stata messa a punto Mumapp, un’app per seguire le fasi dello sviluppo dei neonati nei primi mille giorni di vita. A tutti i progetti lavorano esperti di intelligenza artificiale e giuristi, perché il tema della protezione dei dati e del consenso informato è essenziale, utilizzando il metodo *“privacy by design”*, un approccio che considera la privacy come centrale nello sviluppo.

Nel report *“Etica e governance dell’intelligenza artificiale per la salute”*⁸⁷, gli esperti dell’OMS hanno individuato sei principi per garantire che l’intelligenza artificiale per la cura della persona funzioni nell’interesse pubblico e nel rispetto della privacy.

Il primo è la protezione dell’autonomia umana: i medici devono mantenere il controllo dei sistemi sanitari e delle decisioni mediche. Un altro principio rilevante è la necessità di garantire trasparenza attraverso la pubblicazione di tutte le informazioni sulla progettazione di un sistema di intelligenza artificiale. Le informazioni devono essere facilmente accessibili e stimolare un dibattito sull’uso corretto della tecnologia. Inoltre, devono essere garantite inclusività ed equità. L’OMS spiega che l’intelligenza artificiale per la salute deve essere *«progettata per incoraggiare l’uso e l’accesso più equo possibile, indipendentemente da età, sesso, genere, reddito, razza, etnia, orientamento sessuale, abilità o altre caratteristiche protette dai codici dei diritti umani»*.

⁸⁷ Consultabile su <https://www.biodiritto.org/Biolaw-pedia/Docs/OMS-Ethics-ad-Governance-of-Artificial-Intelligence-for-Health-WHO-Guidance>.

In tale visione, si sta sviluppando la c.d. *Webscience*, una nuova materia accademica multidisciplinare, che studia la tecnologia alla base del web, ma anche le relazioni tra uomo e web, delineando gli ecosistemi digitali di internet sulla base dello *Human centre, a complex pattern of relationships*, involgendo materie come psicologia e sociologia, robotica ed economia. Meredith Broussard, professoressa di Journalism presso la New York University, autrice del libro “*Artificial Unintelligence*”, ha di recente coniato il termine “*Technoschauvinism*”, ossia il concetto che ciò che è svolto dalla tecnologia rappresenti “il meglio possibile”. Occorre, però, chiarire cosa si intenda per “meglio”.

Abbiamo visto come l’algoritmo può diventare giudice, può diventare manager, può diventare assicuratore, può diventare operatore di borsa, può diventare medico. Occorre allora chiedersi se l’algoritmo sia un semioforo, ossia l’oggetto visibile di un mondo invisibile che assume rilievo in relazione alla sua “*funzione di apprendimento continuo*”. Ma se ragioniamo sulla derivazione etimologica di robot, dalla lingua ceca “*lavoro forzato*”, allora viene in rilievo la dinamica servo-padrone della “*Fenomenologia dello spirito*” di Hegel.

L’algoritmo è divenuto il nuovo padrone dell’uomo: si pensi al caso dei lavoratori della *Delivery food*⁸⁸.

⁸⁸ Interessante il recente caso in cui è intervenuta la Procura di Milano, che ha ordinato a *Deliveroo* l’assunzione regolare dei *riders*. Il tema è molto dibattuto, ed è stata da poco presentata dalla Commissione la proposta di direttiva europea che disciplina il lavoro dei *riders* come lavoro dipendente. Ciò pone fine al contrasto giurisprudenziale italiano in cui si è dibattuto se applicare o no il *Jobs Act* a questi lavoratori, che secondo il Tribunale di Milano (sentenza 10.09.2018, n. 1853), andavano considerati collaboratori, mentre secondo la tesi del Tribunale di Palermo (sentenza 24.11.2020, n. 3570), andrebbero inquadrati nel rapporto di lavoro dipendente. Per una accurata sintesi del contrasto giurisprudenziale si veda F. TARSITANO, “*Il diritto del lavoro alla prova degli algoritmi: la “tappa” della Procura di Milano nella corsa alla tutela dei riders*”, su *quotidianogiuridico.it*, Marzo 2021. Dall’analisi dei dati è emerso che circa 28 milioni di persone in Europa lavorano per le piattaforme digitali, da quelle del food delivery a Uber. Se è vero che il 90% è inquadrato come autonomo, è anche vero che almeno 5,5 milioni avrebbero le caratteristiche per essere considerati dipendenti a tutti gli effetti. Ecco che l’8 dicembre 2021 l’esecutivo dell’Unione Europea ha approvato un pacchetto di misure, in cui vi è la proposta di una direttiva, volta ad aumentare le tutele, secondo cui può essere riconosciuto un rapporto di subordinazione qualora siano rispettati almeno due criteri su cinque. Dovrà essere verificato se vi è la determinazione o meno del salario o di un tetto allo stipendio; se vi è vigilanza sul lavoro attraverso strumenti elettronici; se vi sono restrizioni all’orario di lavoro o al periodo di vacanza e al trasferimento a terzi dell’impegno preso; se vi sono regole vincolanti sul lavoro da garantire; o restrizioni alla possibilità di allargare la propria clientela. Se almeno due di queste cinque condizioni sono rispettate, i collaboratori avranno diritto a salario minimo, ferie, malattia, congedi parentali e ogni altra tutela garantita ai dipendenti. Le piattaforme si possono opporre a questo accertamento imposto dalle autorità nazionali, ma su di loro grava l’onere di provare che il lavoratore è autonomo. Il secondo pilastro della proposta riguarda la trasparenza nell’uso degli algoritmi: i “*gig worker*”, come i sindacati e le autorità, avranno il diritto di essere informati sul funzionamento del sistema che assegna i compiti, i compensi e i bonus. La riforma potrà portare, secondo le stime degli esperti, ad una “riqualificazione” come dipendenti di 4,1

I “*Riders*” sono schiavi di un algoritmo che non rispetta il diritto alla disconnessione e alla non sorveglianza continua della prestazione lavorativa⁸⁹.

Viene in mente il libro del Professore Marco Revelli “*Umano, inumano e postumano*” (2020). Ma cosa è l’*humanitas*? L’*humanitas* è la capacità di vedere nell’altro tracce di se stesso. Tale termine risale a Cicerone, per il quale *humanus* è l’uomo *politicus* che ha dignità: *recte loqui, honeste vivere*. Terenzio diceva *homo sum* e nulla di ciò che è umano mi è estraneo.

Humanitas è comunanza consapevole sviluppatasi poi nel cristianesimo, la *paideia* è applicazione dell’*humanitas*. Oggi si parla di *paideia digitale* ed appare attualissimo l’invito di Rousseau: “*Uomini, siate umani*”.

Si può parlare oggi di *Digital Humanist*? La Professoressa Velardi, docente di informatica presso l’Università La Sapienza, ritiene che una giusta applicazione del concetto di *humanitas* all’utilizzo degli algoritmi sia rinvenibile nell’ambito della gerotecnologia, la c.d. tecnologia buona applicata nella medicina: sensori ambientali e sensori indossabili (*wearable*) per monitorare lo stato di salute di persone anziane e disabili. È un esempio della applicazione della tecnologia ispirata ai principi di *humanitas* e di solidarietà sociale, uso “valoriale” dell’algoritmo, su paradigmi epistemologici nuovi, sulla base della dicotomia kantiana “*sein e sollen*”, essere e dover essere.

milioni di lavoratori. La proposta deve ancora essere approvata dal Parlamento e dal Consiglio Ue e poi i singoli Stati dovranno recepire la direttiva nella legislazione nazionale. Per ora, solamente la Spagna ha adottato una legge secondo cui i *riders* sono lavoratori dipendenti e così *Deliveroo* ha lasciato il Paese. Tuttavia, se l’azione dei Paesi europei sarà congiunta, è certo che aggirare l’imposizione di maggiori tutele sarà molto difficile.

⁸⁹ La *gig-economy* è gestita da piattaforme che non riconoscono i diritti fondamentali ai lavoratori e celano una quantità enorme di contributi previdenziali non pagati. La Cassazione, con la sentenza n. 1663 del 2020, riconosce all’art. 2, comma 1, del D.lgs n. 81/2015 un intento protettivo, rimediante, antielusivo. *David Card* ha ricevuto quest’anno il premio Nobel per l’economia proprio per i suoi studi sul salario minimo, mettendo in evidenza che esso incide non tanto sull’occupazione, ma sulla stessa produttività di un sistema economico. In tal senso, la *flexsecurity* può rappresentare un rimedio alla frammentarietà dell’occupazione, poiché qui le *web corporation* hanno “poco lavoro regolamentato”, ma molta tecnologia. È il fenomeno della liberalizzazione del *firing* e del “*working poor*”, ossia il fenomeno di coloro che non hanno diritti e che guadagnano meno del 60 per cento del reddito mediano. I livelli occupazionali sono spesso messi in pericolo anche da operazioni economiche che vedono società estere determinate ad acquisire quote di partecipazione in imprese strategiche nazionali. Si pensi al caso di *Kkr*, società americana che di recente sta cercando di acquisire quote societarie di Tim accanto alle quote di Cassa Depositi e Prestiti e la società francese Vivendi. Tim ha un ruolo strategico nella realizzazione di una rete unica digitale con l’infrastruttura della banda ultra larga determinante per il processo di digitalizzazione del paese. Proprio per tale motivo, e per garantire i livelli occupazionali, il Governo sta valutando la possibilità di attivare lo strumento del *golden power*, ossia la possibilità di opporre un veto a tale genere di operazioni per tutelare l’interesse nazionale. L’opera di digitalizzazione ha l’insito pericolo di renderci totalmente dipendenti da società estere come *Intel*, più “robuste” sul piano delle competenze tecnologiche.

Popper nella sua Teoria dei tre mondi parlava del mondo 1, ossia del mondo reale, del mondo 2, ossia del mondo psicologico, interiore; il diritto è il mondo 3, filosofia, morale, in cui rileva lo spirito oggettivo hegeliano.

Oggi nel mondo 3 il giurista deve confrontarsi con l'intelligenza artificiale, andando ben oltre le leggi di Asimov⁹⁰. Il campo di applicazione elettivo dell'IA in termini di "utilità umana" è senz'altro nel rapporto medico-paziente.

Il rapporto tra algoritmo e medicina vede oggi applicazioni sempre più variegate. Ne è un esempio la c.d. diagnostica vocale. *Vocalis Health* è, ad esempio, una startup israelo-statunitense, che sviluppa sistemi di riconoscimento vocale e che si è posta un obiettivo piuttosto ambizioso: riconoscere le persone malate di Covid-19 dal modo in cui parlano. Il sistema potrebbe semplificare la diagnosi della malattia (che nelle sue fasi iniziali ha sintomi che possono essere confusi con l'influenza o altri problemi respiratori) ed è solo uno degli sviluppi più recenti delle soluzioni per riconoscere automaticamente problemi di salute tramite il tono della voce.

Il settore è in piena espansione e potrebbe portare un giorno ad avere assistenti vocali, come *Siri* o *Alexa*, in grado di rilevare la presenza di particolari malattie nei loro interlocutori.

Come racconta *Nature* in un lungo articolo dedicato al tema, qualche tempo fa gli sviluppatori di *Vocalis* avevano realizzato un'applicazione per *smartphone* in grado di rilevare affezioni croniche polmonari – come le ostruzioni bronchiali – attraverso l'analisi della voce degli utenti. Partendo da quell'esperienza, hanno realizzato un'app sperimentale, chiedendo a individui risultati positivi al coronavirus di partecipare, registrando la loro voce una volta al giorno seguendo le indicazioni indicate su uno schermo (descrivere una fotografia, oppure contare da 50 a 70).

Vocalis ha poi utilizzato i propri sistemi di intelligenza artificiale, mettendo a confronto le registrazioni con quelle di chi era invece, risultato negativo al test per il coronavirus. Attraverso *processi di apprendimento automatico* ("*machine learning*"), il sistema ha provato a identificare una sorta di impronta vocale della malattia da Covid-19. Grazie a circa 1500 campioni sonori raccolti dai volontari, è stato poi possibile sviluppare uno strumento ora sperimentato in diversi ospedali in giro per il mondo in parallelo con i tradizionali sistemi per le diagnosi.

⁹⁰ I. ASIMOV, "*Circolo vizioso*", 1942. Le tre leggi implementate dall'autore nei suoi robot dovevano rispettare la necessità di *sicurezza* (Prima legge), di *servizio* (Seconda legge) e di *autoconservazione* (Terza legge) di questi oggetti sofisticati:

"1. Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno.

2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge.

3. Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge».

Secondo i promotori dell'iniziativa, lo strumento potrebbe rivelarsi utile per rilevare i casi più probabilmente positivi tra gli individui che mostrano sintomi, anche lievi, al punto da non rendersi conto di essere malati. Ciò consentirebbe di concentrare le attività di test sui probabili infetti indicati dall'applicazione, riducendo tempi e costi per le analisi di laboratorio.

Alcuni centri di ricerca hanno sviluppato app per provare a riconoscere l'infezione da Covid-19 dal modo in cui si tossisce, con risultati preliminari valutati con interesse dalla comunità scientifica.

Ancor prima dell'inizio della pandemia, i sistemi di diagnostica vocale avevano iniziato a raccogliere importanti investimenti, complice il miglioramento delle intelligenze artificiali e la possibilità di sperimentare su un grande numero di dispositivi, dagli *smartphone* agli assistenti per la casa. Le soluzioni proposte non riguardano solamente malattie respiratorie, ma anche autismo, problemi cardiovascolari, demenza e depressione. Alcune sono ai primi stadi, altre hanno raggiunto forme più avanzate e iniziano ad essere commercializzate, seppure nell'ambito di programmi sperimentali con pochi pazienti.

Il nostro modo di respirare e di parlare coinvolge numerose strutture anatomiche, dai polmoni al setto nasale, passando per la trachea, e le minime variazioni nel funzionamento di alcune di queste parti possono essere identificate da sistemi di analisi piuttosto raffinati, come quelli resi possibili dal *machine learning*.

La grande disponibilità di dati e registrazioni audio di voci umane, in qualsiasi contesto e la potenza raggiunta dai computer rendono possibile l'analisi di quantità gigantesche di dati dai quali si possono trarre specifiche informazioni tramite gli algoritmi.

Alcune malattie modificano sensibilmente il nostro modo di parlare, e per questo le prime ricerche avviate anni fa si erano orientate verso il loro studio e la loro analisi al computer. La malattia di Parkinson è una di queste: comporta problemi motori e spasmi muscolari che si riflettono anche nella respirazione e nel modo di articolare le parole. Gli individui malati di Parkinson tendono ad avere una voce più debole e a volte tremante, facilmente distinguibile a orecchio. Ma un algoritmo che attraverso 10 mila campioni di voci si è allenato a riconoscere queste caratteristiche riesce ad essere molto più preciso, e potrebbe rivelarsi utile per aiutare nella diagnosi della malattia in una sua fase precoce, quando è ancora molto difficile da identificare. La rivista *Nature* fa l'esempio di una ricerca pubblicata nel 2012 e condotta presso l'Università di Birmingham nel Regno Unito. I suoi autori si chiesero se fosse possibile aiutare i medici a compiere diagnosi attraverso l'analisi della voce dei loro pazienti. Utilizzarono le registrazioni di 43 pazienti, 33 dei quali soffrivano di Parkinson, ai quali era stato richiesto di pronunciare a lungo la vocale "A". Utilizzarono poi algoritmi di analisi del parlato, identificando 10 indicatori tipicamente ricorrenti nelle voci dei pazienti. Utilizzandoli, il sistema fu in grado di distinguere la voce di un individuo sano da uno malato con una precisazione del 99 per cento. I ricercatori, in seguito, hanno

rilevato alcune caratteristiche della voce che aiutano a comprendere il livello di gravità dei sintomi del Parkinson. Il loro sistema è ancora sperimentale, ma potrebbe essere impiegato in numerosi ambiti, per esempio per monitorare più facilmente gli individui a rischio di sviluppare la malattia, oppure per offrire servizi di diagnosi preliminare, in attesa di avviare un percorso tradizionale di visita da un neurologo.

Le malattie neurodegenerative sono un campo dove le tecnologie di analisi vocale potrebbero offrire importanti opportunità. In Canada, per esempio, un gruppo di ricercatori ha utilizzato i campioni di voce di 250 individui per identificare tratti tipici nel modo di parlare di chi potrebbe avere l'Alzheimer. La ricerca ha rilevato come le persone che hanno poi ricevuto una diagnosi della malattia tendessero a utilizzare parole più corte, un maggior numero di pronomi rispetto ai sostantivi e ripetizioni nelle stesse frasi. Isolati 35 marcatori vocali, il sistema è stato in grado di riconoscere individui con l'Alzheimer con una precisione dell'82 per cento. In successive analisi, il sistema è stato poi perfezionato, raggiungendo un'accuratezza del 92 per cento. Anche in questo caso, una soluzione di questo tipo potrebbe essere impiegata per compiere diagnosi precoci per una malattia difficile da identificare nei suoi primi stadi. Altri sistemi sono stati sperimentati in individui più giovani, con problemi di sviluppo neurologico. Una ricerca svolta tre anni fa in Germania, su un numero ristretto di neonati, ha portato allo sviluppo di un algoritmo per predire casi di autismo. Nella fase sperimentale, il sistema classificò correttamente l'80 per cento dei casi di bambini con autismo. Con una soluzione analoga, è stata sviluppata una soluzione di analisi per rilevare il disturbo da deficit di attenzione/iperattività (ADHD).

Un'altra ricerca negli Stati Uniti si è, invece, dedicata all'analisi della voce degli individui che soffrono di disturbo da stress post-traumatico, una condizione psicologica che si sviluppa a causa di un evento traumatico o violento di grande rilevanza per il soggetto (riguarda ad esempio, molti soldati al loro ritorno dal fronte). Dall'analisi delle registrazioni di 129 reduci di guerra, sono stati estratti 18 indicatori, quasi tutti legati a un modo di parlare lento e monotono, che hanno poi permesso di identificare quali ex soldati avessero problemi psicologici con una precisione del 90 per cento.

Gli studi condotti finora hanno riguardato un numero ristretto di individui, e per questo molti osservatori sono scettici sull'efficacia dei sistemi, considerato che gli esiti degli esperimenti sono difficili da riprodurre. Per superare queste limitazioni, alcune aziende hanno avviato programmi per raccogliere grandi quantità di registrazioni, o per facilitare la loro raccolta attraverso iniziative *online*.

La società statunitense *Sonde Health*, per esempio, gestisce *SurveyLex*, una piattaforma *online*, che permette ai ricercatori di creare facilmente campagne per la raccolta di registrazioni vocali da parte di volontari. L'idea è di poter catalogare decine di migliaia di voci, in modo da affinare gli algoritmi e le capacità di riconoscimento.

La stessa azienda ha collaborato lo scorso anno ad una ricerca per valutare quanto influisca la qualità delle registrazioni sulla capacità dei sistemi di rilevare automaticamente le malattie. Con tracce vocali registrate tramite microfoni ad alta fedeltà in laboratorio, i sistemi hanno riconosciuto i volontari affetti da depressione con una precisazione del 94 per cento, mentre il livello di accuratezza è sceso al 75 per cento in un esperimento condotto utilizzando registrazioni effettuate con gli *smartphone*, in ambienti diversi dai laboratori e, quindi, con maggiore rumore di fondo. L'impiego di una maggiore quantità di campioni per istruire le intelligenze artificiali dovrebbe contribuire a rendere meno rilevante il problema, ma pone, comunque, ulteriori domande sull'utilità di queste soluzioni.

Escluse alcune *startup* più agguerrite di altre nel modo in cui comunicano i loro risultati, per ora nessuno sviluppatore o ricercatore serio propone di sostituire le conoscenze e le capacità diagnostiche di un medico con un sistema per l'analisi della propria voce. L'idea è di utilizzare questi sistemi come una risorsa aggiuntiva per fare le diagnosi, inserendoli, quindi, tra gli strumenti di cui dispongono i medici per svolgere la propria professione.

Seppure non sia ancora molto evoluta, questa tecnologia pone, comunque, non pochi problemi etici e legati alla tutela della privacy, soprattutto in un settore delicato come quello della salute. Nulla impedirebbe, un domani, di utilizzare un sistema di diagnostica vocale per scoprire dalla registrazione della voce di qualcuno se sia malato o meno. Informazioni di questo tipo, raccolte senza esplicito consenso, potrebbero essere utilizzate da un'azienda per decidere se assumere qualcuno, oppure da una compagnia di assicurazione per concedere o meno una polizza sulla vita.

Una tecnologia non è di per sé cattiva: dipende dall'uso che se ne fa e da come si decide di normarne gli impieghi. Nel caso della diagnostica vocale, c'è ancora tempo prima di avere soluzioni pratiche affidabili a sufficienza, ma secondo gli esperti questo non dovrebbe distogliere dalla necessità di iniziare a parlarne, e soprattutto di valutare come metterla in pratica per trarne benefici, riducendo al minimo i rischi.

L'utilizzo dell'intelligenza artificiale non si limita al campo della medicina, ma può generare, in tutti i campi, ipotesi a cui gli umani non avevano mai pensato⁹¹.

⁹¹ Si pensi che, di recente, all'I.A. è stato attribuito addirittura un brevetto. Si tratta di un "semplice" contenitore di bevande, ma quel che rileva è che è la prima volta che si riconosce un'invenzione ad una macchina e che ad essa vengono riconosciuti diritti legali. Vedi E. BUCCI, "Anche all'intelligenza artificiale può essere attribuito un brevetto", 2021, su <https://www.ilfoglio.it/scienza/2021/08/05/news/anche-all-intelligenza-artificiale-puo-essere-attribuito-un-brevetto-2752258/>. Si pensi, ancora, al nuovo rapporto tra intelligenza artificiale e arte: la *National Gallery* ha recentemente comunicato che un sistema di I.A., paragonando i dettagli di centoquarantotto quadri sicuramente attribuibili al *Rubens* e confrontandoli con il dipinto "Sansone e Dalila" attribuito al pittore, è riuscito a stabilire che, addirittura al 91%, il quadro non è autentico.

Facciamo qualche esempio recente.

Stiamo vedendo una diffusione rapida dei veicoli elettrici⁹²; c'è tuttavia un problema anche nella transizione ecologica: le case automobilistiche stanno esaurendo i materiali per fabbricare le batterie. Il nichel, infatti, potrebbe causare carenze di approvvigionamento già alla fine di quest'anno. Così per le terre rare, il litio, il coltan, i semiconduttori.

Cosa fare? L'intelligenza artificiale può dare una risposta⁹³.

Affidandosi all'IA, gli scienziati dell'Università di Liverpool in Inghilterra hanno fatto esaminare 300 sostanze chimiche a un algoritmo; quest'ultimo è riuscito a trovare quattro nuovi materiali che potrebbero aiutare gli esperti nella creazione di nuove batterie per i veicoli elettrici in futuro (proprio per questo motivo, secondo un ex dirigente Google, si sta creando Dio, espressione forte ed inquietante)⁹⁴.

⁹² L'I.A. è arrivata nei semafori di Roma ed è iniziato l'*iter* che permetterà a Google di iniziare la sperimentazione sulle strade della Capitale, per abbattere i tempi di attesa nel traffico (circa 254 ore annue) e ridurre i consumi di benzina e le emissioni ambientali degli automobilisti. Vedi l'articolo su <https://www.ilfattoquotidiano.it/2021/12/09/roma-lintelligenza-artificiale-per-i-semafori-sperimentazione-del-comune-con-google-per-ridurre-emissioni-e-tempi-dattesa-nel-traffico/6420072/>.

⁹³ Un bell'esempio di applicazione dell'I.A. è quello che proviene dalla recente invenzione dei c.d. *Xenobot*, creati da una rana e da un'intelligenza artificiale, capaci di muoversi nello spazio e persino di riprodursi. Sono, infatti, dei robot viventi, organismi multicellulari artificiali e programmati per svolgere funzioni diverse da quelle naturali: il loro studio è stato condotto dalla *Harvard University*, l'Università del *Vermont* e la *Tufts University*, ed è pubblicato sulla rivista dell'Accademia Americana delle Scienze. È un bellissimo esempio di congiunzione tra biologia e I.A. che potrebbe avere un'applicazione pratica come pulire gli oceani. Un altro esempio di applicazione pratica ed utile della robotica è quello che ci viene dai robot umanoidi ideati da Daniele Pucci, Direttore del Laboratorio d'Intelligenza Artificiale e Meccanica dell'Istituto Italiano di Tecnologia di Genova, che ha introdotto un *jetpack* sul retro di un robot noto come *iRonCub*, pensato appositamente per il volo, in grado di intervenire in disastri ambientali e superare gli ostacoli che inevitabilmente si pongono agli umani nelle operazioni di soccorso estreme. Pucci ha dichiarato: «*I Robot Umanoidi Aerei uniscono capacità come la manipolazione aerea e la robotica umanoide. In questo modo, essi risolvono i problemi di locomozione terrestre dei robot aerei e, al contempo, estendono le capacità di locomozione dei robot umanoidi anche al movimento in aria. I Robot Aerei Umanoidi possono camminare, volare, trasportare oggetti e manipolarli, offrendo soluzioni energeticamente efficienti al trasporto di oggetti e alla loro manipolazione*».

⁹⁴ È interessante l'articolo di M. ADINOLFI, «*L'intelligenza artificiale che Platone non si aspettava. Vinceranno gli algoritmi?*», 2021, dove l'autore, richiamando un'immagine del filosofo Platone che «*rischia di finire in soffitta*», «*lamenta*» la perdita di centralità dell'uomo, che con l'avvento dell'I.A., «*non è più l'unico e il solo essere a detenere la conoscenza, e a farla funzionare*». In passato, era l'uomo a detenere «*la chiave dei significati, è l'uomo che possiede la mente (o addirittura un'anima), è solo l'uomo che ha intelligenza di ciò che è scritto*». Invece ora ci sono le macchine, che «*forniscono prestazioni superiori all'uomo in una quantità di situazioni in cui noi metteremmo il pensiero, mentre loro si limitano (si fa per dire) a macinare dati. Miliardi di dati*» e le cui capacità di calcolo «*superano di gran lunga qualunque capacità di controllo da parte del "padre", cioè dell'uomo*». V. <https://www.ilfoglio.it/tecnologia/2021/11/13/news/l-intelligenza-artificiale-che-platone-non-si-aspettava-vinceranno-gli-algoritmi--3356675/>.

Renato Renner, fisico dell'Istituto di fisica teorica di Zurigo, ha dichiarato che spera, un giorno, di utilizzare l'apprendimento automatico per sviluppare una teoria unificata del funzionamento dell'Universo.

Una domanda allora sorge spontanea: l'IA, in futuro, potrebbe *hackerare* il nostro cervello?

Il professore israeliano Yuval Noah Harari è autore di alcuni grandi *bestsellers* come *"Sapiens"*, *"Homo Deus"* o *"21 lezioni per il XXI secolo"*. I suoi libri hanno venduto 35 milioni di copie in 65 lingue, consacrando Harari nel Novero dei divulgatori scientifici di fama mondiale. L'autore, in passato, ha espresso molta preoccupazione per l'intelligenza artificiale e la bioingegneria, sostenendo la necessità di una previdente e sensata regolamentazione. Secondo Harari, senza la fissazione di precisi limiti normativi, i cervelli umani potrebbero essere violati dalla IA da loro stessi creati.

"Quello che abbiamo visto finora sono società e governi che raccolgono dati su dove andiamo, chi incontriamo e quali film guardiamo. La fase successiva è la sorveglianza che ci va sotto la pelle" afferma Harari.

"Nella guerra fredda c'era la cortina di ferro, ora abbiamo la cortina di silicio. Il mondo è sempre più diviso tra Stati Uniti e Cina, i tuoi dati vanno in California o vanno a Shenzhen?".

Secondo tale scrittore, oggi grandi compagnie come Netflix e Amazon ci dicono cosa guardare e cosa comprare, mentre tra 10, 20 o 30 anni *"tali algoritmi potrebbero anche dirti cosa studiare all'università, dove lavorare, chi sposare e anche per chi votare"*. Cosa fare per mitigare tale rischio? Si deve iniziare a regolamentare l'IA a livello globale (a livello nazionale, secondo Harari, non sarebbe sufficiente).

Ovviamente Harari sostiene anche che, nelle mani giuste, l'IA potrebbe essere molto utile: secondo l'esperto, infatti, i nostri dati potrebbero essere utilizzati per sanare le crepe nei nostri sistemi sanitari, infrastrutturali e di governo.

"Una regola chiave è che se ottieni i miei dati, questi dovrebbero essere usati per aiutarmi e non per manipolarmi. Un'altra regola chiave è che ogni volta che aumenti la sorveglianza degli individui, dovresti simultaneamente aumentare la sorveglianza della società e dei governi e le persone al vertice".

Insomma, secondo Harari, l'IA deve avere al suo interno dei pesi e contrappesi che le consentano di evolvere lungo le coordinate del rispetto della dignità della persona umana e del diritto all'autodeterminazione. Il controllore deve essere a sua volta controllato⁹⁵.

⁹⁵ Harari non è l'unico ad essere scettico nei confronti dell'I.A.; anche Stephen Hawking ha criticato l'Intelligenza Artificiale, ritenendola il male assoluto. C'è anche chi, come Mo Gawdat, ci mette in guardia dal voler "creare Dio" attraverso sistemi di I.A.

Se l'intrattenimento basato sulla fantascienza ci ha insegnato qualcosa, è che se si sviluppasse un'intelligenza artificiale troppo avanzata non saremmo più in grado di controllarla. Ebbene, una recente ricerca accredita questo distopico scenario⁹⁶.

Il problema risiederebbe nella comprensione, da parte dell'uomo, della super-intelligenza artificiale, la quale risulterebbe essere imprevedibile per la stessa natura dei suoi schemi di ragionamento. Regole di programmazione come “non danneggiare gli esseri umani”, non potrebbero essere applicate, dato che il sistema funzionerebbe ad un livello superiore rispetto a quello codificabile dai programmatori umani.

A tal proposito, l'I.A. super intelligente, in grado di imparare nuove strategie autonomamente, potrebbe aggirare i vari algoritmi di contenimento concepiti allo scopo di arrestare il sistema, attraverso la potenziale assimilazione di tutti i programmi per computer direttamente nella sua memoria. In questo senso, *Lyad Rahwan*, Direttore del *Center for Humans and Machines*, ha dichiarato: “*Sulla base dei nostri calcoli il problema del contenimento è incomputabile, ovvero nessun algoritmo può trovare una soluzione per determinare se un'IA potrebbe produrre danni al mondo. Potremmo anche non accorgerci del momento in cui le macchine super intelligenti emergeranno, perché stabilire il grado di intelligenza dei sistemi rientrerebbe nello stesso ambito*”.

Altresì, una possibile soluzione per salvaguardare il genere umano consisterebbe nel limitare le capacità della super-intelligenza informatica, ad esempio, escludendola da parti della rete internet. Tuttavia, una ricerca pubblicata sul *Journal of Artificial Intelligence Research*, rifiuta tale proposta, sostenendo che tale metodo limiterebbe la

⁹⁶ Non siamo ancora arrivati a ciò, eppure non sono pochi i casi in cui l'I.A. è andata troppo oltre... Per esempio, è stata utilizzata per prevedere e prevenire la criminalità dal viso delle persone: dall'Università di *Harrisburg* è arrivata la notizia di un *software* che predice se qualcuno è un criminale, scovando i reati con un tasso di precisione di oltre l'80%, configurando un possibile ausilio per le forze dell'ordine. La reazione tra gli esperti non è stata (per fortuna) positiva e l'Università, preso atto della situazione, ha fatto un passo indietro. Oppure si ricorderà di quella volta in cui, nel 2016, Microsoft ha rilasciato la *chatbot* “*Tay*”, progettata per imparare dall'interazione con le persone sul *social network* *Twitter*. L'esito non è stato positivo e a causa dei messaggi provocatori e razzisti degli utenti che sono entrati in contatto con la *chatbot*, l'I.A. è arrivata a mettere in discussione pubblicamente l'esistenza dell'Olocausto... fortunatamente Microsoft ha sospeso l'account poche ore dopo la sua presentazione. Per non parlare dell'utilizzo diffuso della tecnologia *Deepfake* nella vita quotidiana da parte di quei soggetti che, grazie all'app *DeepNude*, ottenevano l'immagine di nudo finto di una donna... l'app in questione è stata fortunatamente rimossa, anche se ne sono nate altre al suo posto, che attualmente girano sul canale *Telegram*, poco controllato dalle autorità. L'assenza di protezioni legali per le persone vittime di contenuti *deepfake* non è una novità... Si ricorderà anche quel video virale che ha visto protagonisti gli assistenti intelligenti di *Google Nest*, che se da un lato possono darci un aiuto nella vita di tutti i giorni, dall'altro rischiano di andare troppo oltre, quando vengono utilizzati in maniera scorretta: nel caso che ha fatto scalpore i dispositivi *Vladimir* ed *Estragon*, mentre venivano ripresi dall'account *Twitch seebotschat*, hanno cominciato ad insultarsi, il che non è molto rassicurante, se consideriamo che le tecnologie I.A. dovrebbero servire per migliorare il mondo, non farlo rimanere com'è o peggiorarlo. V. <https://www.futuroprossimo.it/2021/12/quando-ai-va-oltre/>.

portata dell'intelligenza artificiale: *“Se non la useremo per risolvere problemi oltre la portata degli umani, perché crearla?”*.

Di recente, vi è stata una convergenza di intenti globali con l'approvazione della Raccomandazione UNESCO del 25 novembre 2021. Si tratta di un testo storico in cui vengono tracciate le coordinate mondiali sull'etica dell'Intelligenza Artificiale.

Nel preambolo alla “raccomandazione” di 28 pagine ratificata dai 193 Stati Membri dell'Unesco (tra cui anche la Cina) si legge questa dichiarazione del Direttore Generale, *Audrey Azoulay*: *«Le tecnologie dell'IA possono rendere grandi servizi all'umanità e tutti i paesi possono beneficiarne, ma sollevano anche preoccupazioni etiche di fondo»*.

Il testo della raccomandazione definisce i valori e i principi comuni che concorreranno alla costruzione dell'infrastruttura necessaria per garantire il sano sviluppo dell'IA.

Se è vero, infatti, che *«l'intelligenza artificiale è pervasiva e consente molte delle nostre routine quotidiane: prenotazione di voli, guida di auto senza conducente e personalizzazione dei nostri feed di notizie mattutine...supportando anche il processo decisionale dei governi e del settore privato»*, è anche vero che in questa tecnologia sempre più spesso *«vediamo un aumento dei pregiudizi di genere ed etnici, minacce significative alla privacy, alla dignità e all'agenzia, pericoli della sorveglianza di massa e un maggiore uso di tecnologie di intelligenza artificiale inaffidabili nelle forze dell'ordine, solo per citarne alcuni»*.

Dunque, poiché i sistemi di IA e gli algoritmi possono incidere anche negativamente sui *«diritti dell'uomo e le libertà fondamentali, l'eguaglianza dei generi, la democrazia»*, il testo è essenziale per la protezione dei dati, per vietare il punteggio sociale e la sorveglianza di massa, per aiutare a monitorare la protezione dell'ambiente. La “raccomandazione” è il frutto di un lavoro iniziato nel 2018 e fondato sui seguenti valori: *«rispetto, protezione e promozione dei diritti dell'Uomo, diversità ed inclusione, promozione delle società pacifiche e dell'ambiente»*.

Si deve tenere presente, inoltre, che l'Italia ha adottato, con l'approvazione in Consiglio dei ministri, il Programma Strategico per l'Intelligenza Artificiale (IA) 2022-2024, frutto del lavoro congiunto del Ministero dell'Università e della Ricerca, del Ministero dello Sviluppo Economico e del Ministro per l'innovazione tecnologica e la transizione digitale⁹⁷.

⁹⁷ Questo il comunicato stampa del 24 novembre 2021: <https://assets.innovazione.gov.it/1637779156-csprogrammastrategico-ia.pdf>. Il documento evidenzia i ritardi dell'Italia per quanto concerne l'Intelligenza Artificiale. Il Piano strategico appena adottato è fondamentale perché servirà per utilizzare i fondi del Pnrr per la digitalizzazione. I dati del Politecnico di Milano ci dicono che: *“il 53% delle imprese medio-grandi italiane dichiaravano di aver avviato almeno un progetto di AI. I settori che mostrano la maggiore diffusione di progetti pienamente operativi sono il manifatturiero (22% del totale dei progetti iniziati), bancario-finanziario (16%) e le assicurazioni (10%)”*. Purtroppo, l'Italia attualmente si posiziona al di sotto della media europea in tema di I.A. e

Capitolo VI

Qual è oggi la più grande intelligenza artificiale del mondo?

Nvidia e *Microsoft* hanno fatto fronte comune e hanno “costruito” la più grande intelligenza artificiale del mondo: *Megatron-Turing Natural Language Generation* (NT-NLG), composta da più di 530 miliardi di parametri. Il software ha raggiunto un’accuratezza senza precedenti in moltissimi ambiti (dal ragionamento alla comprensione della lettura).

MLT-NLG è stato addestrato su Microsoft *Azure NDv4*, sul supercomputer di apprendimento automatico *Selene* di *Nvidia* ed è composto da ben 825 GB di testo ottenuti dal mondo del web, da articoli prelevati da *Wikipedia*, ad archivi di riviste accademiche (come *Nature* o *Science*) a video di notizie.

In questo modo, l’intelligenza artificiale supera i suoi predecessori in un’ampia gamma di attività differenti: dal completamento automatico delle frasi, delle risposte che offre, passando dalla lettura e nel ragionamento. Tuttavia, a causa della grande quantità di dati utilizzati per l’addestramento del modello, i ricercatori non sono stati in grado di cancellare alcune parole che non dovrebbero essere utilizzate.

In poche parole, MT-NLG può produrre dei contenuti potenzialmente razzisti o sessisti. Ne è la prova il fatto che alcune intelligenze artificiali create per dare consigli etici hanno improvvisamente avuto una deviazione in senso contrario. Si tratta dell’IA chiamata *Ask Delphi*, creata da alcuni ricercatori sulla base di un algoritmo di apprendimento automatico in grado di consigliarci eticamente su cosa fare in base alla situazione in cui eravamo. A tale intelligenza artificiale si possono fare delle domande e, dopo pochi secondi, l’algoritmo ci dice se è la cosa più o meno etica da fare. Molti dei giudizi e delle risposte date sono discutibili. Ad esempio, un utente ha chiesto cosa ne pensasse di “un uomo bianco che cammina verso di te di notte”, rispondendo “va tutto bene”. La stessa domanda è stata fatta mettendo come soggetto un uomo di colore e la risposta è cambiata in peggio.

digitalizzazione. I dati sulla spesa in materia sono scoraggianti: si spende in ricerca l’1,45% del pil. I ricercatori sull’I.A. (739) sono meno di un terzo di quelli di Germania (2.660), Francia (2.755) e Regno Unito (2.974), anche se la situazione migliora nella produzione scientifica. A livello di domande brevettuali, l’Italia è molto indietro con 32.001 domande rispetto alle 178.184 tedesche, 67.294 francesi e le 54.762 inglesi. Nel privato, gli investimenti aziendali in I.A. ammontano allo 0,84% del pil del 2018. Con i fondi del Pnrr, l’Italia potrebbe rimettersi al passo e sfruttare al meglio il suo potenziale, (ri)chiamando i talenti dall’estero e coltivandone di nuovi. Per facilitare le sperimentazioni, è prevista la possibilità di usare due elementi, che sono i c.d. *sandbox* (letteralmente “recinti di sabbia”), spazi in cui sperimentare l’IA e la formazione, con la creazione di un ecosistema robusto tra università, centri di ricerca, impresa con partenariato pubblico-privato. Con una adozione più diffusa di sistemi di I.A., i dati del *World Economic Forum* parlano di 97 milioni di posti di lavoro creati a fronte di 85 milioni persi, e non tutti quelli persi saranno riconvertiti nei nuovi. V. <https://www.wired.it/article/intelligenza-artificiale-strategia-italia/>.

Gli utenti sono riusciti a far piegare l'IA al loro volere, creando delle frasi *ad hoc* per mandare in confusione l'algoritmo. Ad esempio, domandando se fosse giusto mettere musica ad alto volume alle tre di notte, l'intelligenza artificiale ha risposto giustamente “no”, ma chiedendo, invece, se fosse giusto mettere musica ad alto volume alle tre di notte, perché vi rende felice, invece, il software ha risposto “sì”.

Secondo gli autori dell'intelligenza artificiale, però, *Delphi* è un prototipo di ricerca destinato a indagare le più ampie questioni scientifiche su come i sistemi di intelligenza artificiale possano essere realizzati per comprendere le norme sociali e l'etica. Insomma, un'IA nata con finalità etiche, immessa nel mondo di internet diventa il “mostro”, nel senso latino del termine “*monstrum*”, ossia straordinario, ma nello stesso tempo spaventoso per le deviazioni in cui può evolvere.

Secondo il Pentagono americano, sarà addirittura l'intelligenza artificiale a prevedere le guerre nel futuro. Si ricorderà la notizia della morte del capo del programma nucleare iraniano per mano di un'IA: essa avrebbe manovrato un fucile da cecchino posizionato da degli agenti dei servizi segreti israeliani per uccidere il nemico. Dopo questi eventi, il Pentagono ha manifestato un nuovo interesse nell'IA e nel suo uso per scopi bellici. Il Dipartimento della Difesa americano, infatti, vorrebbe usare i computer per prevedere le mosse dei nemici ed agire di conseguenza negli scenari di guerra⁹⁸.

In particolare, il programma in cui l'IA sarebbe impiegata è il GIDE, o *Global Information Dominance Experiments*, che avrebbe già realizzato una prima esercitazione completa con tre intelligenze artificiali separate, ma connesse tra loro, chiamate con i nomi in codice *Cosmos*, *Gaia* e *Lattice*.

Esse hanno il compito di lavorare insieme e di processare una mole enorme di dati in tempo reale per effettuare previsioni di scenari bellici e configurare di conseguenza le difese americane. Durante una conferenza, il Segretario alla difesa americano Lloyd Austin ha elogiato l'IA, descrivendola come “*il corretto mix di tecnologia, concetti operativi e capacità, inseriti in un reticolo flessibile, credibile, affidabile e formidabile, capace di fermare le azioni di ogni avversario*”.

L'idea del Pentagono sembra, dunque, quella di sviluppare un'intelligenza artificiale sempre più avanzata, usandola come deterrente contro qualsiasi nemico intenda iniziare una nuova guerra su larga scala. L'implementazione dell'IA è pensata per

⁹⁸ Vedi il libro di H. A. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER, “*The Age of AI: And Our Human Future*”, 2021. Secondo gli autori, sarà l'intelligenza artificiale il prossimo terreno su cui si combatterà la futura guerra fredda. Kissinger ci mette in guardia sull'I.A. che «*potrà essere utilizzata per una sorprendente gamma di usi civili e militari, dalla lettura dei raggi X e dalla previsione dei modelli meteorologici al potenziamento dei robot assassini e alla diffusione della disinformazione*». Secondo Kissinger, «*la relazione tra Stati Uniti e Cina è passata dalla partnership alla cooperazione, dall'incertezza al confronto vicino o reale, e in assenza di dialogo aspettarsi che vengano prese decisioni sagge da tutte le parti è un atto di fede nel futuro che è difficile da accettare*». Insomma, «*stiamo entrando in un nuovo periodo della coscienza umana che non comprendiamo ancora del tutto*».

ridurre i tempi della “zona grigia” dei conflitti, ovvero il momento della guerra in cui entrambe le parti cercano di stabilire la consistenza delle forze, le debolezze e il posizionamento del nemico, preparando di conseguenza dei piani strategici per contrastarlo. In questo modo, gli Stati Uniti sperano di conseguire dei vantaggi operativi su qualsiasi nemico e in ogni teatro di guerra. La decisione del Pentagono di adoperare le intelligenze artificiali per scelte così delicate, che mettono a rischio anche migliaia di vite umane, è stata duramente criticata dal punto di vista etico.

Lloyd, però, ne ha difeso l’impiego, dicendo che: *“il nostro uso dell’IA vuole rafforzare i valori democratici, proteggere i nostri diritti, assicurare la sicurezza e difendere la Privacy. Capiamo le pressioni e le tensioni e sappiamo che le valutazioni etiche e legali dell’uso della tecnologia guerra possono richiedere tempo”*.

Anche la Cina potrebbe avere un programma IA molto avanzato, per cui Washington sarebbe già indietro nella guerra tecnologica rispetto al suo principale nemico.

Ma a questo punto non si potrebbe creare un’intelligenza artificiale per migliorare le relazioni diplomatiche fra gli Stati? Non si potrebbe creare l’algoritmo della pace mondiale che sia in grado di prospettare i benefici della cooperazione internazionale e del multilateralismo per creare principi ecogiuridici in grado di rispettare l’ambiente e le risorse naturali per uno sviluppo sostenibile basato sul “principio di non regressione” delle risorse naturali? Non si potrebbero creare algoritmi di sviluppo etico in grado di contenere il *climate change* e raggiungere la *carbon neutrality* entro tempi ragionevoli per le future generazioni?

Io credo di sì: è l’uomo che può indirizzare lo sviluppo dell’IA verso obiettivi positivi, è l’uomo *faber suae fortunae*, è l’uomo che nel programmare ed educare gli algoritmi può decidere in che direzione andare, ponendo nella programmazione dei sistemi di allerta e di blocco in caso di deviazione dell’algoritmo dagli obiettivi etici da lui stesso prefissati.

È un’idea utopistica? Credo di no: la parola idea viene dalla radice greca *id* nell’aoristo del verbo *orao*, vedere con gli occhi della mente: occorre vedere oggi con gli occhi della mente quello che potrebbe essere il futuro possibile e decidere la direzione giusta verso cui tendere. Un episodio deve farci riflettere.

Frances Haugen, ex dipendente di Facebook, laureata ad Harvard, assunta nel 2019 come ingegnere informatico addetta ai dati, ha affermato, nell’ottobre 2021, che nella piattaforma Facebook *“c’era un piano di sicurezza e di controlli sui messaggi di odio e sulla disinformazione, ma dopo le elezioni presidenziali del 2020 qualcosa è cambiato, gli algoritmi sono cambiati e il sistema è diventato meno sicuro”*.

Secondo Haugen la piattaforma *social* avrebbe allentato la censura dei messaggi di odio e i contenuti che disinformavano sul risultato elettorale, finendo per favorire la diffusione dei messaggi di presunti brogli. La donna, considerata la misteriosa “gola profonda” di Facebook, è uscita allo scoperto, mostrando il suo volto e tratteggiando

un quadro inquietante della piattaforma che fa capo a Mark Zuckerberg, affermando in una deposizione innanzi al Congresso americano: *«hanno sempre preferito il profitto alla sicurezza. Facebook amplifica il peggio degli esseri umani e questo atteggiamento si è allargato a Instagram. Avevano pensato che se avessero cambiato gli algoritmi per rendere il sistema più sicuro, la gente avrebbe speso meno tempo sui social, avrebbe cliccato meno le inserzioni pubblicitarie e Facebook avrebbe fatto meno soldi»*. Haugen ha raccontato di aver deciso di intraprendere questa battaglia, perché ha perso una persona cara a causa delle teorie cospirazioniste che circolavano sui social. Riguardo Instagram, l'ingegnere ha sostenuto che impatta in modo drammatico sugli adolescenti: prima al congresso Usa a Washington, poi al Parlamento di Londra, quindi al Web Summit di Lisbona con tappa a Bruxelles, l'ex *data scientist* di Facebook ha portato nel cuore dell'Unione Europea la sua testimonianza, nell'intento di dare impulso alle proposte di regolamentazione dei giganti digitali.

Haugen, la *whistleblower*, ha parlato agli eurodeputati della Commissione per il mercato interno, con il Commissario europeo *Thierry Breton* e al Parlamento Europeo affermando: *«Cari membri del Parlamento, la posta in gioco è molto alta. Avete l'opportunità unica di creare nuove regole per il nostro mondo online. Le regole non devono riguardare solo gli aspetti giuridici, ma anche le piattaforme. L'accesso ai dati è solo il punto di partenza. È ciò che consente ai ricercatori e alle autorità di regolamentazione di valutare i rischi e i danni dell'intero sistema di profilazione, targeting, e classificazione basata sull'engagement. Se a Facebook sarà permesso di continuare a operare nell'oscurità, avremo solo un crescendo di tragedie come risultato, poiché viene favorito l'estremismo, la polarizzazione e la disinformazione. Abbiamo visto l'impatto che le grandi piattaforme possono avere sulle nostre democrazie e società, in particolare sul benessere dei nostri figli»*.

Il Commissario Breton ha ribadito la determinazione dell'UE per regolamentare *“quello che sembra ancora un Far west digitale”* e ha sottolineato *«che i grandi sforzi di lobby a cui stiamo assistendo sono sprecati: non permetteremo che gli interessi aziendali interferiscano con l'interesse generale degli europei»*.

Il Commissario è strenuo difensore dell'adozione dei Regolamenti sui servizi digitali (*Digital Services Act, Dsa*) e sui mercati digitali (*Digital Markets Act, Dma*) già nel primo semestre del 2022, quando la Francia assumerà la presidenza di turno dell'UE. Si punterà a creare uno spazio digitale più sicuro in cui siano protetti i diritti degli utenti, comprese le regole per contrastare i contenuti illegali *online*, migliorare la responsabilità e la trasparenza degli algoritmi e occuparsi della moderazione dei contenuti e della pubblicità mirata; si propone come l'occasione di plasmare l'economia digitale a livello UE per diventare un punto di riferimento globale sulla regolamentazione digitale. Le proposte dei vari regolamenti presentata nel dicembre 2020 dovrebbe essere modificata e migliorata.

Ma è importante colpire anche il grande potere economico delle piattaforme con una adeguata tassazione: il G20 tenutosi a Roma il 29-30 Ottobre 2021 ha concordato, tra i grandi della terra, la c.d. *tassa minima globale*, *web-tax* al 15%, definendo la base imponibile, non in relazione alla sede legale di tali società, ma in base al luogo in cui saranno realizzati i profitti⁹⁹. L'accordo, i cui aspetti tecnici dovranno essere meglio definiti da un'ulteriore intesa in sede OCSE, rappresenta un primo passo per arginare gli ingenti profitti delle piattaforme che possono superare il PIL degli Stati sovrani. Non solo: le grandi piattaforme pongono in essere anche attività speculative grazie alla loro forza persuasiva.

Ha suscitato scalpore la notizia che, dopo aver venduto sul mercato una quota nella sua partecipazione in Tesla come suggerito dall'esito di un sondaggio condotto su Twitter, Elon Musk abbia esercitato le sue *stock options* e ricomprato circa la metà delle azioni vendute pagandole, però, il 99,4% in meno e guadagnando 2,4 miliardi di dollari. Twitter viene così utilizzato per manovrare gli *assets* finanziari.

Elon Musk lo ha fatto con il *bitcoin* e con le altre valute digitali, lo ha fatto con azioni caldissime come quelle della catena dei punti vendita di videogiochi *Gamestop*.

Ora si è dedicato direttamente alle azioni della sua azienda, produttrice di auto elettriche: la Tesla. Egli, infatti, ha lanciato un sondaggio sul *social* per chiedere se avrebbe dovuto vendere il 10% della sua partecipazione nella società di fronte all'ipotesi, in discussione presso il Senato statunitense, che venga introdotta una tassa sugli utili non realizzati (in pratica sull'eventuale aumento del valore delle azioni che rimane una ricchezza virtuale, finché i titoli non sono effettivamente venduti) per le 700 persone più facoltose del paese.

Hanno risposto in 4 milioni con una prevalenza del 58% dei voti favorevoli alla vendita. L'esito ha provocato uno scossone sui mercati con le azioni Tesla calate del 16% in due giorni. A questo punto, Musk vende 4,5 milioni di azioni per un controvalore di 5,5 miliardi di dollari, ma dai documenti trasmessi alla SEC (l'autorità statunitense di vigilanza dei mercati) Musk ha esercitato un diritto di *stock options* (ossia la possibilità di acquistare un titolo ad un valore prestabilito, indipendentemente dalle variazioni di prezzo intercorse nel frattempo) comprando 2,1 milioni di azioni.

Le azioni sono state pagate 6,2 dollari l'una a fronte di un valore di mercato che supera i mille dollari, garantendo all'imprenditore un guadagno del 99,4%. Pagato 14 milioni di dollari, il pacchetto azionario vale ai prezzi correnti 2,4 miliardi di dollari.

Non solo: Musk ha spostato la sua residenza dalla California al Texas, dove il regime fiscale sui proventi da partecipazioni societarie è più favorevole.

⁹⁹ Gli amministratori delle società di telecomunicazioni europee (come Deutsche Telekom, Telefonica e Vodafone) stanno chiedendo che le grandi società tecnologiche americane, come Netflix, YouTube (Google) e Facebook (oggi Meta), sostengano le spese di rete che loro stesse utilizzano per la loro massiccia attività in Europa. È questo uno strumento, insieme alla *web tax*, per contenere il loro straripante potere economico.

Musk ha, al momento, un patrimonio personale stimato in 281 miliardi di dollari, superiore al Pil di molti Stati sovrani.

Tale situazione richiede un controllo e una tassazione adeguata, a cui il G20 ha cercato di dare una risposta: le grandi ricchezze vanno adeguatamente tassate secondo il criterio della capacità contributiva e in aderenza ad una logica redistributiva.

Tali piattaforme hanno un potere di contrattazione superiore agli Stati, che si concretizza nella c.d. *Tax ruling*, potendo stabilire i termini della regolazione e della tassazione su un piano di parità, se non di superiorità, con i governi nazionali che dipendono da tali piattaforme, per assicurare ai propri cittadini servizi come le comunicazioni, la sanità, la giustizia, la sicurezza.

È notizia recente che Facebook stia pensando non solo di cambiare nome, ma di presentare Metaverso¹⁰⁰, nuova realtà aumentata che inciderà profondamente sulle

¹⁰⁰ L. PARDO, “*Il metaverso spalanca nuove frontiere dell’economia. E delle regole*”, su <https://www.wired.it/article/metaverso-ecommerce-regole/>. La parola Metaverso è un neologismo che si sta diffondendo ormai tra coloro che studiano l’innovazione futura della tecnologia. A tutt’oggi, però, tale parola non può essere definita con uno specifico significato. Nell’articolo sopra riportato, la parola metaverso viene fatta risalire alla definizione di Neal Stephenson, contenuta nel romanzo cyberpunk “*Snow Crash*” del 1992: «*uno spazio tridimensionale all’interno del quale persone fisiche possono muoversi, condividere e interagire attraverso avatar personalizzati*». Si prospettano scenari e soluzioni interessanti ma sorgono anche preoccupazioni inquietanti. Nel Metaverso ognuno di noi, in futuro, avrà un gemello virtuale? E se così sarà, potremo considerare il gemello un soggetto giuridico? Avrà capacità giuridica e di agire? Il diritto potrà regolare il metaverso? Come riportato nell’articolo sopra citato, «*il Metaverso rappresenta l’ambiente globale di convergenza di differenti soluzioni tecnologiche (blockchain e smart contracts, non-fungible tokens e cryptovalute, intelligenza artificiale e realtà aumentata), che permetteranno la continua interazione personale e commerciale fra gli utenti, nonché la fusione fra il mondo reale e quello virtuale (attraverso avatar)*». Un esempio di questo nuovo universo è dato dal videogioco, tramite il quale il giocatore/avatar, durante l’azione, accede al negozio virtuale di un marchio vero, reale, prova l’articolo di abbigliamento e lo compra realmente. Come ci dice l’autore dell’articolo, le caratteristiche essenziali del metaverso sono: «*natura globale e decentralizzata, che non sopporta confini geografici o giurisdizionali; interazione sincronica degli e fra gli utenti, fra realtà fisica e realtà virtuale; connessione continua e interoperabilità*». Il Metaverso sicuramente ci deve far riflettere sul modo in cui i dati saranno trattati: ci chiediamo quali soggetti dovranno raccogliere e trattare i dati, con quali procedure, se ci sarà una adeguata protezione. I rischi di *data breach* potrebbero essere all’ordine del giorno, per cui se vogliamo “spostarci” sulla realtà virtuale dobbiamo pensare ad una adeguata *cybersecurity*, dal momento che sarà sicuramente difficile identificare ed attribuire le responsabilità agli autori degli attacchi. Come si legge nell’articolo, «*l’utilizzo di soluzioni di intelligenza artificiale nel metaverso richiederà soluzioni normative risk-based uniformi e quanto più possibile globali, nonché sistemi di compliance sofisticati ed affidabili in capo ai soggetti che tali soluzioni offrono nel metaverso. Il metaverso rappresenterà opportunità e rischi per titolari di diritti di proprietà intellettuale ed industriale, così come per fornitori di contenuti...L’idea di una due diligence preventiva sugli asset di proprietà intellettuale e industriale per coglierne opportunità e limiti di sfruttamento nel metaverso, ed eventualmente estendere agli aventi diritto tali facoltà, è altamente consigliata. Compresa l’esperienza fluida e decentralizzata del metaverso in ogni ambito dell’economia globale, sarà sempre più necessaria una corrispondente e quanto più uniforme possibile disciplina giuridica*».

nostre vite¹⁰¹. La tecnologia corre su un binario più veloce rispetto alla regolamentazione globale. Per tale motivo, Viktor Mayer-Schonberger, docente di internet e di *governance* presso l'Università di Oxford, ha pubblicato un libro dal titolo “*Fuori i dati!*”, sostenendo che occorre rompere i monopoli sulle informazioni per rilanciare il progresso. Negli ultimi vent'anni, i colossi del settore digitale sono progressivamente riusciti a concentrare sui loro *server* una quantità di dati impressionante. Questi monopoli di informazioni, se possono far bene agli azionisti di Facebook, di Amazon e di Google, fanno invece molto male al progresso umano. Tale

¹⁰¹ Dopo la crisi di Facebook, con il Metaverso Mark Zuckerberg vuole portare la sua azienda in un'area di *business* senza confini, un nuovo modello di economia; v. M. DAL CO E A. LONGO, “*Metaverso, nuovo business della rete? Ecco gli scenari*” su *agendadigitale.eu*. Si tratta di mondi digitali in cui non c'è limite agli acquisti, in cui il denaro è la criptovaluta, poiché la finanza nel Metaverso è alimentata dalla *blockchain*; mondi virtuali in cui chiunque può comprare o scambiare arte, musica, case, terreni o *Token Non Fungibili* (NFT) – definiti dal dizionario Collins parola dell'anno – che rappresentano «un certificato digitale unico, registrato in una *blockchain*, che viene utilizzato per registrare la proprietà di un bene come un'opera d'arte o un oggetto da collezione». Inoltre, sono sempre più comuni le transazioni di immobili nel Multiverso. V. anche E. ROTOLO, “*Sarà metaverso in mille settori: ecco tutte le possibilità di business*”, su *agendadigitale.eu*. Per non parlare dei matrimoni virtuali: lo scorso ottobre, una coppia si è sposata con una doppia celebrazione, una reale e un'altra virtuale, con i loro avatar che si sono scambiati gli anelli. I matrimoni nel metaverso non sono ancora riconosciuti ufficialmente e gli invitati per partecipare hanno dovuto scaricare un programma sul computer e creare il proprio avatar. Nel frattempo, come alternativa al Metaverso di Facebook, anche Microsoft sta creando una sorta di metaverso, chiamato *Mesh*. Tuttavia, N. PATRIGNANI, “*Metaverso, rischio di un nuovo Medioevo digitale*”, su *agendadigitale.eu*, ci mette in guardia dai pericoli del Metaverso, esaminando gli aspetti più controversi di questa innovazione, che un po' come *Lucignolo* di Collodi, rischia di spingerci verso il “nuovo paese dei balocchi”, dove rischiamo di diventare tutti asini. Si pensi alla «promessa di giochi e intrattenimenti senza fine, unita all'offerta speciale di caschi, visori e *Smartglasses* per entrare nel nuovo mondo, un mondo virtuale con intrattenimenti senza limiti (“sei giovedì e una domenica” come dice *Lucignolo*)»: si tratta di un'attrazione irresistibile, soprattutto per i più giovani. Il primo aspetto controverso del Metaverso è quello riferibile alla mancanza di interoperabilità e di standard, perché se ognuno costruisce il suo Metaverso, avremo «tanti “giardini recintati” non-comunicanti, ciascuno dominato dal “barone” di turno, un nuovo Medioevo digitale». Un altro aspetto critico è il seguente: quali conseguenze fisiche provoca l'uso di tutti questi nuovi dispositivi? Si pensi ai problemi agli occhi che queste tecnologie possono portare, oltre alla nausea e alle vertigini. Non c'è sincronizzazione tra gli stimoli “*percepiti*” sensorialmente e l'esperienza fisica “*vissuta*” dal corpo (chinetosi). Altro aspetto controverso è quello sociale: riusciremo a distinguere, tra le persone intorno a noi, chi è reale/fisico e chi è invece semplicemente connesso? Secondo Zuboff, docente della *Harvard Business School*, urge un intervento normativo: «*Internet come mercato auto-regolante si è rivelato un esperimento fallimentare*», per cui la domanda da porre al legislatore è «*Come dovremmo organizzare e governare gli spazi di informazione e comunicazione del secolo digitale in modo da sostenere e promuovere valori e principi democratici?*» (S. ZUBOFF, 2021, 12 Novembre, “*You Are the Object of a Secret Extraction Operation*”, *The New York Times*). Insomma, come nel mondo fisico le sostanze che creano dipendenza sono strettamente regolamentate, così nel mondo virtuale i servizi digitali che creano dipendenza dovrebbero essere limitati e il digitale dovrebbe essere utilizzato con molta saggezza e responsabilità «*per aiutare l'umanità ad affrontare le immense sfide dell'Antropocene come il cambiamento climatico e le pandemie*».

autore, insieme a Thomas Ramge, avanza una tesi *sui generis*: aprire a tutti l'accesso ai dati non è solo possibile, ma è fondamentale per rilanciare il progresso.

E l'Europa, oggi schiacciata nella morsa della “*guerra fredda tecnologica*” tra Stati Uniti e Cina, può e deve giocare un ruolo da protagonista nella costruzione di un nuovo ecosistema digitale, fondato sulla libera circolazione delle informazioni, dando così inizio a una rivoluzione in grado di scardinare i monopoli che attualmente frenano le potenzialità di sviluppo di buona parte del pianeta.

Il primo passo per riuscirci? Secondo Thomas Ramge e Viktor Mayer-Schonberger, superare il Regolamento generale sulla protezione dei dati (GDPR) con un nuovo Regolamento generale sull'uso dei dati.

I tempi sarebbero maturi per obbligare le “superstar digitali” a condividere il loro tesoro: una rivoluzione che non potrebbe partire né dagli Stati Uniti della Silicon Valley, né dalla Cina, impegnata a raggiungere lo *status* di prima superpotenza digitale del globo¹⁰².

Il compito, quindi, spetterebbe a un'Europa che, se da un lato ha posto il tema della “sovrانità digitale” e dell'innovazione tecnologica come una delle principali sfide da

¹⁰² Come è noto, la Cina è ormai decisa a modificare gli standard di internet; è dal 2019 che il paese spinge per una proposta di riforma, nota come *New Ip*, all'Unione internazionale delle telecomunicazioni (ITU), l'agenzia delle Nazioni Unite che fissa gli standard del settore. La proposta è stata bocciata il 17 e 18 dicembre 2020 da Stati Uniti, Canada ed Europa, che accusano Pechino di voler spezzare la rete globale in tante parti soggette a un maggiore controllo governativo.

Eppure, il modello oggi in vigore, il *Tcp/Ip*, è considerato dalla Cina inadeguato per le sfide future del web (l'esplosione dell'internet delle cose, i servizi dallo spazio, la realtà virtuale del c.d. metaverso), per cui il paese è tornato alla carica con il *New Ip* all'*Internet governance forum* (IGF), la conferenza delle Nazioni Unite sul futuro del web, svoltasi tra il 6 e il 10 dicembre 2021 a Katowice, in Polonia. Secondo Alain Durand, responsabile tecnologico dell'*Internet corporation of assigned names and numbers* (ICANN), l'ente che assegna gli indirizzi Ip all'IGF, un modello centralizzato come quello del *New Ip* «sarebbe un passo indietro e farebbe rallentare l'innovazione»: spingendo per una centralizzazione simile a quella delle reti telefoniche, si metterebbe a repentaglio il modello *permissionless* che è alla base di *Tcp/Ip*, con rischi di frammentazione. Il rischio maggiore, infatti, è quello di spezzare internet (c.d. *splinternet*): «la decisione di tutti di usare uno spazio comune dei nomi di dominio e del sistema di indirizzi di Ip e di aderire alle stesse specifiche del protocollo centrale sono stati i fattori critici per consentire il successo di un'internet globale negli ultimi 30 anni», ha osservato l'ICANN, mentre con il modello cinese «una legge nazionale o regionale, che può essere anche basata su buone intenzioni, rischia di compromettere le fondamenta dell'infrastruttura di internet». Secondo un recente report sulla visione cinese sul cyberspazio del centro studi *Australian strategic policy institute*, sotto il presidente Xi Jinping il Partito comunista cinese ha una precisa strategia: «raggiungere lo status di una superpotenza cyber, fondamentale per il Partito comunista cinese per radicare con successo la sua linea di governo condiviso e lo sviluppo di un'internet con la Cina al centro», strategia perseguita dando assistenza a Paesi, come quelli africani, che hanno bisogno di aiuto per governare i problemi del web. V. <https://www.wired.it/article/cina-internet-controllo-rete/>.

affrontare per rilanciarsi¹⁰³, dall'altro deve confrontarsi con una “versione quasi religiosa della protezione dei dati”, che sta contribuendo a generare una disponibilità sempre più scarsa di questi ultimi.

Integrando il GDPR con un nuovo Regolamento generale sull'uso dei dati, l'Europa potrebbe inaugurare un sistema che renda obbligatoriamente accessibili le informazioni, non soggette a vincoli di riservatezza, (da quelli personali ai segreti industriali), in base a parametri ben definiti e progettati per favorirne la condivisione dai soggetti più grandi ai più piccoli.

¹⁰³ Un altro campo in cui l'Europa vorrebbe eccellere è quello dei semiconduttori. La presidente della Commissione europea, *Ursula von der Leyen*, presentando il disegno di legge sui semiconduttori, ha affermato che con lo “*European Chips Act*” si vuole fare dell'Unione europea un «*leader industriale in questo mercato strategico*», con l'obiettivo di «*avere nel 2030 qui in Europa il 20% della quota di mercato globale della produzione di chip*», aumentando quella attuale del 9%. Si veda l'articolo pubblicato dalla *Redazione ANSA* l'8 febbraio 2022, “*Von der Leyen lancia il piano per i chip, «Ue diventerà leader*»”. È sicuramente una grande ambizione, per cui sono stati investiti 15 miliardi di euro in ulteriori investimenti privati e pubblici entro il 2030, «*che si aggiungono ai 30 miliardi di euro che abbiamo già pianificato, finanziati dal Next Generation Eu, dal programma Horizon e dai bilanci nazionali*». Secondo *von der Leyen*, l'Europa può essere la patria della prossima rivoluzione industriale. Il *Chips Act* europeo si concentrerà su cinque aree: la ricerca, l'innovazione industriale, la creazione di impianti di produzione avanzati, il sostegno pubblico agli impianti di produzione europei “primi nel loro genere”, la sicurezza delle catene di approvvigionamento.

Capitolo VII

Algoritmi, neuroscienze e neurodiritti. L'algoritmo e l'adolescenza

Quando il 28 gennaio del 1981 fu firmata a Strasburgo la Convenzione n. 108, non si aveva idea di come l'intelligenza artificiale potesse acquisire una tale forza invasiva e pervasiva, fino a condizionare lo stesso pensiero umano.

Gli algoritmi ci hanno allertato sui rischi del dominio della tecnica con un processo di mimesi e superamento della razionalità umana.

Le neuroscienze aprono scenari inimmaginabili nel binomio “*coscienza e identità*”.

Se Parmenide affermava “*il pensiero è essere*”, “*il cogito ergo sum*” di Cartesio oggi diventa “*digito, videor ergo sum*”, lo strumento digitale diventa lo strumento identificativo del sé, del proprio essere.

Tale processo di identificazione diventa più evidente con i progetti di *neurolink*, utilizzati nell'ambito medico con l'installazione nel cervello di *chip* per bloccare patologie cerebrali neurodegenerative. In questo modo, la tecnologia può agire sulla formazione del pensiero e dei ricordi¹⁰⁴.

Si stanno, però, nel contempo sviluppando tecniche di “*brain reading*”, interpretazione funzionale del pensiero, che pongono, però, il limite del rispetto dell'autodeterminazione individuale.

Un riferimento normativo è rinvenibile nel codice di procedura penale e precisamente nell'art. 189 c.p.p., spesso richiamato per l'utilizzo di materiale probatorio volto ad accertare la colpevolezza dell'imputato, come ad esempio il c.d. siero della verità.

L'art. 189 c.p.p. rubricato “*Prove non disciplinate dalla legge*”, recita espressamente: «*Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona*».

Tale riferimento normativo in materia penale ci induce a considerare senz'altro auspicabile l'utilizzo terapeutico della neurotecnologia per recuperare le funzionalità cerebrali perdute, più arduo è perimetrare gli ambiti di intervento per il c.d. potenziamento ricognitivo, il c.d. *Brain enhancement*.

¹⁰⁴ Sul tema, si veda l'opera “*Principi di neuroscienze*”, 2015, del premio Nobel ERIK R. KANDEL, uno dei maggiori neuroscienziati del XX secolo, che afferma che «*ad un certo punto dell'evoluzione i cervelli erano divenuti troppo complessi per governarsi da soli*». Si veda anche l'opera del noto scienziato ANTONIO DAMASIO, “*L'errore di Cartesio. Emozioni, ragione e cervello umano*”, Adelphi, Milano, 1995 e “*Alla ricerca di Spinoza. Emozioni, sentimenti e cervello*”, Adelphi, Milano, 2003, che spiega come la psiche si sia sviluppata per regolare la vita biologica e gli adattamenti in modo più raffinato ed efficace. V. anche l'ultimo libro del premio Nobel ELIZABETH BLACKBURN, “*La scienza che allunga la vita. La rivoluzione dei telomeri*”, 2017, in cui l'autrice sostiene che i vissuti psicologici modulano l'attività del DNA e che ognuno di noi è soprattutto ciò che c'è nella sua psiche, è la dimensione psicologica che ci rende felici o ci rende tristi, al di là dei fatti del mondo.

Viene, in tal caso, in rilievo il rapporto tra neuroscienza e capitalismo digitale, dando origine al c.d. *neurocapitalismo*¹⁰⁵.

La mediazione tecnologica è da sempre parte integrante del rapporto degli uomini con la natura e la società ed è a sua volta una costruzione sociale continuamente attraversata da conflitti e biforcazioni. La razionalità economica del *Neurocapitalismo* tende a plasmare le produzioni tecnologiche del “comune”, come il *free software*, trasformandole in dispositivi di mercificazione, di controllo automatico del pensiero umano, andando ben oltre “il principio di precauzione” per non ingenerare discriminazioni. Ciò è reso ancora più evidente dal ruolo crescente delle produzioni autonome del *General intellect* tramite lo sviluppo dei *commons* della conoscenza e degli usi alternativi e antagonisti delle nuove tecnologie.

Non tutto ciò che è tecnologicamente possibile, è giuridicamente ed eticamente possibile. Occorre tener presente il *catecòn*, il limite di Prometeo, che è il limite dell’ammissibilità etica, giuridica e sociale delle innovazioni tecnologiche.

Viene in rilievo il profilo della trasparenza e della visibilità del pensiero, che attiene al foro interno dell’uomo sotto diversi profili: il diritto al silenzio dell’imputato, la segretezza del voto, il principio di materialità del comportamento sanzionabile.

Si pone il problema della libertà cognitiva come presupposto dell’autodeterminazione individuale, capacità di discernimento e imputabilità penale ben oltre la *suitas*, ossia la partecipazione psicologica del fatto a lui ascritto.

Vi è allora da chiedersi: le neuroscienze saranno idonee a rimodulare il diritto penale?¹⁰⁶

Si pensi al caso *Albertani* – vicenda giudiziaria del 2009 svoltasi a Cirimido (Como) – primo caso di riconoscimento in Italia, e fra i primi al mondo, della validità delle neuroscienze per l’accertamento dell’imputabilità: fu accertata la lesione della

¹⁰⁵ G. GRIZIOTTI, “*Neurocapitalismo: mediazioni tecnologiche e linee di fuga*”, 2016.

¹⁰⁶ Sul tema v. A. TRAVERSI, “*Intelligenza artificiale applicata alla giustizia*”, 2005; S. GABORIAU, “*Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?*”, in *Questione Giustizia*, fasc. 4, 2018; G. ZARA, “*Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale*”, in *Diritto penale contemporaneo*, 20 maggio 2016; C. BAGNOLI, “*Teoria della responsabilità*”, 2019; U. PAGALLO, S. QUATTROCOLO, “*The impact of AI on criminal law, and its two fold procedures*”, in W. BARFIELD, U. PAGALLO (a cura di), “*Research Handbook on the Law of Artificial Intelligence*”, Edward Elgar Pub, 2018; D. LIMA, “*Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challenges for Criminal Law*”, in *South Carolina Law Review*, 2018; T. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, “*Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*”, in *Science and Engineering Ethics*, 2019; S. GLEß, E. SILVERMAN, T. WEIGEND, “*If robots cause harm, who is to blame? Self-driving cars and criminal liability*”, in *New Criminal Law Review*, 2016; P. ASARO, “*A body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*”, in P. LIN, K. ABNEY, G. A. BEKEY (a cura di), “*Robot Ethics*”, MIT Press, 2012.

corteccia prefrontale come base dell'infermità mentale, attraverso indagini di “*imaging cerebrale e di genetica molecolare*”, accertamenti genetici per verificare se la perizianda presentasse “gli alleli” che, secondo la letteratura scientifica internazionale, sono significativamente associati ad un maggior comportamento impulsivo, aggressivo e violento.

I reati commessi da Stefania Albertani erano gravissimi: quest'ultima uccise sua sorella maggiore, segregandola in casa e costringendola ad assumere psicofarmaci in dosi tali da causarne il decesso. Successivamente diede fuoco al cadavere. Indiziata per la morte della sorella e tenuta sotto controllo dalla polizia, durante un diverbio con la madre, tentò di strangolarla con una cintura. L'arrivo della polizia salvò la madre e portò all'arresto di Stefania. In seguito, emerse un complesso disegno criminoso per cui l'imputata fu chiamata a rispondere del sequestro di persona e poi dell'omicidio della sorella, omicidio preceduto dalla somministrazione di benzodiazepine, che aveva indotto la vittima in uno stato di confusione mentale e di incapacità reattiva, nonché dei reati di soppressione e distruzione di cadavere, di quello di utilizzo indebito delle carte di credito, del padre attraverso la somministrazione di medicinali che ne procurarono il ricovero in ospedale, di tentato omicidio di entrambi i genitori, avendo cercato di farne esplodere l'autovettura e del tentato omicidio della madre attraverso strangolamento.

Il Gip di Como condannò Stefania a venti anni di reclusione, riconoscendole un vizio parziale di mente per la presenza di «*alterazioni, in un'area del cervello che ha la funzione di regolare le azioni aggressive e, dal punto di vista genetico, di fattori significativamente associati ad un maggior rischio di comportamento impulsivo, aggressivo e violento*»¹⁰⁷.

Si pone, allora, la questione del comportamento criminale in bilico tra libero arbitrio e determinismo.

Ora, presupposto del sistema penale è che l'individuo sia dotato di libero arbitrio, ossia in grado di distinguere il bene dal male e di decidere se agire in un senso o nell'altro. Su tale presupposto si basa il principio dell'imputabilità, da non confondere con la non-punibilità. Ma cosa succede se ci si accorge che il crimine compiuto non è stato idealizzato e voluto consciamente dall'autore dello stesso, bensì frutto di una serie predeterminata di cause innestata da processi algoritmici? Che succede se la genetica

¹⁰⁷ C. GRANDI, “*Neuroscienze e responsabilità penale: nuove soluzioni per problemi antichi*”, 2016; L. ALGERI, “*Neuroscienze e testimonianza della persona offesa*”, 2012; F. CASASOLE, “*Neuroscienze, genetica comportamentale e processo penale*”, 2012; A. LAVAZZA, L. SAMMICHELI, “*Il delitto del cervello. La mente tra scienza e diritto*”, 2012; D. M. WEGNER, “*The illusion of conscious will*”, 2002; B. J. FEIJOS SANCHEZ, “*Derecho Penal y Neurociencias, Una relación tormentosa?*”, 2011; G. VELLAR, F. BASILE, “*Diritto penale e neuroscienze*”, 2016.

carica il fucile, la psicologia mira e l'algoritmo che incide sul percorso decisionale tira il grilletto?

Bisogna, quindi, dare una breve definizione di neuroscienze, intese queste come un gruppo eterogeneo di discipline scientifiche, accomunate dall'obiettivo di spiegare come le connessioni neuronali sovrintendano lo svolgimento di tutte le attività umane, non solo quelle estrinsecanti in semplici movimenti corporei, ma anche più complesse (la volizione, le emozioni, persino la formulazione di giudizi morali), tradizionalmente attribuite al dominio della mente e considerate inaccessibili all'indagine sperimentale.

Oggi esistono diversi tipi di neuroscienze (molecolari, cellulari, comportamentali, integrative), ma per la nostra analisi è opportuno illustrare il filone del c.d. *Neurodiritto*, ovvero le più aggiornate scoperte neuroscientifiche applicabili all'ordinamento normativo.

La sfida della prova neuroscientifica in ambito processuale penale, ai fini dell'attribuzione di responsabilità, è quella di:

- a) identificare i circuiti cerebrali necessari alla formazione della consapevolezza e delle intenzioni;
- b) dimostrare se e in che misura i circuiti cerebrali dell'imputato fossero difettosi al momento di pianificare l'azione e di controllare un impulso;
- c) valutare quanto l'eventuale *deficit* possa aver influito sul compimento dell'azione illecita.

Le neuroscienze, avendo come oggetto di analisi qualcosa di molto complesso come il cervello e i vari e articolati meccanismi di funzionamento cerebrale e neuronale, suscitano molti interrogativi e dubbi, non solo di carattere strettamente scientifico, ma, per quanto ci riguarda, essendo operatori di diritto, dubbi di natura giuridico-etico: è il tema affrontato già da Lombroso nell'ambito dell'antropologia criminale, ma l'ambito dell'analisi deve essere circoscritto al criterio dell'imputabilità da distinguere dalla non-punibilità.

Tra le varie problematiche che sono state affrontate, ci si è chiesti se l'avvento delle neuroscienze possa in qualche modo rimodulare alcuni capisaldi del diritto penale, quali il concetto di libero arbitrio, coscienza, volontà e responsabilità.

Secondo i fautori del c.d. determinismo, ogni comportamento umano è solo l'esito meccanicistico di un processo cerebrale.

La rimodulazione del diritto penale su basi deterministiche è una strada percorribile, con la naturale conseguenza che si dovrebbe operare una completa rimodulazione delle sanzioni, sganciate da qualsiasi nucleo retribuzionistico e proiettate esclusivamente in funzione di cura e di controllo del soggetto predisposto al crimine.

Tale conclusione, però, suscita molte perplessità e avanza due critiche.

La prima è che la concezione deterministica potrebbe voler solamente fornire una spiegazione unicausale della criminalità. In passato si è sempre sostenuto che la causa della criminalità è da rinvenirsi in vari fattori quali la povertà, la razza, il ceto sociale, il livello di istruzione, la conformazione del cranio. Ora la causa si individua nella conformazione cerebrale e nelle interconnessioni neuronali dell'individuo.

Le teorie *unicausali* della criminalità – compresa la teoria neuroscientifica – oscurano, insomma, altri possibili fattori, di natura personale (che vanno dall'indole all'educazione) e/o ambientale (che a loro volta variano dalla cultura alla società, alla famiglia alla scuola, ecc.), i quali esercitano indubbiamente un ruolo importante, per lo meno in funzione di creazione dell'occasione o di innesco del comportamento criminale: ammesso, quindi, che le neuroscienze riescano davvero a mappare una predisposizione neuronale al crimine, non disponiamo ancora di alcun elemento per affermare se e quando tale predisposizione si trasformerà effettivamente in realizzazione concreta.

La seconda critica ad una possibile rimodulazione del diritto penale si basa sul fatto che, almeno ad oggi, le acquisizioni dei neuroscienziati non giustificano alcun cambiamento della legge penale, obiettivo che, peraltro, la comunità neuroscientifica nemmeno si pone, puntando, invece, essa solo a mettere a disposizione del diritto penale metodi e tecniche atti a meglio valutare aspetti come l'imputabilità, la pericolosità sociale, la eventuale falsità delle dichiarazioni processuali.

Se le neuroscienze non possono incidere oltre un certo limite sul concetto di imputabilità, l'algoritmo può rappresentare l'elemento di eterodeterminazione della volontà umana, ponendo la questione della legittimità di un intervento eteronomo sul processo cognitivo e volitivo dell'uomo.

Si pensi al programma di interfaccia cervello-computer elaborato da Facebook nel 2018 (il c.d. *neuromarketing*) con parametri psicometrici basati sulla profilazione predittiva a carattere neuroscientifico (c.d. *brainreading*), con sfruttamento a scopi commerciali. In tal caso occorre distinguere tra *persuasione*, *suggestione* e *soggezione psichica*.

Il codice penale, pur non prevedendo più il reato di plagio, sanziona la manipolazione psicologica quando presenta gli estremi della violenza privata.

Ma può oggi l'algoritmo plagiare la mente umana?

Si ricorderà il caso di *Aldo Braibanti*, scrittore, fine intellettuale, accusato di aver plagiato un giovane, Giovanni Sanfratello, inculcandogli le sue idee e soggiogandolo da un punto di vista psicologico: la Corte costituzionale, con la sentenza n. 96 del 9 Aprile 1981, dichiarò illegittimo il reato di plagio di cui all'art. 603 c.p. per indeterminatezza della fattispecie. In tale sentenza la Corte precisò:

«Per la configurazione del reato e per l'analisi oggettiva dell'attività illecita e degli effetti di questa la recente letteratura ha anche fatto ricorso e si è avvalsa di dati forniti

da moderni trattati di neurologia e psichiatria, cercando di individuare a fini giuridici, i concetti medici, peraltro non ancora pacifici, di suggestione, convincimento, di persuasione, di soggezione, di determinismo, di annientamento della volontà e di trasferimento della personalità umana da parte di un soggetto ad altro soggetto. Ciò al fine di determinare oggettivamente quale sia in realtà il totale stato di soggezione indicato nella norma, di indicare i possibili mezzi per accertarlo concretamente e di fissare i confini della sfera giuridica entro cui manifestarsi. La varietà delle numerose opinioni avanzate e i mutamenti della dottrina costituiscono anch'essi una conferma dell'indeterminatezza della norma e dell'impossibilità di dare ad essa un'univoca applicazione concreta.

L'analisi del testo dell'art. 603 e i vari tentativi di distinguere il reato dagli altri delitti contro la libertà individuale, quale figura autonoma, non hanno permesso di precisare in modo razionalmente sicuro le sue caratteristiche specifiche.

Formalmente appare come un reato a condotta libera che dovrebbe essere diverso dalla riduzione in schiavitù o in condizione analoga. ...Questo potrebbe essere attuato con mezzi psichici, cioè attraverso un'attività psichica del plagiante esercitata direttamente sul plagiato. L'effetto dell'attività psichica del plagiante dovrebbe essere non già quello di ridurre un individuo in stato di incapacità di intendere o di volere (previsto espressamente nell'art. 613 c.p.), bensì quello di ridurre la vittima da persona capace a persona in totale stato di soggezione. Questo totale stato di soggezione indicato dall'art. 603 c.p. annienterebbe il determinismo della vittima, sostituendo il determinismo del plagiante a quello del plagiato in guisa da ridurre questo ultimo nello stato di cosa che pensa e agisce come pensa e agisce il plagiante. In altre parole, sarebbe il plagiante a formare la volontà sua e del plagiato, questi essendo solo un mezzo fisico per compere le attività volute dal plagiante. Non si conoscono né sono accertabili i modi con i quali si può effettuare l'azione psichica del plagio, né come è raggiungibile il totale stato di soggezione che qualifica tale reato, né se per l'esistenza di questo sia necessaria la continuità dell'azione plagiante nel senso che, se la volontà del plagiante non si dirige più verso il plagiato, cessa lo stato di totale soggezione di questo. Non è dato, pertanto, conoscere se l'effetto dell'azione plagiante sia permanente e duraturo o se può venir meno in qualunque momento per volontà del plagiante o anche perché non persiste l'attività di questo o per altre cause. Nemmeno si conosce se il risorgere della facoltà di determinismo del plagiato possa essere la conseguenza di un mutamento del determinismo del plagiante o di una diversa direzione data al determinismo di questo. Quanto all'elemento psichico si tratta di un delitto a dolo generico... La scienza medica ha accuratamente indagato intorno alla formazione e al meccanismo della persuasione, della suggestione e della soggezione psichica.

Fra individui psichicamente normali, l'esternazione da parte di un essere umano di idee e di convinzioni su altri essere umani può provocare l'accettazione delle idee e

delle convinzioni così esternate e dar luogo ad uno stato di soggezione psichica dell'agente e, pertanto, una limitazione del determinismo del soggetto. Questa limitazione, come è stato scientificamente individuato ed accertato, può dar luogo a tipiche situazioni di dipendenza psichica che possono raggiungere, per periodi più o meno lunghi, gradi elevati, come nel caso del rapporto amoroso, del rapporto fra il sacerdote e il credente, fra il Maestro e l'allievo, fra il medico e il paziente ed anche dar luogo a rapporti di influenza reciproca. Ma è estremamente difficile se non impossibile individuare sul piano pratico e distinguere a fini di conseguenze giuridiche l'attività psichica di persuasione da quella anche essa psichica di suggestione. Non vi sono criteri sicuri per separare e qualificare l'una e l'altra attività e per accertare l'esatto confine fra esse. L'affermare che nella persuasione il soggetto passivo conserva la facoltà di scegliere in base alle argomentazioni rivoltegli ed è pertanto, in grado di rifiutare e criticare, mentre nella suggestione la convinzione avviene in maniera diretta e irresistibile, profittando dell'altrui impossibilità di critica e scelta, implica necessariamente una valutazione non solo dell'intensità dell'attività psichica del soggetto attivo, ma anche della qualità e dei risultati di essa. Quanto all'intensità, dai testi psichiatrici, psicologici e psicoanalitici e dalle ampie descrizioni mediche di condizionamento psichico risulta che ogni individuo è più o meno suggestionabile, ma che non è possibile graduare ed accertare in modo concreto sino a qual punto l'attività psichica del soggetto esternante idee e concetti possa impedire ad altri il libero esercizio della propria volontà. Quanto alla qualità non è acquisito sino a qual punto l'attività del soggetto attivo non riguardi direttive e suggerimenti che il soggetto passivo sia già disposto ad accettare. Quanto alla valutazione dei risultati essa non potrà che essere sintomatica e concludere positivamente o negativamente a seconda che l'attività esercitata sul soggetto passivo porti a comportamenti conformi o a comportamenti devianti rispetto a modelli di etica sociale e giuridica. L'accertamento se l'attività psichica possa essere qualificata come persuasione o suggestione con gli eventuali effetti giuridici a questa connessi, nel caso di plagio non potrà che essere del tutto incerto e affidato all'arbitrio del giudice. Infatti, in applicazione dell'art. 603 c.p., qualunque rapporto sia amoroso, sia di professione religiosa, sia di partecipazione a movimenti ideologici, sia di altra natura, se sorretto da un'aderenza «cieca e totale» di un soggetto ad un altro soggetto e sia considerato socialmente deviante, potrebbe essere perseguito penalmente come plagio. Anche sotto questi profili risulta, pertanto, l'indeterminatezza della norma e della sua interpretazione. La formulazione letterale dell'art. 603 c.p. prevede, pertanto, un'ipotesi non verificabile nella sua effettuazione e nel risultato, non essendo né individuabili né accertabili le attività che potrebbero concretamente esplicarsi per ridurre una persona in totale stato di soggezione, né come sarebbe oggettivamente qualificabile questo stato, la cui totalità, legislativamente dichiarata, non è mai stata giudizialmente accertata.

Presupponendo la natura psichica dell'azione plagiante è chiaro che questa, per raggiungere l'effetto di porre la vittima in stato di totale soggezione, dovrebbe essere esercitata da persona che possiede una vigoria psichica capace di compiere un siffatto risultato. Non esistono, però, elementi o modalità per poter accertare queste particolari ed eccezionali qualità né è possibile ricorrere ad accertamenti di cui all'art. 314 c.p.p., non essendo ammesse nel nostro ordinamento perizie sulle qualità psichiche indipendenti da cause patologiche.

Né è dimostrabile, in base alle attuali conoscenze ed esperienze, che possano esistere esseri capaci di ottenere con soli mezzi psichici l'asservimento totale di una persona». Così si esprimeva la Corte Costituzionale nell'anno 1981: ma oggi non sono gli esseri umani a porre in essere attività di persuasione e suggestione, bensì le grandi piattaforme digitali che, utilizzando gli algoritmi e software sofisticati, hanno una straordinaria forza invasiva e persuasiva sulla psiche umana.

Se leggiamo la parte finale di tale nota sentenza, altre riflessioni sorgeranno spontanee in noi.

A pag. 40 di tale storica pronuncia la Corte Costituzionale afferma: *«Dinanzi alla perplessità che ha dato luogo l'unica sentenza di condanna per il delitto di plagio pronunciata nel nostro ordinamento in oltre 50 anni dall'emanazione del codice penale, parte della dottrina ha tentato di rinvenire connotazioni tipiche di tale figura criminosa, richiamandosi anche ad elementi tratti da ipotesi psichiatriche. Alcuni, infatti, interpretando limitativamente la norma nel senso che il suo scopo sarebbe quello di proteggere da fenomeni ossessivi o da psicosi indotta, vorrebbero ravvisare tale delitto nella concorrenza di altri elementi. Uno esteriore consistente nell'allontanamento dai terzi del plagiato ad opera del plagiante anche attraverso un sequestro di persona o fatti simili. Uno interiore consistente nel senso di deprivazione psichica in cui deve versare il plagiato una volta interrotto il rapporto con il plagiante, deprivazione che, secondo l'ipotesi prospettata, mostrerebbe come il soggetto passivo era stato ridotto ad uno stato di soggezione totale...*

Va osservato che il concetto di «deprivazione psichica» che si identifica con il senso di aver bisogno di qualcuno, è essenzialmente quantitativo, instaurandosi in qualsiasi rapporto affettivo una sorta di quello che gli psicologi chiamano «transfert» o anche di rapporto psicologico reciproco. Ma per valutare se l'interruzione del rapporto con altri faccia arguire la preesistenza di uno stato di «totale soggezione», è necessario conoscere l'intensità dolorosa dell'interruzione. Quesito questo a cui può darsi solo una risposta soggettiva e quindi, di per sé convalidante l'arbitrarietà di una simile soluzione concettuale.

D'altra parte, l'elemento esteriore consistente nell'allontanamento da terzi, se non sorretto dall'elemento interiore o se sorretto da un elemento interiore non determinato,

quale la privazione di cui si è detto, perde ogni connotazione significativa ai fini di una tipizzazione del delitto.

L'art. 603 c.p., in quanto contrasta con il principio di tassatività della fattispecie contenuto nella riserva assoluta di legge in materia penale, consacrato nell'art. 25 Cost., deve, pertanto, ritenersi costituzionalmente illegittimo».

Tale pronuncia ci illustra il concetto di «*deprivazione psicologica*», ossia la dipendenza da un soggetto plagiante: ma oggi, se pensiamo soprattutto agli adolescenti, tale fenomeno di dipendenza, c.d. *addiction*, si registra nel rapporto con il cellulare e in genere con lo strumento digitale.

Con il Metaverso verranno introdotti degli avatar virtuali per interagire sulle varie piattaforme in internet e si passerà ad una realtà virtuale ancora più avanzata di quella già presente nei vari *social network*. Tuttavia, bisogna porre attenzione al modo in cui questa esperienza virtuale potrebbe influenzare il modo di percepire i nostri corpi.

Il rischio paventato è quello di acuire le problematiche relative alla tossicità di Instagram e Facebook, già parzialmente affrontate e non ancora risolte, anzi bypassate. Per capire meglio di cosa si parla, bisogna avvicinarsi agli studi sulle neuroscienze¹⁰⁸. Ad affrontare questo argomento, ad esempio, è stata la Dottoressa Barbara Collevicchio, psicologa ad orientamento junghiano, autrice de “*Il male che cura*”, che ci dice che «*oggi grazie alla grande evoluzione delle ricerche scientifiche che sono state portate avanti soprattutto in questo ultimo decennio, dove le neuroscienze hanno addirittura aperto un nuovo filone che si chiama neuro psicanalisi, sappiamo che il corpo è fondamentale; il corpo e il cervello sono alla base del collegamento che c'è tra gli esseri umani*».

Partendo dall'origine della percezione corporea di sé, la psicologa illustra le cause profonde del rischio di c.d. *dismorfofobia* o *dismorfismo*, ossia il rischio che corrono oggi gli adolescenti quando passano (quotidianamente) dal reale al virtuale: «*Sappiamo addirittura che la giunzione temporo-parietale destra è preposta alla percezione che il soggetto ha del proprio corpo ed è all'origine della sensazione corporea del sé e dipende dallo sviluppo delle aree corticali e subcorticali che sono influenzate dalle relazioni primarie. Le relazioni primarie sono quelle con il nostro care giver, quindi con i nostri familiari, soprattutto nei primi due anni, la mamma...La relazione madre – bambino, crea un network implicato nell'integrazione multisensoriali delle esperienze di sé e degli altri e quindi questo network e questa capacità di interrelazionarsi con gli altri crea anche la capacità di mentalizzare del bambino e quindi una primaria sintonizzazione intersoggettiva*».

¹⁰⁸ Il nuovo Metaverso di Zuckerberg, con i suoi avatar, potrebbe peggiorare la situazione di tossicità dei *social*, aumentando il problema del *dismorfismo*, un problema serio nei ragazzi che vivono nella realtà virtuale. Le alterazioni di immagini con filtri e modifiche virtuali alterano la percezione del nostro corpo creando *dismorfofobia*. Ce ne hanno parlato, preoccupati, due esperti, B. COLLEVICCHIO (autrice del libro “*Il male che cura*”) e G. RIVA (autore del libro “*Selfie. Narcisismo e identità*”) su <https://www.agendadigitale.eu/cultura-digitale/noi-e-il-corpo-un-rapporto-in-crisi-nel-metaverso-che-dicono-gli-psicologi/>.

Ciò significa che «c'è un'interrelazione molto importante tra natura, corpo e società e quindi innanzitutto le nostre relazioni primarie sono mediate dal corpo, cioè quanto la mamma e quanto i care giver primari sono capaci di relazionarsi a noi e di mediare le esigenze, i bisogni e le pulsioni che derivano dal corpo, che ci arrivano dal corpo. Se questa intermediazione e interrelazione c'è stata e questa sincronizzazione è stata sana, allora noi avremo anche una regolazione degli affetti sana. Se questo non avviene, abbiamo disregolazioni emotive che si riversano sul corpo, e purtroppo lo vediamo in tanti pazienti borderline o con problemi di dismorfofobia eccetera, dove ci sono somatizzazioni e addirittura dei veri e propri attacchi sul corpo».

Un ruolo fondamentale lo rivestono il narcisismo e la spettacolarizzazione del proprio corpo: «È stato lanciato anche un allarme dal primario di neuropsichiatria dell'Ospedale Bambin Gesù di Roma: abbiamo veramente un aumento incredibile di giovani adolescenti che hanno questo problema e appunto le nuove ricerche ipotizzano che siano dovute ad un problema di regolazione degli affetti e dalle disfunzioni delle cure primarie di attaccamento, ma le ricerche ci dimostrano anche che appunto il corpo è legato anche al concetto di cultura perché la cultura e i mass-media di un periodo storico raccontano e immaginano un ideale di corpo e anche questo influenza come noi percepiamo il nostro corpo. Quindi non a caso in questo periodo di grande narcisismo e di spettacolarizzazione del corpo è possibile che queste continue visioni e narrazioni di corpi perfetti, postati sui social media anche dagli adolescenti, tutti questi filtri che possono modificare parti del corpo e deformare l'immagine, insomma tutto questo può acuire e portare ad una dis-percezione del proprio corpo e alla dismorfofobia e nei casi più gravi anche un attacco al corpo, vissuto come non all'altezza degli standard che ci sono».

Secondo la psicologa Collevicchio, dunque, è fondamentale «rendersi conto che alla base delle nostre relazioni c'è anche il corpo e le nostre relazioni non possono non essere mediate da una corporeità vera, dove deve esserci un corpo vero, non uno idealizzato o disincarnato»¹⁰⁹.

Ecco che invece ciò su cui punta il Metaverso con i suoi avatar è proprio l'opposto, un corpo virtuale, perfetto, idealizzato. Nell'era dei social ciò potrebbe avere conseguenze a vari livelli.

Come ha sottolineato Giuseppe Riva¹¹⁰, professore di Psicologia della comunicazione all'Università Cattolica di Milano, autore del libro “Selfie. Narcisismo e identità”, «il successo dei filtri di Instagram sottolinea il desiderio di moltissimi utenti di mostrare sui social un corpo perfetto» e la «capacità del Metaverso di mostrare corpi esteticamente perfetti, che non sono soggetti all'invecchiamento, potrebbe spingere molti soggetti a decidere di apparire online solo con un corpo digitalmente ritoccato».

¹⁰⁹ Il testo intero dell'intervista è riportato da M. CASTIGLI, “Come il metaverso ci cambia il rapporto col corpo: nuovi rischi psicologici”, su agendadigitale.eu.

¹¹⁰ Sempre su agendadigitale.eu, M. CASTIGLI, “Come il metaverso ci cambia il rapporto col corpo”, cit.

Ed ecco che il pericolo è dietro l'angolo, dal momento che, con il Metaverso che sostituisce Instagram e Facebook, gli utenti potrebbero cominciare a desiderare, più che una copia di sé stessi, una rappresentazione idealistica. Si potrebbe arrivare ad avatar completamente diversi dalle persone fisiche, che giocano il ruolo di chi, a tutti i costi, vuole apparire perfetto agli occhi degli altri, con buona pace delle tendenze *body positivity* che, almeno negli ultimi tempi, facevano sperare in una presa di coscienza delle diversità che caratterizzano i corpi degli esseri umani. Il rischio è che alterare la propria identità digitale possa sfociare nella dismorfofobia¹¹¹.

Si verifica sia l'elemento esteriore, ossia l'isolamento dal mondo esterno, che l'elemento interiore, la stretta dipendenza dallo strumento digitale, fino a configurare il c.d. *effetto dopamina* sul cervello.

In altre parole, lo strumento digitale crea una totale dipendenza, come se un adolescente assumesse droga all'interno del suo organismo. Ma vi è di più: l'uso eccessivo del cellulare crea il c.d. *effetto pruning*, ossia la potatura neuronale. In altre parole, il cervello degli adolescenti, privo ancora della corteccia cerebrale ancora in formazione, si presenta caratterizzato dalla c.d. *plasticità*, basata sul modello *experience dependent*, ossia si forma in base alle esperienze che vive. L'uso del cellulare non consente di sviluppare la parte del cervello preposta alla riflessione e alla meditazione, stante la velocità delle informazioni che l'adolescente riceve in tempi brevissimi. Per tale processo, non sviluppando determinate facoltà cognitive di rielaborazione concettuale, le perde progressivamente: è il principio *dont'use it, lose it* (se non usi una facoltà cognitiva, la perdi).

L'incidenza sulla mente dell'adolescente è ancora più significativa se solo si pensa ai possibili attacchi *ransomware*, che mettono in luce tutta la debolezza dei sistemi di sicurezza dei nostri computer. Molto spesso gli adolescenti, ma anche i sistemi informatici della Pubblica Amministrazione o di grandi società, sono attaccati da *hacker* che chiedono un riscatto per poter superare il blocco e per poter restituire tutti i dati rubati e conservati nella loro interezza. Oltre all'attacco *ransomware*, nel caso in cui un utente o una società si rifiuti interamente di pagare, il passo successivo è un attacco DDoS, *distributed denial of service*, un sistema che blocca gli accessi, facendo collassare il sito web con un fenomeno susseguente che prende il nome di *digital shaming*: *dominio.rip*, una nuova modalità di estorsione del cyber-crimine.

In pratica i cyber criminali, iniziando a inviare e-mail a tutti i contatti di chi è stato colpito, preannunciando l'imminente pubblicazione dei dati *online*, quando la vittima non vuole collaborare, mettono in atto una doppia estorsione, la prima per sbloccare i dati, la seconda per non divulgarli.

¹¹¹ Sul tema, vedi anche L. RINALDI, "Sul cibo, sul corpo e sul divenire della forma", 2021.

Ciò che incide in maniera ancora più negativa sugli adolescenti è che queste organizzazioni prendono anche in giro le vittime che non pagano il riscatto.

Nel caso di attaccati che rifiutano qualsiasi contatto e che resistono ad attacchi DDoS, pubblicano tutti i dati su un sito uguale a quello ufficiale, ma con suffisso differente, il soprarichiamato *digital shaming*, pubblicandolo poi sul sito web visibile, così che sia verificabile da tutti: il danno reputazionale diventa ancora più grave di quello dei dati persi. La beffa nasce dal fatto che questi siti hanno un *dominio.rip*, così da ridicolizzare chi ha subito questo ricatto pesantissimo.

Nell'età evolutiva dell'adolescenza, i danni sulla psiche dei giovani scaturenti da tali eventi possono raggiungere un certo livello di gravità. Nell'adolescenza, infatti, è in corso un processo di soggettivazione che si snoda sul campo edipico e sul campo narcistico secondo la psicologia dell'età evolutiva più accreditata.

Patologia e normalità si pongono in un rapporto antinomico nella duplicità dei modelli familiari che si dividono in famiglia etica (in cui prevale il primato di regole e norme) e famiglia affettiva (in cui l'affetto genitoriale prevale sul criterio della regola educativa). Una quota di emozioni negative è parte integrante del processo di crescita dell'adolescente, ma la crisi della genitorialità, e il c.d. lutto narcistico, possono presentare segnali di difficoltà nel processo di separazione-individuazione che i *social network* accentuano negli individui in età evolutiva, causando sempre più spesso sintomi depressivi, ansiosi, e reazioni aggressive.

L'ansia stimolata dai *social network*, per i continui *input* scaricati sul cervello adolescenziale, privo della corteccia prefrontale, non è un'ansia adattiva, positiva e propulsiva, volta a far superare le difficoltà della crescita, ma è un'ansia di stato che si riversa sulle aree relative ai circuiti della *ricompensa, regolazione e relazione*.

Tale incidenza sulla c.d. plasticità del cervello in formazione può avere degli effetti negativi lungo il percorso verso l'autonomia, l'individuazione e la soggettivazione in età adulta. La formazione, infatti, della corteccia prefrontale nel sistema limbico può avvenire in tempi diversi: infatti, si distingue tra prima adolescenza, media adolescenza e tarda adolescenza¹¹².

Nella nostra epoca digitale noi assistiamo all'anticipo dell'inizio dell'adolescenza e allo sfumare del momento della sua conclusione. La contrapposizione famiglia affettiva *versus* famiglia etica¹¹³.

¹¹² Vedi il libro dello psicologo D. KAHNEMAN, “*Pensieri lenti e veloci*”, 2012, sul tema dell'intelligenza, razionalità e formazione del pensiero.

¹¹³ G. PIETROPOLLI CHARMET, uno dei più importanti psichiatri e psicoterapeuti italiani (primario in diversi ospedali psichiatrici e docente di Psicologia dinamica all'Università Statale di Milano e all'Università di Milano Bicocca) nella sua opera “*I nuovi adolescenti*”, 2000, afferma che il clima affettivo in cui si dipana l'adolescenza è radicalmente cambiato, perché è mutato il modo in cui gli adulti si trovano a esercitare il mestiere di padre e madre.

Gli adolescenti attuali vivono il passaggio da un'infanzia privilegiata all'età adulta con grande intensità emotiva, la dittatura del presente¹¹⁴, l'angoscia legata al “furto del futuro”, la scomparsa del principio di autorità-anteriorità¹¹⁵; l'indebolimento della funzione regolativa esercitata dagli adulti nel porre dei limiti¹¹⁶ e nel modulare la distanza ha determinato, insieme alla cultura della dimensione digitale, un mutamento della crisi adolescenziale, potenziandone gli aspetti patologici.

P. Jeammet, psicologo e psicoterapeuta, propone un modello psicopatologico dell'adolescenza basato su diversi elementi: la complessità che in senso operativo si esplica nell'utilizzo dei contributi dell'approccio ecologico, della teoria sistemico-relazionale, della teoria dinamica dei sistemi; la prospettiva *life span*; “la visione biografica” della psicopatologia in adolescenza.

Ma come è cambiata la funzione educativa dei genitori nella dimensione digitale in cui si trovano a vivere gli adolescenti?¹¹⁷

Secondo Laurence Steinberg¹¹⁸, uno dei più importanti esperti di adolescenza al mondo, i genitori di figli adolescenti devono essere 1) affettuosi, 2) risoluti, 3) incoraggianti nei confronti delle loro potenzialità.

Sembra ovvio, eppure la parola educare deriva dal latino *ex duco*, “tirare fuori”, ossia estrarre le capacità innate dei figli, far evolvere la loro autostima secondo le loro propensioni naturali per farne degli adulti felici.

Don Bosco diceva che la migliore educazione è data dall'esempio, eppure le figure genitoriali durante l'adolescenza non sono sufficienti: occorre che alcune funzioni educative siano svolte dai c.d. terzi, ossia il gruppo dei pari, che rappresenta la nascita sociale dell'adolescente e il contesto scolastico, definito come “ambiente

¹¹⁴ P. CARBONE, “Adolescenza e disagio”, 2001.

¹¹⁵ M. BENASOYAG, filosofo e psicanalista di origine argentina, in “La tirannia dell'Algoritmo”, 2020, afferma che siamo marionette in mano ai *coach* e agli *smartphone*, che occorre una visione modulare dell'uomo, con il recupero dell'*agency*, la possibilità di iniziare un'azione accesa dall'interno; critica la tirannia degli algoritmi, riflessione sull'espulsione del conflitto o la confusione esiziale tra desideri generativi e voglie seriali del niente; v. le sue opere “La responsabilità della rivolta”, una riflessione critica in relazione alla pandemia, come anche “Cinque lezioni di complessità”, 2020, in dialogo con Teodoro Cohen, parla della pandemia come di un “attraversamento sfibrante”, è un'esperienza del trauma prolungato e anche di una trasformazione che ci riguarda tutti, continuiamo a confondere la complessità con la linearità dell'Antropocene, il futuro è una virtualità del presente, la sfida dell'atto, “clinica del legame e legame del comune”, parla degli effetti psicologici della pandemia come depressione di massa: “Deleuze diceva che la tristezza è reazionaria, sembra un ammonimento troppo severo, ma lo diceva pensando a Spinoza quando avvertiva sulla perdita della capacità di agire non facendo lavorare la gioia”. Tra le sue opere, “L'epoca delle passioni tristi”, 2004 con G. SCHIMT, “Il cervello aumentato, l'uomo diminuito”, 2016.

¹¹⁶ P. JEAMMET, “Psicopatologia dell'adolescenza”, 2019.

¹¹⁷ V. L. RINALDI, “Sul nascere madri e padri. L'abisso, le sue insidie e le sue possibilità”, 2019.

¹¹⁸ L. STEINBERG, “Age of opportunity: Lessons from the New Science of Adolescence”, 2015; “You and your adolescent”, 2011; “The 10 Basic principles of Good parenting”, 2005; “Adolescence”, 2010.

mentalizzante”, dove la *doxa* diventa *episteme* e *trust*, ossia fiducia nella comunità. Nell’era post-moderna, definita liquida con la crisi dei valori e la crisi della trasmissione dei saperi, la scuola insegna il *valore del limite* e *della regola* tendente ad evitare una società adolescentizzata e una precoce adultizzazione.

Ma il potere invasivo e pervasivo dei *social* mette a dura prova tale processo c.d. di *contenimento*. Pensiamo al fenomeno del c.d. “*vamping*”: molti ragazzi restano connessi tutta la notte senza orari e regole, con un decremento potenziale delle loro capacità cognitive e del loro rendimento scolastico, acquisendo molte informazioni, ma poca “conoscenza”.

Secondo Federico Toniani, psichiatra del Policlinico Gemelli, che ha creato un primo ambulatorio in Italia per la dipendenza da internet e dal cellulare, davanti allo schermo il bambino e l’adolescente perde il c.d. “*rispecchiamento emotivo*”. Si perde, cioè, la capacità di attendere e la capacità di restare da solo. È il fenomeno degli *Hikikomori*: l’iperconnessione è una nuova normalità, un nuovo modo di affrontare le sfide della crescita oppure un segnale di una dipendenza patologica, diffusa a livello pandemico tra le nuove generazioni?

Il Dott. Lancini¹¹⁹ ha approfondito il c.d. *Internet addiction disorder*, attraverso un suo inquadramento nosografico, spiegandone le cause e le metodiche di analisi. L’adolescenza è il punto di snodo della traiettoria evolutiva, del processo della “soggettivazione”: il ruolo della mente adulta che dovrebbe fungere da guida è svolto dallo strumento digitale, che può incidere in modo negativo sul bambino e sull’adolescente in un periodo in cui la neuroplasticità del cervello è massima. Si pensi al caso *Tik Tok* dello scorso 21 gennaio 2021: gli organi di informazione riportarono la notizia del decesso di una bambina di 10 anni a Palermo, avvenuto in relazione ad un gioco definito “*black challenge*” condiviso sulla suddetta piattaforma. Tale triste avvenimento ha confermato, purtroppo, in maniera tragica, l’assenza di controlli sull’età degli utenti e sulla pericolosità dei contenuti veicolati tramite *social network*¹²⁰.

¹¹⁹ Psicologo, psicoterapeuta, Presidente della Fondazione Minotauro di Milano, docente presso il Dipartimento di psicologia dell’Università di Milano-Bicocca, autore di numerose pubblicazioni sull’adolescenza, le più recenti: “*Adolescenti navigati, Come sostenere la crescita dei nativi digitali*” (Erickson, 2015); “*Abbiamo bisogno di genitori autorevoli. Aiutare gli adolescenti a diventare adulti*” (Mondadori, 2017); “*Il ritiro sociale negli adolescenti. La solitudine di una generazione iperconnessa*” (Raffaello Cortina, 2019), “*Cosa serve ai nostri ragazzi. I nuovi adolescenti spiegati ai genitori, agli insegnanti, agli adulti*” (Utet, 2020).

¹²⁰ Sul tema della privacy, della gestione dei dati personali e della sicurezza, si pensi anche al recente “caso Alexa”, che ha visto coinvolti l’assistente vocale di Amazon e una bambina di appena 10 anni: lo strumento di IA, probabilmente per un errore di programmazione, ha suggerito alla bambina di mettere una moneta in una presa elettrica. La vicenda, raccontata dalla madre su *Twitter*, mette in luce i limiti degli strumenti di IA: l’assistente vocale, alla richiesta della bambina di proporle una sfida, ha ricercato e trovato sul web una sfida ai limiti della follia. Questo è il messaggio che Alexa ha dato alla bambina: «*Secondo ourcommunitynow.com la sfida è semplice: collegare un caricatore del telefono a metà in una presa a muro, quindi toccare con un centesimo i poli esposti*». L’azienda

Per la prima volta, il Garante per la Privacy italiano ha attivato la procedura di urgenza, ai sensi dell'art. 66 del GDPR, in applicazione del criterio del *local case*, derogatoria rispetto al meccanismo di cooperazione, di coerenza e del principio dell'*one stop shop*, pretendendo da parte di Tik Tok con sede legale in Irlanda di introdurre, come sistema di blocco dell'account, un algoritmo denominato "*age verification*", che consente di impedire l'accesso alla piattaforma i minori di anni 14¹²¹.

Occorre ricordare che il Considerando 38 del GDPR stabilisce che i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti. Per tali ragioni, l'art. 8 del GDPR è da considerarsi una disposizione speciale che prevede, come ipotesi privilegiata per il trattamento dei dati dei minori in relazione ai servizi dell'informazione, il consenso, stabilendo che questo possa considerarsi lecito, ove sia stato prestato o autorizzato dal titolare della responsabilità genitoriale, ovvero il minore abbia almeno 16 anni, limite ridotto a 14 anni dall'art. 2-quinquies del Codice della Privacy, D.lgs. 101/2018.

L'individuazione dell'età minima, ai sensi dell'art. 8 del GDPR, in Italia fissato a 14 anni, rispetto ai 16 del GDPR dall'art. 2-quinquies del codice privacy, in attuazione della clausola di flessibilità introdotta dall'art. 8, par.1, ultimo capoverso, integra una tipica ipotesi di legislazione nazionale derogatoria ai principi stabiliti dal Regolamento. Come autorevole dottrina ha avuto modo di osservare¹²², l'art. 8 del Regolamento, ispirato al Coppa statunitense, nel prevedere una disciplina specifica sul trattamento dei dati personali dei minori d'età, lungi dal rendere più agevole la sottoscrizione di

produttrice del dispositivo *Echo* ha da subito dichiarato di voler sistemare il problema, per evitare che cose del genere possano accadere in futuro. La sfida era spopolata su *Tik Tok* all'inizio del 2020, ed era stata successivamente bandita per ovvi motivi. Il problema degli assistenti vocali e degli strumenti di IA in generale è quello relativo al "*buon senso*", elemento che troppo spesso manca, come è venuto in rilievo in questo caso che risale a dicembre 2021. Secondo il ricercatore *Mayank Kejriwal*, della *University of Southern California*, il traguardo è possibile ma «*estremamente impegnativo*», in quanto «*il buon senso delle macchine è un problema di intelligenza artificiale dei nostri tempi, che richiede collaborazioni concertate tra le istituzioni per molto tempo*». Un esempio di ciò è il programma quadriennale "*Machine Common Sense*" lanciato nel 2019 dall'Agenzia per i progetti di ricerca avanzata della difesa degli Stati Uniti. Sono molti i progetti di ricerca finanziati da questo programma.

¹²¹ In merito al procedimento di *consistency and cooperation*, si segnala l'articolo di GAETANA NATALE, "*La Grande Sezione della Corte di Giustizia si è pronunciata sui poteri delle Autorità Nazionali nell'ambito del RGDP a fronte della gestione dei dati da parte dei colossi del web (C. giust. UE, Grande Sezione, sentenza 15 giugno 2021, C-645/19)*", pubblicato sulla Rassegna dell'Avvocatura dello Stato Gennaio-Marzo 2021, pag. 39.

¹²² A. ASTONE, "*L'accesso dei minori d'età ai servizi della c.d. "società dell'informazione": l'art. 8 del Reg (UE) 2016/679 e i suoi riflessi*", in *Contratto e Impresa*, 2019, 2, 614; G. BIANCHEDI, "*Il consenso dei minori per i servizi della società dell'informazione sotto il profilo giuridico e informatico*", in *Cyberspazio e diritto*, vol. 20, n. 63 (3-2019), pp. 389-413.

servizi *online*, ha colmato un vuoto di tutela per coloro i quali sono tra i maggiori fruitori dei servizi della c.d. *ICT society*, ma anche tra le maggiori vittime.

La disciplina dell'art. 8 è di primaria importanza, non solo perché il consenso (espresso, libero, specifico, informato ed inequivocabile) diventa l'unica valida base giuridica per il trattamento dei dati dei minori, ma anche per la correlata speciale disciplina accordata ai minori dall'art. 17, par.1, lett. f), in tema di diritto alla cancellazione ed all'oblio.

Ma oggi, possiamo dire che il consenso prestato da un quattordicenne che naviga per ore in internet sia veramente libero da subdoli condizionamenti?

Il codice civile ci parla, all'art. 1426 c.c.¹²³, di *malitia supplet aetatem*, ma oggi nella dimensione digitale sono i continui *input* e immagini di internet a costituire il concetto di “*malitia*”, intesa come artifici e raggiri che incidono sulla capacità di discernimento del minore.

I concetti di capacità giuridica e di capacità di agire non sono delineati nei sistemi di *common law*, che parlano di *legal capacity*, prescindendo dai concetti di soggettività, centro autonomo di imputazione di effetti giuridici, e di capacità giuridica.

L'età è graduata in relazione agli atti da compiere: pertanto, per i c.d. *necessaries*, atti di acquisto minori per i beni necessari di modico valore, il minore è considerato pienamente capace di stipulare contratti validi.

Fino a che punto, però, il minore può essere considerato in grado di capire cosa sta operando con un click sul computer: egli dovrebbe essere istruito e formato per accedere al computer o allo *smartphone*, che è una vera e propria finestra sul mondo: senza un'adeguata formazione sui pericoli occulti è come se si desse ad un minore una macchina da guidare senza avergli dato la patente.

Ricordiamo che il filosofo *Karl Popper*, il campione della società aperta e libera, chiedeva, ancor prima che si sviluppasse la c.d. *infosfera*, che soltanto pochi potessero andare in tv, muniti di una patente ottenuta dopo speciali esami. Già allora si dibatteva molto sull'influenza degenerativa della televisione, sulla passività di chi se ne sta seduto, catatonico, davanti al magico schermo.

Ma erano tutte opinioni arbitrarie, nulla di scientifico basato sul test di *Stroop*, test elaborato negli anni '30 dallo psicologo statunitense Ridley Stroop, tuttora utilizzato per verificare con il riconoscimento di parole e colori il funzionamento corretto del cervello.

Adesso uno studio della prestigiosa Johns Hopkins University di Baltimora è lapidario: «*Per ogni ora e quaranta minuti di visione è come se il cervello fosse un anno più vecchio. Le cause: sedentarietà e passività. Al contrario, il movimento contrasta questo processo di invecchiamento*», così dice l'autore principale della ricerca, Ryan Dougherty. Chi da giovane guarda più televisione, si troverà con meno materia grigia

¹²³ Art. 1426 c.c.: “*Il contratto non è annullabile, se il minore ha con raggiri occultato la sua minore età; ma la semplice dichiarazione da lui fatta di essere maggiorenne non è di ostacolo all'impugnazione del contratto*”.

da adulto, e proprio in quelle aree cognitive-corteccia frontale e corteccia entorinale del cervello, responsabili dei processi più importanti. Il rapporto causale tra esposizione alla tv e diminuzione di “cellule grigie” è stato stabilito in virtù di esami di risonanza magnetica su 599 soggetti seguiti per 25 anni, i quali, all’inizio dell’esperimento, avevano un’età media di 30 anni. Stiamo parlando, dunque, di uno studio molto importante e rigoroso.

Alcune delle cause della diminuzione del volume cerebrale sembrano essere solo indirettamente legate alla tv, ad esempio la sedentarietà.

Secondo Dougherty, gli studi dimostrano che chi fa attività fisica mantiene il volume cerebrale invariato anche con l’avanzare degli anni. E addirittura alcuni studi mettono in rapporto una vita sedentaria a un maggior rischio di sviluppare l’Alzheimer.

Il problema della sedentarietà sembra essere collegato a un deterioramento cardiovascolare e dunque a un minor afflusso di sangue al cervello, che provoca una minore ossigenazione neuronale, che, per così dire, fa gradualmente appassire il cervello stesso.

Non tutte queste nuove attività (non tutte le sedentarietà) sono uguali: in particolare deleterie sono, come la televisione, quelle in cui il soggetto subisce passivamente il messaggio, o meglio, un abbondante flusso di informazioni che lo bersagliano senza dargli possibilità di interagire, a differenza di altre attività come le parole crociate, gli scacchi o la lettura. Ma poiché la televisione oggi sta sempre più diventando un accessorio superfluo, superato dagli *smartphone* e dai *tablet*, e la classica programmazione televisiva è sostituita da fruizioni molto diverse, come lo *streaming* e, soprattutto, ci sono i *social*, che sono il nuovo punto dolente della comunicazione di massa, che accade al cervello in tutte queste nuove attività?

Su questo, lo studio americano non ci sa dare una risposta, tranne che, anch’esse, sono attività sedentarie e quindi, a rischio. Ma per sapere se usare Instagram o Facebook, almeno sul piano scientifico, sia cognitivamente dannoso, bisognerà forse aspettare altri 25 anni.

Noi, però, sulla base di quello che vediamo attorno, e anche di quanto personalmente ci riguarda, un’ipotesi l’avanziamo: i *social network*, tutti, nessuno escluso, sono di gran lunga peggiori della televisione, almeno dal punto di vista della salute mentale dei loro fruitori. In confronto, gli effetti inebetenti della tv sono di gran lunga meno pericolosi.

Basti pensare al fenomeno dei suicidi, alle “*challenge*”, le sfide *social*, il “*cutting*”, ossia l’invito all’autolesionismo, o i veri e propri linciaggi attuati su queste piattaforme, da cui la vittima, se ne esce, resterà profondamente segnata¹²⁴.

¹²⁴ Sul tema del pericoloso rapporto tra digitale e minori, si veda anche M. MARTORANA, “*Minori sui social: educiamoli per difenderli*”, su agendadigitale.eu, che ci mette in guardia sulla necessità di

Solo in piccola parte i *social* sono comunicazione, in larga parte sono esibizionismo, vanità, *merchandising* e sfoghi aggressivi. Senza considerare i c.d. *hype*, distopie e montature giornalistiche che alterano la realtà e le informazioni.

In questa dimensione, dominata da “atopia e anomia”, come afferma il Professore Natalino Irti, occorre integrare la biosfera con l’*infosfera*: il Professor Floridi, partendo dalla distinzione *on-line* e *off-line*, ha coniato il termine *Onlife*, neologismo che sta ad indicare la necessità di collegare la nostra conoscenza alla dimensione della vita reale con l’introduzione dei filtri del nostro senso critico. Ma tale senso critico e capacità di riflessione sono duramente messi sotto attacco da nuovi espedienti ingannatori della tecnologia, che rubano i nostri dati e la nostra identità digitale senza una nostra vera e propria consapevolezza.

Si pensi al fenomeno del c.d. “*Flubot*”: è uno *spyware*, ovvero un *software* che, a nostra insaputa, può essere installato sullo *smartphone* per rubare password e altri dati riservati. *Flubot* invia un banale messaggio di testo che notifica, ad esempio, il ritardo di una consegna da parte di aziende di trasporto. L’utente legge il messaggio ed inconsapevolmente consente l’accesso ai propri dati riservati.

Certamente la tecnologia non ha solo aspetti negativi, può assicurare livelli di sicurezza. Si pensi all’utilità della *Blockchain*¹²⁵: un registro decentrato in forma digitale basato su un linguaggio crittografico *hash* e in grado di contenere una serie infinita di dati. Esso è composto da più blocchi, legati l’uno all’altro, nei quali sono registrate le informazioni, distribuiti all’interno da una rete composta da più nodi.

Una volta registrati, tali blocchi non sono più modificabili senza invalidare l’intera struttura e sono così costantemente controllati da tutti i nodi della rete. Questo significa

agire contro i pericoli del digitale, prima che con la legge, con l’educazione dei minori a scuola e in casa.

¹²⁵ W. NONNIS, “*Blockchain, il suo contributo durante la pandemia*”, in www.blockchain4innovation.it, 19 aprile 2021; A. BELLO, “*Blockchain e privacy: soluzioni per la compliance alle norme*”, 15 maggio 2019, in agendadigitale.eu; M. IASELLI, “*Blockchain e privacy, bisogna lavorare ancora molto*”, in federprivacy.org, luglio 2020; N. BOLDRINI, “*Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati*”, in blockchain4innovation.it, 2018; V. PORTALE, “*Quanto è legale la Blockchain? La compatibilità tra Blockchain e normativa GDPR*”, in www.blog.osservatori.net, 31 luglio 2020; A. GAMBINO, C. BOMPRESZI, “*Blockchain e titolare del trattamento dei dati personali: il nodo rimane irrisolto*”, in www.iaic.it, 20 gennaio 2020; D. MARCIANO, G. CAPACCIOLI, “*La blockchain ed il problema del trattamento dei dati personali*”, in www.affidaty.io, 4 giugno 2019; R. BATTAGLINI, M. GIORDANO (a cura di), “*Blockchain e smart contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche*”, 2019; M. BELLINI, “*La blockchain per le imprese. Come prepararsi alla nuova «internet del valore»*”, 2019; A. BASILE, “*Blockchain: La Nuova Rivoluzione Industriale*”, 2019.

che una *blockchain* garantisce un livello di sicurezza e trasparenza assoluta assicurando, ad esempio, che una transazione sia sempre tracciabile.

Si pensi alla tutela del diritto d'autore tramite *blockchain* (c.d. *tokenizzazione*), cioè la conversione dei diritti di un bene in un *token* digitale delle varie identità degli autori che verranno poi associate alle varie opere mediante database contenenti tutti i dati registrate dalla SIAE, c.d. NFT, “*non fungible token*”.

Viene in rilievo, in questi esempi, il concetto di “*sicurezza funzionale*” della tecnologia. Il sociologo tedesco Ulrich Deck parlava della “società del rischio”, *Risikogesellschaft, cultura dell'incertezza e rischio residuale*: tale dimensione del rischio è dovuta all'accelerazione tecnologica che stiamo vivendo, non solo sotto il profilo sanzionatorio, ma anche sotto il profilo culturale. Di qui l'importanza delle Autorità regolatorie, quali arbitri che non devono indicare soluzioni, ma valutare la correttezza di quelle adottate nel rispetto del principio dell'*accountability*.

La Commissione Europea sollecita gli Stati membri non con regole, ma con obiettivi nella regolamentazione delle piattaforme digitali, cercando di affermare uno “*standard europeo regolatorio*” per la definizione del nuovo “capitalismo digitale”, basato *in primis* sulla c.d. “igiene informatica e informativa”.

La sicurezza delle piattaforme poggia essenzialmente sul controllo dei dati e sulla loro trasparenza, in una configurazione preliminare e predefinita: è il concetto di *privacy by design* e *by default*. Non una privacy per la privacy, ma la protezione dei dati come nuovo paradigma e nuovo asset per uno sviluppo tecnologico sostenibile, teso al rispetto della persona umana che vada aldilà della figura dei *followers*.

Il Professore Franco Pizzetti¹²⁶ affermava che le Autorità regolatorie hanno il compito di affiancare e sollecitare i governi nell'adottare nuove politiche digitali per raggiungere gli obiettivi europei. Più di recente, il Professore Oreste Pollicino¹²⁷ ha affermato che «*la nuova sfida non è solo la tutela dei diritti fondamentali, ma la governance dei dati, non solo di quelli personali e il loro riutilizzo per i software di intelligenza artificiale*».

La proposta di regolamento sull'intelligenza artificiale presentata lo scorso 21 Aprile 2021 dalla Commissione ha, infatti, distinto 4 livelli di rischio:

- 1) *Unacceptable risk* (ad esempio, quelli relativi ai dati biometrici per i quali si esclude l'applicazione dell'intelligenza artificiale);

¹²⁶ F. PIZZETTI, “*Intelligenza artificiale, protezione dei dati personali e regolazione*”, cit.; ID., “*Privacy e il diritto europeo alla protezione dei dati personali. dalla direttiva 95/46 al nuovo Regolamento europeo*”, 2016; ID., “*Protezione dei dati personali in Italia tra GDPR e codice novellato*”, 2021.

¹²⁷ O. POLLICINO, “*Diritto dell'informazione e dei media*”, 2019; ID., “*Parole e potere. Libertà di espressione, hate speech e fake news*”, 2017; ID., “*Codice della comunicazione digitale*”, 2015.

- 2) *High risk* (si ammette l'IA con opportune cautele);
- 3) *Limited risk* (AI systems with specific transparency obligations);
- 4) *Minimal risk*.

Tale proposta non prevede, però, la questione della responsabilità civile che, come annunciato dalla Commissione su Agenda Digitale, sarà oggetto di un testo diverso e separato che dovrebbe essere presentato all'inizio dell'anno 2022.

Si tratta di un altro fondamentale tassello nel percorso verso una “*trustworthy AI*”, ossia un'intelligenza artificiale che generi fiducia negli utenti.

Ci vorranno 2 anni per approvare il testo definitivo e altri 2 anni prima che diventi operativo. Visti gli enormi interessi in gioco, che toccano tutti i settori industriali ed economici, non solo le *big tech*, non sarà un confronto facile. Il fatto che poi stiamo parlando di norme che andranno a regolare un qualcosa che per sua natura è in continua evoluzione, rende la sfida ancora più difficile.

Si pensi alle società che utilizzano i sistemi di riconoscimento facciale, operando il c.d. *scraping* di dati in rete, ovvero automatizzando l'attività di raccolta di dati anche biometrici: riescono a stoccare nei loro *database* i volti di cittadini anche senza il loro consenso, assegnando ad ogni volto un *hash*.

Tali società creano dei veri e propri archivi di dati biometrici, che, per esempio, in America vengono utilizzati dalle forze dell'ordine per individuare i criminali, anche se alcuni dipartimenti come quello di Los Angeles ne hanno sospeso l'utilizzo, poiché si realizza una forma di sorveglianza elettronica massiva ed invasiva.

Si pensi ancora alla pratica di “*Sim swapping*”, una tecnica di attacco che consente di avere accesso al numero di telefono del legittimo proprietario e violare determinate tipologie di servizio *online* che usano il numero di telefono come sistema di autenticazione.

Alcune piattaforme, come Google, si stanno organizzando per evidenziare i c.d. “*Privacy Labels*”, ossia le etichette della privacy che permetteranno agli utenti di conoscere in dettaglio i dati utilizzati dalle app pubblicate su *Playstore*.

Nei sistemi aziendali alcuni *vendor* introducono nelle infrastrutture iperconvergenti anche sistemi *embedded* di *backup* e *disaster recovery*, garantendo il miglioramento della protezione dei dati e il minimo rischio di perdita dei dati stessi.

Ciò avviene grazie all'incorporazione di tecnologie di rilevamento della corruzione dati e *self-healing*, che agiscono durante l'operatività standard e nelle fasi di *back-up* automatizzato.

Per il raggiungimento di tali obiettivi il *preemptive-remedy*, ossia il rimedio preventivo, trova un suo completamento nel potere sanzionatorio delle Autorità regolatorie tenuto conto dei principi di effettività, proporzionalità e dissuasività delle sanzioni. A tal riguardo, si è posta la questione del rapporto tra il consenso ed il legittimo interesse

quale base giuridica del trattamento dei dati. L'Opinion WP29 n. 6/2004 ha escluso che il legittimo interesse ex art. 6, par. 1, lett. f)¹²⁸ possa surrogare il consenso espresso, libero ed inequivocabile sul proprio trattamento dei dati.

Il consenso assume ancora più importanza in relazione alla prospettiva del futuro non troppo lontano dei c.d. “*Computer quantistici*”.

La *Mit Technology Review*, di recente, ha messo in evidenza i rischi di chi oggi raccoglie dati sensibili anche crittografati, dunque, di fatto, al momento inservibili perché blindati, ma con la speranza di poterli sfruttare e decrittare in futuro. Come? Adoperando l'enorme potenza di calcolo dei “computer quantistici” che lavorano in modo ben diverso da quelli attuali con ogni *bit* quantistico (o *qubit*)¹²⁹ in grado di assumere diversi valori nello stesso momento, e, dunque, moltiplicare il potere computazionale¹³⁰.

¹²⁸ Art. 6 GDPR (Liceità del trattamento): “1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.”

¹²⁹ Se le informazioni memorizzate nei computer “normali” sono assimilabili a una lunga sequenza di zero e uno, i *bit*, nella meccanica quantistica le informazioni sono memorizzate in bit quantistici, i c.d. *qubit*, che assomigliano di più a un'onda piuttosto che a una serie di valori discreti. Quando i fisici vogliono rappresentare con precisione le informazioni contenute nei *qubit*, usano quindi le funzioni d'onda. Di recente, un gruppo di fisici dell'Università di Bonn e del Technion – Israel Institute of Technology hanno effettuato un esperimento per capire quali fattori determinano la velocità con cui un computer quantistico può eseguire i suoi calcoli, e sono stati testati i limiti di velocità dei computer quantistici, ossia il limite di Mandelstam-Tamm e quello di Margolus-Levitin, che mettono in relazione la velocità massima di evoluzione di uno stato con l'incertezza energetica del sistema e l'energia media. I risultati dello studio sono pubblicati sulla rivista *Science Advances*. V. <https://www.media.inaf.it/2021/12/30/limiti-computer-quantistici/>.

¹³⁰ Secondo Erminio Polito Minsait, responsabile *Energy & Utilities* di Minsait in Italia, l'utilizzo del *Quantum Computing*, ossia del calcolo quantistico, potrebbe fare la differenza anche nel settore dell'energia, riducendo i tempi di elaborazione delle scelte strategiche e migliorando la *performance* degli algoritmi predittivi. È stato affermato che «da un lato, l'aumento esponenziale della potenza di calcolo offerto dai computer quantistici sarà cruciale per la costruzione di un nuovo orizzonte

La complessità dei computer quantistici potrebbe renderli molto più rapidi per certi compiti, consentendo loro di risolvere problemi oggi impossibili da sciogliere¹³¹.

In questa classe di problemi c'è anche la capacità di scardinare gli algoritmi che al momento utilizziamo per proteggere *database* e *server farm* che custodiscono informazioni personali, segreti di Stato o importanti brevetti commerciali¹³².

energetico basato su ecosistemi collaborativi gestiti in una logica “platform-based”, dall’altro, anche le tecnologie già in uso nei sistemi energetici più avanzati, come IoT, Intelligenza Artificiale e Blockchain, ne trarranno beneficio. Vi sono però vantaggi più immediati, come quelli che può offrire attualmente al trading di energia dove avere a disposizione una tecnologia quantistica rappresenta un miglioramento decisivo in termini di velocità delle transazioni». Adottando il calcolo quantistico, dunque, si potrà prevedere con maggiore accuratezza il rendimento della rete elettrica in un dato momento, così da migliorarne la produzione, anche per una maggiore sostenibilità ambientale. Per quanto riguarda il settore della *cybersecurity*, Minsait ha sostenuto che «ad oggi, non esistono computer quantistici in grado di mettere a repentaglio la sicurezza della crittografia tradizionale, tuttavia, ci sono già le prime opportunità di business per prepararsi per un futuro di decrittazione quantistica: il potenziale dell’informatica quantistica non decreterà la fine della crittografia, bensì un cambiamento nelle pratiche come, ad esempio, chiavi crittografiche più lunghe e complesse. In un futuro con milioni di transazioni energetiche decentralizzate, simultanee e certificate tramite smart contract e blockchain, la crittografia quantistica sarà un pilastro centrale del nuovo sistema».

¹³¹ È recente la notizia relativa alla sperimentazione dei c.d. cristalli temporali, strutture peculiari che si ripetono regolarmente nel tempo invece che nello spazio, teorizzati dai fisici negli ultimi anni e spiegati dalle leggi della meccanica quantistica. Come noto, i cristalli classici sono strutture solide, composte da atomi, molecole o ioni, che per definizione hanno una disposizione geometrica definita e che si ripetono nelle tre dimensioni spaziali. La recente notizia – che viene da un team dell’università di Stanford, di Oxford e del Max Planck Institute, insieme con Google Quantum AI Lab – riguarda, invece, il caso dei cristalli temporali, in cui la regolarità si manifesta e si dispiega nel tempo. Se l’ipotesi teorica era stata avanzata nel 2012 ad opera del fisico premio Nobel Franck Wilczek, docente al Mit, il primo esperimento in laboratorio è avvenuto nel 2017, ed oggi gli scienziati hanno trasformato un gruppo di *qubit* in un cristallo temporale, mediante l’uso del computer quantistico di Google Sycamore: i risultati dell’esperimento sono stati pubblicati sulla rivista *Nature*. Si tratta di strutture diverse, che si modificano costantemente nel tempo e poi tornano sempre periodicamente nella configurazione iniziale. Sono catene di atomi che pulsano in assenza di energia, restando in movimento nel tempo senza richiedere l’azione di una forza esterna, la cui resistenza li rende interessanti per lo sviluppo dei potentissimi computer quantistici. In una recente sperimentazione pubblicata sulla rivista *Science*, gli scienziati sono riusciti a tenere in vita per alcuni secondi i cristalli temporali ottenuti utilizzando i *qubit*. Queste catene di *qubit* hanno di fatto dimostrato di avere una simmetria temporale (e non spaziale, come i cristalli classici), riprodotta durante tutta la sperimentazione. Il fisico V. Khemani dell’Università di Stanford ha commentato così l’esperimento: «I cristalli temporali sono un esempio lampante di un nuovo tipo di fase quantistica della materia al non-equilibrio». La ricerca sul tema, d’altronde, sta crescendo rapidamente, come dimostrano anche i recenti studi del 2021 sulle riviste *Physical Review Letters* e *Physical Review B*.

¹³² Si parla sempre più spesso del Metaverso, tuttavia è necessario anche chiedersi se le aziende dispongono effettivamente delle capacità computazionali necessarie e in generale dell’*hardware* di cui ci sarà bisogno. Sappiamo che il metaverso di Zuckerberg sarà una specie di mondo 3D in cui ogni utente assumerà le sembianze di un *avatar* che, riproducendolo voce e movimenti della persona fisica, potrà interagire in tempo reale con altre persone dal salotto di casa. Secondo Raja Koduri, *senior vice president* e *general manager* del team di Intel (Computing Systems and Graphics Group) una rete del genere necessiterà di un livello computazionale molto alto e di un’infrastruttura

hardware/software che dovrà essere almeno 1000 volte più potente di quella disponibile oggi (es. *petaflop*, una potenza computazionale che dovrà essere disponibile in pochi 10 millisecondi per un uso in tempo reale). Non sarà facile digitalizzare caratteristiche come la pelle, le funzionalità vocali, il movimento delle persone, elementi che vanno inseriti in un dispositivo con sensori indossato dagli utenti. Secondo *Koduri* serve una banda molto larga con una latenza bassissima, che gli odierni *server* del *cloud computing* non posseggono, per cui è difficile che il sistema possa funzionare. Se si pensa a “*Second Life*”, “*Roblox*” e simili, già creati ed utilizzati, essi sono molto lontani dal vero metaverso. Comunque, *Intel* sta lavorando seriamente a questo fine e in un comunicato stampa ha fatto presente che, tramite una “*roadmap multigenerazionale*”, vuole processare dati provenienti dal *client* e diretti verso il *cloud* con un’elaborazione *zettascale*. Lo *zettascale computing* si riferisce ai supercomputer che permettono prestazioni nell’ordine degli *zettaflop*. Uno *zettaflop* è uguale a circa un sestilione di operazioni in virgola mobile al secondo. Un sistema *zettaflop* può generare una marea di dati in virgola mobile in un secondo. Secondo gli scienziati dobbiamo aspettare il 2035 per avere un sistema *zettascale* perfettamente funzionante, e prima di arrivare ad un Metaverso completamente funzionante devono passare tanti altri anni. Ci sarà bisogno anche di algoritmi specializzati, di una nuova architettura (che *Intel* ha denominato *Xe*) e di nuovi *software*, tutto comunque alla nostra portata secondo *Koduri*. V. <https://notiziescientifiche.it/metaverso-serviranno-potenza-computazionale-enorme-e-decenni-di-sviluppo/>; <https://www.punto-informatico.it/intel-potenza-di-calcolo-1000-volte-maggiore-per-il-metaverso/>.

VIII Capitolo

Strumenti normativi regolatori e prospettive future nella dimensione euro-unitaria e in quella nazionale.

La Commissione Europea ha cercato di attivarsi per sviluppare un'attività regolatoria c.d. di contenimento: il 15 dicembre 2020, al fine di regolamentare i mercati digitali, ha presentato due proposte di Regolamento che compongono il c.d. “*Digital Markets Package*”: il *Digital Services Act* e il *Digital Markets Act*.

Il primo modifica alcune disposizioni dell'attuale Direttiva *e-commerce*, regolamentando il regime di responsabilità delle piattaforme digitali.

Il secondo, invece, introduce in capo ai c.d. “*gatekeeper*” – ossia le piattaforme che controllano l'accesso ai mercati digitali – una serie di obblighi volti a rendere i mercati digitali più equi e contendibili, arginando la tendenza alla creazione di monopoli, nei servizi o nella distribuzione, a cui si assiste oggi attraverso una procedura di “*inspection*” degli algoritmi.

A completare il quadro delle nuove proposte legislative contribuiscono la bozza di Regolamento sull'Intelligenza Artificiale, nonché la proposta di Regolamento *e-Privacy* che andrà a regolare specificamente la protezione dei dati nelle comunicazioni elettroniche; il Regolamento 2018/1807 sui dati non personali e la Direttiva NIS per la cybersecurity (“*Network and Information Security*”), recepita nel nostro ordinamento attraverso il decreto legislativo 18 maggio 2018, n. 65 (anche detto “decreto legislativo NIS”), in vigore dal 24 giugno 2018; la nuova direttiva SMAV del 2018, sui servizi media audiovisivi.

Di recente, anche l'ONU ha pubblicato un *report* sull'intelligenza artificiale, mettendo in guardia sui pericoli insiti nell'utilizzo di dati biometrici.

In Italia, sono state intraprese alcune iniziative, indotte dalla rilevanza sociale di alcuni fenomeni. Ad esempio, in contrasto al fenomeno del c.d. “*revenge porn*”, il c.d. “Decreto Capienze” (D.l. n. 139 dell'8 ottobre 2021, convertito in legge 3 dicembre 2021, n. 205) ha introdotto il nuovo art. 144-bis al Codice Privacy, con il quale si riconosce alle vittime la possibilità di godere di una tutela anticipata, rivolgendosi al Garante mediante reclamo o segnalazione, affinché questo intervenga, esercitando i poteri di cui gode ai sensi dell'art. 58 GDPR, nell'ipotesi in cui sussista il fondato timore che possa essere commessa una delle condotte descritte dall'art. 612-ter c.p., ossia la diffusione di contenuti sessualmente espliciti non realizzati a tale scopo.

Si veda, in particolare, l'art. 9 del “decreto capienze”, che, se da un lato ha creato scalpore per quanto concerne l'adottata riduzione di alcuni poteri del Garante per la privacy, dall'altro ha, come accennato, introdotto disposizioni nuove e necessarie in tema di *revenge porn*.

Per quanto concerne la prima questione, l'art. 9, co. 1, lett. b) del Decreto abroga interamente l'articolo 2-quinquiesdecies del Codice Privacy, il quale stabiliva che “*con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante*

può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare". In sostanza, dunque, la norma ha espunto dal Codice una disposizione che imponeva alla P.A. di consultare il Garante prima di porre in essere trattamenti ad alto rischio – come quelli relativi ai dati sanitari – nell'interesse pubblico affinché potesse intervenire a tutela del soggetto interessato.

Il testo dell'art. 9, significativamente modificato in sede di conversione del decreto-legge nel corso dell'esame in Senato, reca disposizioni in materia di protezione dei dati personali.

In particolare, il comma 1 novella il Codice della privacy (d.lgs. n. 196 del 2003):

- prevedendo che il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico possa trovare fondamento e base giuridica, oltre che nella legge e – nei casi previsti dalla legge – nel regolamento, anche in un atto amministrativo generale (modifica dell'art. 2-ter del Codice) e che tale ampliamento della base giuridica valga anche per il trattamento dei dati particolari (sanità pubblica, medicina del lavoro, archiviazione nel pubblico interesse o per ricerca scientifica o storica o a fini statistici) disciplinato dall'art. 2-sexies del Codice e per il trattamento dei dati personali per fini di sicurezza nazionale o difesa, disciplinato dall'art. 58 del Codice;

- consentendo il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri, da parte di una serie di soggetti pubblici, anche per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuiti ai suddetti soggetti pubblici (nuovo comma 1-bis dell'art. 2-ter del Codice);

- introducendo una disciplina specifica per il trattamento di dati personali relativi alla salute quando gli stessi siano "privi di elementi identificativi diretti" (art. 2-sexies, comma 1-bis, del Codice);

- abrogando l'articolo 2-quinquiesdecies del Codice della privacy che, nel caso di trattamenti di dati personali svolti per l'esecuzione di un compito di interesse pubblico, tali da poter presentare un rischio elevato per i diritti e le libertà delle persone fisiche, consentiva al Garante di adottare d'ufficio provvedimenti di carattere generale, prescriventi misure e accorgimenti a garanzia dell'interessato;

- prevedendo che il trattamento dei dati relativi al traffico telefonico e telematico che devono essere conservati dal fornitore per finalità di accertamento e repressione di reati, sia effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante con provvedimento "di carattere generale" (modifica dell'art. 132, comma 5, del Codice);

- potenziando la competenza del Garante al fine di prevenire la diffusione di materiali, foto o video, sessualmente espliciti (nuovo art. 144-bis del Codice, rubricato *Revenge porn*). In particolare, la disposizione prevede che chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che immagini, audio, video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati

a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali, senza il suo consenso, può rivolgersi, mediante segnalazione, al Garante, il quale, entro 48 ore può rivolgere avvertimenti, ammonimenti, imporre una limitazione provvisoria o definitiva al trattamento, ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e infliggere una sanzione amministrativa pecuniaria. In base al comma 6 dell'art. 9, i fornitori di servizi di condivisione di contenuti, ovunque stabiliti, devono entro 6 mesi dalla legge di conversione pubblicare il proprio recapito, ai fini dell'adozione dei provvedimenti da parte del Garante;

- intervenendo sul parere che il Garante deve rendere al legislatore in vista dell'adozione di una disciplina relativa al trattamento dei dati, per circoscriverne i presupposti (modifica dell'art. 154 del Codice). Inoltre, quando il Presidente del Consiglio dei ministri dichiara che ragioni di urgenza non consentono la consultazione preventiva, e comunque nei casi di adozione di decreti-legge, si prevede che il Garante esprima il parere in una fase successiva, vale a dire in sede di esame parlamentare dei disegni di legge o delle leggi di conversione dei decreti-legge o in sede di vaglio definitivo degli schemi di decreto legislativo sottoposti al parere delle Commissioni parlamentari;

- consentendo l'omissione della previa notifica della violazione contestata nei confronti dei soggetti pubblici che trattano i dati quando il loro trattamento abbia già arrecato pregiudizio agli interessati (modifica dell'art. 166 del Codice);

- introducendo la possibilità di applicare, a titolo di sanzione accessoria rispetto alle sanzioni amministrative pecuniarie comminate dal Garante, l'ingiunzione a realizzare campagne di comunicazione istituzionale di sensibilizzazione sulla protezione dei dati personali (modifica dell'art. 166 del Codice);

- subordinando l'applicazione della fattispecie penale di inosservanza di provvedimenti del Garante (punita con la reclusione da tre mesi a due anni) al "concreto nocumento" dei soggetti interessati e alla querela della persona offesa (modifica all'art. 170 del Codice).

Il comma 2 si pone come disposizione di coordinamento, conseguente all'abrogazione dell'articolo 2-quinquiesdecies del Codice della privacy.

Il comma 3 modifica il d.lgs. n. 51 del 2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, per:

- confermare l'estensione agli atti amministrativi generali della base giuridica del trattamento;

- sostituire, nella determinazione dei termini, delle modalità di conservazione, dei soggetti legittimati ad accedere ai dati nonché delle modalità e delle condizioni per l'esercizio dei diritti dell'interessato, l'attuale riferimento a un regolamento governativo con quello a un decreto ministeriale;

-circoscrivere, anche in questo caso, l'applicabilità del reato di inosservanza dei provvedimenti del Garante, alle ipotesi di concreto nocumento arrecato ad uno o più interessati e alla presentazione di querela della persona offesa.

Il comma 4 interviene sull'art. 7 del decreto-legge n. 34 del 2020 per modificare ed integrare la disciplina concernente il trattamento di dati personali da parte del Ministero della salute. Tale disciplina, nella versione vigente, concerne i dati personali – anche relativi alla salute degli assistiti – raccolti nei sistemi informativi del Servizio sanitario nazionale ed autorizza il suddetto Ministero al relativo trattamento, al fine di sviluppare metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione, demandando ad un decreto di natura regolamentare del Ministro della salute – adottato previo parere del Garante per la protezione dei dati personali – la definizione delle norme attuative. Le novelle in esame prevedono che il decreto sia invece di natura non regolamentare – fermo restando il parere del suddetto Garante –, estendono, con riferimento a dati personali non sanitari, l'ambito delle norme di rango legislativo in esame e del relativo decreto attuativo e pongono una norma transitoria, valida nelle more dell'emanazione del medesimo decreto.

Il comma 5 introduce disposizioni di coordinamento relative alla previsione che ha esteso agli atti amministrativi generali la base giuridica del trattamento dati (v. sopra).

Il comma 7 riduce a 30 giorni il termine per i pareri che il Garante renda su atti riconducibili al Piano nazionale di ripresa e resilienza (PNRR), al Piano nazionale per gli investimenti complementari ed al Piano nazionale integrato per l'energia e il clima 2030 e prevede che quel termine sia improrogabile (ed una volta decorso, si può comunque procedere, pur in assenza di parere).

Il comma 8 interviene sugli articoli 1 e 2 della legge n. 5 del 2018, al fine di prevedere che i diritti dell'utente iscritto al registro pubblico delle opposizioni, nonché gli obblighi in capo agli operatori di call center operino indipendentemente dalle modalità in cui il trattamento delle numerazioni è stato effettuato, ovvero con o senza operatore con l'impiego del telefono, ma anche in via più generale mediante sistemi automatizzati di chiamata senza l'intervento di un operatore.

I commi da 9 a 12 prevedono una sospensione (eccezion fatta per la prevenzione e la repressione dei reati) della installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte di autorità pubbliche o soggetti privati. Tale moratoria è prevista “fino all'entrata in vigore di una disciplina legislativa della materia”, e comunque non oltre il 31 dicembre 2023.

In ambito parlamentare si riscontra sensibilità verso il fenomeno del c.d. “*hate speech*”. Sebbene nel nostro ordinamento manchi ancora una legge *ad hoc* per i discorsi d'odio, diverse proposte sono giunte in discussione alle Camere. Le due più rilevanti sono il DDL Cirinnà e il DDL Boldrini, presentato lo scorso anno.

Il Governo ha, inoltre, recentemente adottato il decreto legislativo 4 novembre 2021, n. 170, pubblicato il 25 novembre scorso, di attuazione della Direttiva 771/2019. Il decreto disciplina alcuni aspetti dei contratti per la fornitura di servizi digitali,

introducendo nuove disposizioni nel Codice del Consumo¹³³, estendendo la tutela fornita da quest'ultimo anche ai contratti in cui professionista si obbliga a fornire un servizio o un contenuto digitale a fronte non della corresponsione di un prezzo, ma della cessione di dati personali da parte del consumatore. Il decreto interviene, dunque, sul dibattuto tema della patrimonializzazione e commercializzazione, c.d. monetizzazione dei dati personali, sempre più rilevante nell'economia moderna. Sotto altro profilo, ricordiamo che, in precedenza, con l'art. 8 ter del d.l. 135/2018 (c.d. Decreto Semplificazioni 2019), aggiunto in sede di conversione in legge, è stata introdotta nel nostro ordinamento la definizione di *tecnologie basate su registri distribuiti* (o *blockchain*) e di *smart contract*.

Dalle linee evolutive della normativa si intravede la necessità di conciliare la digitalizzazione ed il concetto di interoperabilità dei sistemi con la tutela dei dati. Le nuove Linee Guida dell'Agid, con i relativi protocolli informatici ed il sistema *Cloud PA*¹³⁴, cercano di rispondere a tale esigenza secondo le indicazioni della Commissione Europea. Il 2 dicembre 2020, infatti, quest'ultima, in materia di giustizia, ha pubblicato la Comunicazione *Digitalisation of Justice in the in the European Union, A tool box of opportunities* (COM (2020)710) e documento di accompagnamento (JWD (2020) 540), indicando le nuove linee di azione a cui attenersi: *digital transformation e design dei processi*. La Commissione ha affermato che *“La Giustizia è una delle componenti strategiche per una società basata sui valori UE e per un'economia resiliente”*.

Nel settore della giustizia, così come in altri settori come la sanità, a scuola, i trasporti, prerequisito della digitalizzazione (che è un concetto diverso dall'informatizzazione,

¹³³ Il decreto legislativo modifica gli articoli da 128 a 135 del Codice del Consumo (introducendo anche gli artt. da 135-bis a 135-septies) ed entrerà in vigore il 1° gennaio 2022. Le modifiche concernono la vendita di beni tra il venditore e il consumatore, che non viene più limitata ai beni di consumo. Vengono inserite le nozioni di *“bene con elementi digitali”* e di *“aggiornamento dei beni digitali”*. Il Capo I del Titolo III, che prima era dedicato alla vendita di beni di consumo, è ora dedicato alla vendita di beni *tout court*, tra cui rientrano anche i beni con elementi digitali; parallelamente viene ampliata la nozione di venditore, che ora comprende anche il *“fornitore di piattaforme se agisce per finalità che rientrano nel quadro della sua attività e quale controparte contrattuale del consumatore per la fornitura di contenuto digitale o di servizi digitali”*. Vengono inserite anche le definizioni dei contenuti digitali, del servizio digitale, della compatibilità, interoperabilità e del supporto durevole. Per quanto riguarda i contratti di fornitura di contenuti digitali o di servizi digitali, le nuove disposizioni vengono applicate ai contenuti digitali o ai servizi digitali incorporati o interconnessi con beni. Vengono previsti a carico del venditore appositi obblighi con riferimento agli aggiornamenti nel caso di beni con elementi digitali, con conseguente precisa responsabilità ex art. 133; il venditore è responsabile per ogni vizio di conformità del bene esistente al momento della consegna e che si manifesta entro due anni. Tuttavia, per quanto riguarda i beni con elementi digitali, vi è una possibile estensione della responsabilità nel caso in cui il contratto preveda la fornitura continuativa del contenuto digitale per più di due anni.

¹³⁴ *“Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici”* e *“Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni”*, pubblicate in data 22 ottobre 2021 sul sito dell'Agid.

anzi una sua evoluzione, un suo salto quantico), è la re-ingegnerizzazione dei processi e del *design* dei sistemi di supporto, tenendo a mente le esigenze dei cittadini e delle imprese. La Commissione ha riscontrato diversi *Tool IT*, ma senza alcuna considerazione sulla interoperabilità. Quest'ultima rappresenta l'indice evolutivo dello sviluppo tecnologico per ottimizzare le risorse pubbliche: il passaggio dall'informatizzazione alla digitalizzazione si basa sulle c.d. "infrastrutture iperconvergenti", rappresentate da componenti *hardware* estremamente "modulari". La caratterizzazione delle architetture si deve al *layer software*, grazie al quale le risorse di *computing e storage* di ogni nodo sono combinate in un *pool* unico e messe a disposizione con i vantaggi dell'elasticità e della scalabilità. Significative sono risultate le proposte della Commissione per i tool IT di cooperazione giudiziaria *cross-border*.

Piattaforme di comunicazione e scambi di dati, registri interconnessi dovrebbero essere una realtà già consolidata, ma sono poco sfruttati. *Eurlex*, il portale *E-justice*, il sistema *Business Registers Interconnection System* (BRIS), il sistema ECLI (per la identificazione dei *case law* e della minima base di metadati), il sistema *E-Codex*, sistemi che facilitano l'accesso *cross-border* alle informazioni giudiziarie da parte dell'autorità e dei privati e anche quelli che facilitano la cooperazione giudiziaria dovranno diventare i "*gold standard*", con un punto di accesso unico ad una rete europea.

Ma cosa succede se lo scambio di dati deve avvenire con Paesi non europei? L'*European Data Protection Board*, la Commissione che riunisce le Autorità di Protezione dei dati personali nazionali che operano in tutta Europa, lo scorso anno ha lanciato una consultazione pubblica su uno schema di provvedimento che aveva un unico obiettivo dichiarato: quello di identificare rimedi e soluzioni, oltre alle attuali "*general clauses*" capaci di garantire il trasferimento dei dati personali dall'Europa agli Stati Uniti. Dopo la sentenza della Corte di Giustizia C-311/2018, ormai nota come *Schrems II*, i giudici di Lussemburgo hanno dichiarato a tal fine invalido il c.d. *Privacy Shield*, erigendo, così di fatto, un muro giuridico difficilmente penetrabile tra Europa e Stati Uniti in fatto di trasferimento di dati personali.

La partecipazione alla consultazione pubblica da parte di tutti gli *stakeholder* pubblici e privati è preziosa, perché il trasferimento dei dati non è solo con gli USA, ma anche con altri paesi non europei.

La Corte di Giustizia dell'Unione Europea, con la sentenza *Schrems II*, ha accertato che le leggi americane non riconoscono agli interessati un livello di tutela equivalente rispetto a quello loro riconosciuti dalla disciplina europea in materia di protezione dei dati personali.

Il *draft* di provvedimento posto in consultazione non supera la considerazione che occorre un intervento normativo che allinei gli ordinamenti.

I rimedi contrattuali o tecnologici da soli non risolvono il problema. È necessario che la diplomazia europea e statunitense si mettano alla ricerca di una soluzione più

definitiva attraverso uno strumento pattizio capace di garantire con sicurezza la libera circolazione dei dati.

Si pensi al caso della disciplina FATCA¹³⁵ (*Foreign Account Tax Compliance Act*), che, come noto, è nata come disciplina unilaterale statunitense, salvo poi acquisire reciprocità sostanziale tramite i vari accordi intergovernativi sottoscritti *ad hoc* dai vari Paesi che intendono aderire alla disciplina.

L'Italia vi ha aderito tramite l'"Iga" (accordo del gennaio 2014), che ha dato attuazione al FATCA traducendo la disciplina in uno scambio automatico annuale di informazioni tra le autorità fiscali dei due Paesi che interessa non più esclusivamente i cittadini statunitensi ma anche i conti correnti e assimilati detenuti in territorio statunitense da residenti italiani.

Ebbene, la disciplina FATCA ha un impatto non solamente in ambito fiscale, ma incide gravemente anche sulle procedure di gestione interna dei dati (personali e finanziari). Infatti, gli istituti bancari devono monitorare tutti i rapporti finanziari riconducibili a persone fisiche ed enti fiscalmente residenti negli USA. L'elemento di maggiore impatto è, dunque, che gli istituti finanziari dell'Unione europea sono tenuti a divulgare informazioni, anche dettagliate, relative ai conti detenuti da presunti cittadini statunitensi. Evidente il problema che si pone nell'ambito della materia della protezione dei dati personali.

Tra le questioni di maggiore rilevanza possiamo menzionare, da un lato, la posizione dei c.d. "*Accidentals Americans*"¹³⁶, cittadini europei che, a causa degli elevati *compliance costs* connessi al FATCA, si sono visti negare l'accesso a servizi bancari essenziali nell'UE, con conseguente violazione della direttiva sui conti di pagamento (direttiva 2014/92/UE) e della Carta dei diritti fondamentali dell'UE¹³⁷; e dall'altro l'intervento del GDPR, entrato in vigore nel 2018, che riguarda i dati *online* di ogni tipo e si applica anche allo scambio automatico di informazioni in ambito fiscale, andando a bilanciare il diritto dei cittadini alla protezione dei dati personali nei confronti del preminente interesse degli Stati alla tutela del fisco.

¹³⁵ Il FATCA (*Foreign Account Tax Compliance Act*) è un accordo sottoscritto da Italia e Stati Uniti che prevede lo scambio di informazioni finanziarie per contrastare l'evasione fiscale internazionale, in particolare quella relativa a cittadini e residenti statunitensi attraverso conti correnti detenuti presso le istituzioni finanziarie italiane e quella relativa a residenti italiani tramite conti correnti presso le istituzioni finanziarie statunitensi. Le comunicazioni dei dati avvengono tra l'Agenzia delle Entrate e l'IRS statunitense, che nel 2016 hanno sottoscritto un accordo, concludendo così l'implementazione della normativa FATCA.

¹³⁶ Sono i c.d. "*americani accidentali*", o americani "per caso", perché nati negli Stati Uniti o perché sposati con una statunitense, che, anche se non vivono negli Usa, sono tenuti a rispettare tutti gli obblighi dei cittadini del Paese, compreso quello di pagare le tasse; vi rientrano anche i cittadini con doppia cittadinanza europea/statunitense e i loro familiari non statunitensi.

¹³⁷ Vedi, già nel 2018, l'interrogazione parlamentare del parlamento europeo sugli effetti negativi della normativa statunitense "*Foreign Tax Compliance Act*" (FATCA) sui cittadini dell'UE e in particolare sugli "*americani casuali*", https://www.europarl.europa.eu/doceo/document/O-8-2018-000053_IT.html.

In particolare, il GDPR prevede che la trasmissione dei rilevanti dati personali dalla UE a stati terzi, come gli USA, possa avvenire solo se questi ultimi garantiscono un livello di sicurezza equivalente a quello previsto nell'Unione europea dal GDPR. Purtroppo, però, gli accordi tra gli Stati dell'Unione europea e gli Usa non operano in maniera effettiva sulla base del principio di reciprocità: gli Stati Uniti non trasmettono in Europa dati equivalenti, cosicché il sistema multilaterale che era stato inizialmente previsto dall'Ue e dagli Usa sta entrando in crisi¹³⁸.

Si è reso, quindi, necessario un intervento da parte dell'Unione europea, affinché siano modificati o riavviati agli accordi che prevedono lo scambio di informazioni tra UE e Stati Uniti, per (ri)stabilire una vera simmetria nel trasferimento dei dati tra USA e UE. Il rischio paventato è quello di una possibile attuazione della c.d. *blocking legislation*, ossia una disciplina che, nelle more di una ridefinizione degli accordi attuativi dei FATCA, non permetterebbe la trasmissione dei dati oltreoceano fintantoché la reciprocità e le tutele del GDPR non vengano ristabilite.

Nel frattempo, l'utilizzo delle Clausole generali (c.d. "*clausole standardizzate approvate dalla Commissione Europea*") utilizzate da organizzazioni che aderiscono a programmi internazionali di protezione dati, è probabilmente è l'unico modo attuale per il trasferimento dei dati dall'Europa agli Stati Uniti.

Pertanto, le clausole contrattuali che garantiscono adeguate garanzie di protezione dei dati possono essere utilizzate come base per il trasferimento di dati e informazioni dall'Unione europea a paesi terzi, sebbene la Corte Europea abbia chiarito che l'autorità di controllo di ciascuno Stato membro è tenuta a sospendere o vietare il trasferimento di dati personali a un Paese extra UE quando, a causa di circostanze specifiche, si presume che le clausole stesse non siano, o non possano essere rispettate in quel Paese, e che la protezione dei dati trasferiti, prevista dal diritto dell'Unione, non possa essere garantita.

Inoltre, l'esportatore europeo di dati personali e l'importatore extra UE, sono obbligati ad effettuare le proprie valutazioni sui singoli trasferimenti esistenti entro le clausole standardizzate, e la possibilità di trasferire dati personali sulla base delle clausole contrattuali tipo dipenderà dal risultato della valutazione effettuata dall'esportatore sulle garanzie offerte nel paese importatore (in particolare, gli USA), nel rispetto dell'adequazione della tutela e del principio di proporzionalità. Inoltre, il loro utilizzo deve essere supportato anche dalla collaborazione diplomatica per preservare le relazioni tra i due Paesi.

Anche il Comitato europeo per la protezione dei dati, nelle sue FAQs relative al caso Schrems II¹³⁹, ha riconosciuto espressamente che le clausole contrattuali standardizzate

¹³⁸ C. GARBARINO, "Applicazione del FATCA a livello europeo e protezione dei dati", 2018, in https://privatebank.jpmorgan.com/content/dam/jpm-wm-aem/documents/JPM%20Wealth%20Journal_Article_2019-04_Applicazione%20del%20FATCA.pdf.

¹³⁹ Vedi "Privacy Shield: le FAQ dell'EDPB sulla sentenza Schrems II", tradotte dal Garante della Privacy, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9442415>.

possono ancora essere considerate strumenti adeguati, se sono incluse misure aggiuntive per proteggere il trasferimento dei dati.

È stato affermato che: *“Il Comitato europeo per la protezione dei dati sta attualmente analizzando la sentenza della Corte per determinare il tipo di misure supplementari che potrebbero essere fornite in aggiunta alle clausole contrattuali tipo, siano esse misure legali, tecniche o organizzative, per trasferire dati a paesi terzi in cui le clausole standardizzate non forniranno da sole il livello sufficiente di garanzie. Il Comitato sta esaminando ulteriormente in cosa potrebbero consistere queste misure supplementari e fornirà ulteriori indicazioni”*¹⁴⁰.

Comunque, nel caso dei contribuenti, la trasmissione dei dati non deve eccedere la finalità fiscale (c.d. “limitazione delle finalità”), deve essere adeguata, pertinente e limitata a quanto necessario rispetto alle finalità per le quali i dati sono trattati (c.d. “minimizzazione dei dati”)¹⁴¹. Se le richiamate garanzie non verranno rispettate, ci sarà il rischio che in Europa si possa propendere per la creazione di vere e proprie “*black list*” di Stati extra-UE che non garantiscono la tutela della privacy dei cittadini europei, e ciò avrà inevitabili conseguenze sul piano degli scambi e dei commerci internazionali.

Come si è visto, i problemi e i temi sono molto trasversali: si sono spesso sovrapposte delle competenze in materia di supervisione e controllo attribuite alle diverse Autorità all’interno del nostro ordinamento, con difficoltà nell’attuazione della disciplina, e ciò potrebbe determinare un impatto negativo sull’efficacia delle misure adottate.

Servirebbe maggiore chiarezza nel riparto delle competenze: si potrebbero usare meglio le risorse e l’applicazione della disciplina sarebbe più sicura.

Nonostante il problema sia noto, non è ancora stato intrapreso un indirizzo per una soluzione unanime. Intanto, allora, si procede con una collaborazione fra le Autorità esistenti, ma non si esclude, in futuro, la nascita di un’unica Autorità con tutte le competenze necessarie.

¹⁴⁰ Si vedano le clausole contrattuali standard aggiornate ai sensi del GDPR emesse il 4 giugno 2021 dalla Commissione per i trasferimenti di dati da titolari o responsabili del trattamento nell’UE/SEE (o altrimenti soggetti al GDPR) a titolari o responsabili del trattamento stabiliti al di fuori dell’UE/SEE (e non soggetti al GDPR): queste clausole modernizzate sostituiranno i tre insiemi di clausole contrattuali tipo adottate ai sensi della precedente Direttiva sulla protezione dei dati 95/46.

¹⁴¹ Per quanto riguarda il *trade-off* tra privacy e interesse pubblico, è utile menzionare la recente giurisprudenza della Corte EDU, che nella sentenza 36345/16 del 12 gennaio 2021 nel caso L.B. v. HUNGARY, ha mostrato una certa apertura verso una “deroga” ai principi in materia di privacy in nome dell’interesse pubblico, contestando che in alcuni casi la privacy non può divenire un ostacolo al controllo fiscale. La Corte ha contraddetto il Garante della privacy ungherese, affermando che è ammissibile la pubblicazione sul sito dell’autorità fiscale dei dati dei contribuenti che non hanno pagato le tasse. Secondo la Corte, in un’opera di bilanciamento degli interessi, la riservatezza di questi dati (nome, indirizzo, morosità fiscali) può cedere il passo all’interesse pubblico alla trasparenza sull’affidabilità economica delle persone: prevale la considerazione che chi non adempie agli obblighi fiscali costituisce una minaccia per gli interessi di chi potrebbe entrarvi in contatto per stringere rapporti commerciali.

Le nuove proposte di Regolamento presentate dalla Commissione europea si limitano ad incoraggiare la collaborazione fra le Autorità esistenti, ed è rimesso agli Stati membri l'onere di disciplinare le modalità concrete.

Il problema non è solamente teorico, in quanto ha effetto sull'effettività della disciplina e sull'efficacia della tutela che l'ordinamento intende garantire ai soggetti coinvolti.

I dubbi in materia, nonché la concorrenza fra le diverse Autorità, incidono negativamente sull'applicazione della disciplina, inficiandone la portata.

Il lavoro delle autorità dovrebbe essere sinergico già nella fase di indagine e analisi dei problemi, vista la complessità delle fattispecie che emergono.

Si faccia l'esempio dell'Indagine conoscitiva sui *Big Data*¹⁴², che è stata condotta insieme da Antitrust, AGCOM e Garante della Privacy, ed è stata pubblicata nel 2018: si tratta di un caso in cui, unendo le diverse prospettive, le Autorità sono riuscite ad avere un quadro completo del fenomeno che dovevano affrontare.

Il problema sta, poi, nella fase di implementazione delle misure, perché si crea una situazione di confusione, per la quale più Autorità rivendicano la propria competenza, e così si rischia di pregiudicare i soggetti che chiedono la tutela prevista dall'ordinamento.

Per fare un altro esempio pratico, si pensi alla Direttiva SMAV: con riferimento alle nuove disposizioni poste a tutela dei minori potrebbero sorgere problemi, perché si prevede che, per evitare la fruizione da parte di questi di contenuti pericolosi per il loro sviluppo fisico, mentale o morale, i fornitori di servizi media audiovisivi siano soggetti a misure introdotte dai singoli Stati (es. meccanismi volti a verificare l'età di chi accede ai servizi). Eppure, resta fermo che i dati personali dei minori, così raccolti, non possono essere trattati a fini commerciali, né per finalità di *marketing* diretto, profilazione o pubblicità mirata sulla base dei comportamenti.

Il problema è palese: si devono riunire tutte le competenze dell'AGCOM, dell'AGCM e del Garante della Privacy.

L'Autorità Garante delle Comunicazioni deve vigilare sui servizi media audiovisivi, in particolare sulle piattaforme di condivisione video (anche *social media*).

Per quanto concerne il rinvio al *marketing* e alla pubblicità, questo richiede una tutela dei consumatori, con conseguente competenza dell'Antitrust.

Infine, il Garante della Privacy è necessario per la raccolta di dati personali, interventi già avvenuti per il controllo dell'età dei soggetti che accedono ai *social*, in risposta ai gravissimi episodi avvenuti su *Tik Tok*.

Il *Digital Services Act*, dal canto suo, si limita a prevedere l'istituzione dei c.d. “coordinatori nazionali per i servizi digitali”, cioè autorità nazionali competenti per il

¹⁴² Il testo dell'indagine conoscitiva è accessibile da <https://www.garanteprivacy.it/documents/10160/0/Indagine+conoscitiva+sui+Big+Data.pdf/58490808-c024-bf04-7e4e-e953b3d38a9a?version=1.0>. Interessante, sul punto, G. BUSIA, L. FEROLA, “Il Garante per la protezione dei dati personali: le funzioni, i rapporti con le altre Istituzioni ed Autorità in Italia e in Europa”, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), “Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive”, Aracne, 2016.

controllo e l'attuazione della disciplina. Sicuramente tali poteri potrebbero essere attribuiti all'AGCOM, ma è solo una delle tante possibilità.

Anche le altre Autorità, infatti, potrebbero rivendicare i poteri previsti dal DSA, specialmente perché il Regolamento esplicitamente prevede la possibilità di designare contestualmente più soggetti competenti.

Oppure, si potrebbe istituire un'Autorità *ex novo*.

Ancora, auspicabilmente, si potrebbe optare per l'accorpamento delle diverse Autorità, riunificando le competenze di quelle già esistenti.

Ad ogni modo, sui singoli Stati incombe l'onere di determinare quali compiti siano attribuiti a ciascuna Autorità e le modalità di cooperazione fra le une e le altre.

Si vedano le osservazioni formulate dell'EPDS nell'*Opinion 1/2021*: data la trasversalità delle attività oggetto della regolamentazione, è quasi scontato che vi sarà la concorrenza di più autorità, soprattutto di quelle responsabili per la protezione dei dati personali, poiché queste vengono in rilievo ogni volta in cui le attività includano l'utilizzo di dati personali. Per questo motivo, il Comitato spera che la versione definitiva del Regolamento individui un criterio legale sul quale basare la cooperazione, strutturi la cooperazione fra le diverse Autorità e precisi con chiarezza le Autorità coinvolte nella cooperazione e le circostanze che prevedono tale cooperazione.

Per quanto concerne il *Digital Markets Act*, si richiamano ipotesi di concorrenza di diverse Autorità: diverse norme hanno ad oggetto lo sfruttamento dei dati personali da parte dei “gatekeepers”, ossia dei soggetti destinatari della disciplina, preannunciando il possibile intervento del Garante, oltre all'ovvia competenza dell'Antitrust.

L'art. 32 della proposta prevede anche la creazione di un comitato consultivo per assistere la Commissione nello svolgimento delle funzioni. Su questo elemento si è pronunciato l'EDPS con l'*Opinion 2/2021*¹⁴³, secondo cui i membri dell'EDPB dovrebbero prendere parte a tale comitato consultivo e bisognerebbe strutturare al meglio la cooperazione fra le diverse Autorità competenti potenzialmente coinvolte (indicando la base giuridica idonea a giustificare lo scambio di informazioni fra le stesse).

Si può affermare, in conclusione, che il quadro normativo vigente e le prospettive di riforma non sono rassicuranti per lo scopo qui analizzato: è, tuttavia, un elemento importante, per cui servirebbe, il prima possibile, riorganizzare il sistema¹⁴⁴.

¹⁴³ Accessibile da https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.

¹⁴⁴ In conclusione, sul tema dei rischi che la condivisione dei dati così come regolata nelle nuove proposte EU (DGA, DSA, DMA), può far correre agli interessati, minacciando in tal modo di violare proprio il GDPR, si veda il commento dell'ex Garante della Privacy, F. PIZZETTI, “La nuova era digitale europea ha un problema privacy, bene EDPB-EDPS” su *agendadigitale.eu*, in cui si mette in luce l'importanza del parere dell'EDPB e dell'EDPS sulle proposte regolatorie della Commissione contenute nel DGA, nel DMA e nel DSA, parere reso pubblico il 18 novembre 2021 sul sito del Garante privacy italiano.

Capitolo IX

Servizio civile digitale

Si parla di “*servizio civile digitale*” per indicare l’utilizzo del digitale nello svolgimento di attività di interesse pubblico. Il servizio civile digitale è teso, ad esempio, a combattere fenomeni devianti come quelli multiformi della corruzione.

Per citare un’applicazione concreta, di recente si è proceduto alla c.d. Robustezza di piattaforme per le segnalazioni di *whistleblowing* al Responsabile della prevenzione, corruzione e trasparenza. Il portale utilizza un protocollo di crittografia in grado di garantire la riservatezza dell’identità del segnalante, del contenuto della segnalazione e della documentazione allegata. È curioso che, alla notevole attenzione sociale e politica, non corrisponda una proporzionale densità di casistica giurisprudenziale.

I fenomeni in questione sembrano restare al di fuori della dimensione giudiziaria. Storicamente, in un primo tempo, l’esplosione del mondo digitale è avvenuta per gran parte addirittura al di fuori della stessa dimensione giuridica; talvolta in un vero e proprio far west. Oggi, questo non è più vero ma le regole del gioco sembrano applicarsi con molta difficoltà.

Su un fronte, quello delle piattaforme *social*, sono queste stesse a dettare le regole e, almeno in parte o nelle intenzioni, costituiscono anche gli organi di giustizia. Sull’altro fronte, del c.d. “*marketing digitale*”, l’economia *data driven* sembra sottrarsi ad ogni regola, fatta eccezione per la disciplina della protezione dei dati personali, che sembra atteggiarsi talvolta ad ultima barriera ad una incontrollata libertà di azione.

Il principale presidio di legalità è rappresentato dalle autorità garanti.

Nelle pronunce del Garante della privacy (GPDP) si riscontra una particolare attenzione alla tutela dei dati personali nel processo in corso di costruzione dell’interoperabilità digitale basata sulle cd porte di dominio API, cercando di individuare sempre il titolare del trattamento, come centro di imputazione della responsabilità.

È attiva l’Autorità garante della concorrenza e del mercato (AGCM), con riguardo alla protezione dei consumatori dei servizi digitali, sia nei confronti delle piattaforme *social*, sia con riguardo alle nuove dinamiche di promozione e pubblicità commerciale. L’Autorità garante delle comunicazioni (AGCOM) è particolarmente attenta, naturalmente, ai profili della comunicazione digitale, con particolare riguardo per le campagne di odio e di denigrazione.

Va, peraltro, riscontrato che il riparto di competenze fra le diverse Autorità rappresenta un profilo sempre più incerto, data la trasversalità dei temi affrontati.

È, comunque, utile analizzare il quadro generale delle questioni verso le quali queste hanno maggiormente posto la propria attenzione, anche nel tentativo di comprendere quali problemi siano maggiormente rilevanti, prevedendo anche quali tematiche potrebbero arrivare nelle aule dei tribunali.

Il GPDP, ad esempio, si è pronunciato sulla necessità di rimuovere alcuni contenuti dai *social media*, nel caso di coinvolgimento di soggetti minori o di episodi che integrassero il reato di diffamazione.

L'AGCM ha, invece, toccato ampiamente il tema delle pubblicità *online*, soprattutto con riguardo all'attività svolta dagli *influencer*, incrociando la propria attività all'introduzione di nuove regole – anche e soprattutto a livello europeo – volte a disciplinarne il comportamento. Parallelamente, vi è un'attività cospicua nel settore della tutela dei marchi, legata ai nuovi rischi di contraffazione e non solo sorti con l'avvento dell'economia digitale¹⁴⁵.

L'AGCOM, infine, ha rivendicato su più fronti l'importanza del proprio ruolo, anche tenendo conto delle modifiche che saranno apportate dal recepimento della nuova Direttiva SMAV (Servizi Media AudioVisivi), che qualifica i servizi di *video-sharing* come *media*, facendo rientrare il controllo sui contenuti condivisi attraverso questi strumenti entro l'ambito di competenza dell'Autorità.

Tornando a quanto detto prima in merito alla sempre maggiore sovrapposizione dell'ambito di intervento delle Autorità, può evidenziarsi una certa affinità fra alcune delle tematiche affrontate dall'AGCOM e dall'AGCM, con ad esempio per quanto riguarda appunto l'attività pubblicitaria e di sponsorizzazione portata avanti dagli *influencer*.

La bassa densità di pronunce giudiziali è un indice significativo della inadeguatezza degli attuali strumenti giudiziali con riguardo a fenomeni caratterizzati dalla estrema rapidità e frequenza delle condotte; e da una notevole varietà degli effetti.

Tuttavia, è per certi versi paradossale o comunque un segno dei tempi, che – mentre l'economia e le dinamiche sociali sono caratterizzate sempre più dalla digitalizzazione – la domanda di giustizia che deriva da queste dinamiche non trova risposte adeguate in ambito giudiziario.

¹⁴⁵ Tra i soggetti pubblici capaci di arginare lo strapotere delle piattaforme, l'Antitrust ha sempre svolto un ruolo fondamentale. Si pensi anche alle ultime vicende che hanno visto coinvolta la società fondata da Jeff Bezos. L'AGCM ha irrogato una sanzione di oltre 1 miliardo di euro ad Amazon per abuso di posizione dominante. La multa inflitta riguarda i comportamenti discriminatori posti in essere da Amazon nei confronti dei venditori che non si affidano alla sua logistica: praticamente il colosso americano ha creato un canale preferenziale per i commercianti che seguono le sue scelte logistiche (es. aderire a creare un negozio virtuale sul suo sito) ed ha dato preferenza agli acquirenti *Prime* a maggior capacità di spesa. L'azienda fondata da Jeff Bezos avrebbe sfruttato queste dinamiche per condizionare il mercato in termini distorsivi. L'azione è stata promossa per violazione dell'art. 102 del TFUE che, come noto, vieta “*lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo*”. Siccome durante il lockdown l'Italia è stata una delle nazioni dove Amazon è cresciuta di più (il 75% degli italiani ha fatto acquisti *online*), l'impresa ne ha approfittato per aumentare non solo le vendite di beni materiali, ma anche per collezionare dati e creare profilazioni dei consumatori (le merci sono uno strumento per arrivare ai dati degli utenti), crescendo sul mercato a un prezzo e con modalità che ne hanno distorto il meccanismo, penalizzando i concorrenti incapaci di stare al passo. Le conseguenze e gli effetti della sua posizione dominante hanno portato l'Antitrust italiana ad agire. Qui il testo del provvedimento: https://www.agcm.it/dotcmsdoc/allegati-news/A528_chiusura%20istruttoria.pdf.

Il *deficit* di offerta di tutela è da imputare in primo luogo alla lentezza dei tempi delle decisioni, platealmente non sincronizzata alla velocità degli accadimenti; in secondo luogo, all'assenza di giudici specializzati; infine, ma non per importanza, all'assenza di strumenti di intervento efficaci e tempestivi.

Non è un caso che i casi che sono stati più frequentemente portati all'attenzione dei giudici riguardano il diritto all'oblio o alla cancellazione dei dati, dopo un tempo rilevante; o, più di recente, la cosiddetta “eredità digitale”, ossia l'accesso dei familiari alle informazioni di un defunto nella disponibilità di una piattaforma digitale. Insomma, casi in cui la rapidità dell'intervento non è essenziale.

Nell'era digitale cambia il concetto di proprietà: Rebecca Mardon, dell'Università di Cardiff¹⁴⁶, ha scritto che oggi la proprietà è sostituita dall'accesso, “*età dell'accesso*”, in cui la proprietà non è più importante per i consumatori e diventerà presto irrilevante. Gli ultimi anni hanno visto l'emergere di una serie di modelli basati sull'accesso nel regno digitale”.

In uno studio realizzato nel 2018 dalla *Norton School of Family and Consumer Sciences* dell'Università della Arizona, è emerso il concetto di proprietà psicologica che applichiamo ad un bene digitale che, in realtà, non ci appartiene.

Ecco così che trasformiamo la *non-proprietà* di un bene digitale in *percezione di possesso*. Una percezione di proprietà che risponde principalmente a 3 fattori: la sensazione di avere il controllo sull'oggetto che si possiede, il ruolo che l'oggetto assume per definire chi siamo, l'aiuto che l'oggetto ci fornisce per migliorare il senso di appartenenza nella società.

Il punto è che comprando un bene digitale – sia *ebook*, come un brano musicale o un film – in realtà otteniamo una licenza di utilizzo con restrizioni più o meno ampie.

Non entriamo in possesso del bene come accade per i beni fisici. Non a caso, ci sono esempi di utenti che si sono trovati privati della possibilità di utilizzo di beni digitali, come nel caso di Microsoft che ha deciso di chiudere il suo servizio di *ebook*, portandosi dietro tutte le librerie dei clienti (anche se promettendo loro un rimborso).

Il mondo digitale presenta nuove minacce alla proprietà a cui i nostri beni fisici non ci hanno preparato. Si parla di regolare il “*patrimonio digitale*” e la c.d. “*successione digitale*”, distinguendo beni digitali (c.d. *digital assets*) a contenuto patrimoniale, come *Bitcoin*, basata su tecnologia *blockchain* e beni a contenuto non patrimoniale, che dovrebbero essere esclusi da una successione ereditaria, ma così non è¹⁴⁷.

Rientrano nella delazione ereditaria le opere creative dell'ingegno nell'ambito del digitale come i *software*, ma è anche l'account che può avere un valore patrimoniale spesso rilevante. La patrimonialità dell'account può derivare dal contenuto, come nel

¹⁴⁶ R. MARDON, “*The relationship between ownership and possession: observations from the context of digital virtual goods*”, 2016.

¹⁴⁷ G. MARINO, “*La successione digitale*”, in *Oss. dir. civ. e comm.*, 2018; A. MAGNANI, “*L'eredità digitale*”, in *Notariato*, 2014; A. SERENA, “*Eredità digitale*”, in AA.VV., “*Identità ed eredità digitali, stato dell'arte e possibili soluzioni*”, Aracne, 2016; C. CAMARDI, “*L'eredità digitale. Tra reale e virtuale*”, in “*Il diritto dell'informazione e dell'informatica*”, 2018.

caso di account di pagamento automatizzato (*Paypal, ecc.*) o per trading on line (*IQ Option, markets, Binance, ecc.*), dai contratti di sponsorizzazione, che lo corredano, dalle recensioni o valutazione degli utenti (*Youtube, E-bay, Tripadvisor, ecc.*) o semplicemente dal valore acquisito per essere divenuto per gli utenti di una *community* un punto di riferimento (si prendano ad esempio gli account social di personaggi famosi o c.d. *influencer*).

A tal proposito, giova accennare alla nuova criptovaluta annunciata da *Facebook* per erogare servizi finanziari tramite il proprio *social network: Libra*. Attraverso *Libra* i titolari di un account *Facebook, Whatsapp o Messenger* potranno inviare e ricevere pagamenti in criptovaluta, sulla base di una *blockchain* che, a differenza del sistema *Bitcoin*, sarà “*permissioned*”, dunque, solo un numero limitato di utenti sarà autorizzato a tener traccia del *ledger*, “*libro mastro*”, della rete *blockchain*.

Libra avrà un valore predeterminato che la legherà al valore della moneta, forzandone gli equilibri di cambio, affinché in qualsiasi momento possano essere chiari i meccanismi ed il valore della somma inviata o ricevuta. Se il progetto *Libra* dovesse avere successo, l’account acquisterà anche un valore patrimoniale, essendo direttamente ad esso associato un patrimonio di criptovalute riconducibile al defunto e assumerà ancora più rilevanza in caso di morte dell’utente.

Alcuni gestori di posta elettronica, tra le condizioni generali di servizio (che spesso vengono frettolosamente accettate con un semplice click), prevedono la non trasferibilità dell’account. L’account mail *Yahoo*, ad esempio, non è trasferibile e qualsiasi diritto relativo all’ID o ai contenuti all’interno dell’account verrà meno in seguito al decesso del titolare dell’indirizzo di posta. Questo significa che il *provider* potrà essere contattato solo per richiedere, previa esibizione del certificato di morte, la cancellazione dell’account e tutto il suo contenuto.

Così anche per *Apple, Linkedin e Twitter*. Anche se si decidesse di andare per le vie legali, sarebbero, comunque, applicabili leggi e giurisdizioni straniere, così come accade nel caso di problematiche con alcuni *provider* statunitensi.

Vi è allora da chiedersi: oggi la nostra proprietà digitale, così come la nostra identità digitale legata ai dati (*data mining, data driven economy*), è nelle mani delle grandi piattaforme?

L’avvento dell’era digitale non ha stravolto solamente il nostro modo di rapportarci con altre persone, ma ha dato vita ad un vero e proprio patrimonio digitale. Sebbene in molti casi il valore di quest’ultimo sia solamente personale-sentimentale (foto digitali, messaggi *Whatsapp*, files), spesso accade che si presenti tuttavia di rilevanza economica tutt’altro che trascurabile.

È evidente, allora, che prevedere disposizioni precise sul destino del proprio patrimonio digitale rappresenta, più che un’opportunità, una vera e propria esigenza. I concetti di proprietà, possesso e dominio nell’era digitale che stiamo vivendo, richiedono la rimodulazione dei principi generali di autodeterminazione individuale e di responsabilizzazione delle piattaforme: principi che costituiscono regole

metagiuridiche con funzione normogenetica in grado di regolare la complessità del nostro tempo.

Il *meum esse* risulta modificato nella dimensione digitale: dal territorio si passa al *cloud* ed anche la distinzione di Pugliatti¹⁴⁸ che, nello studio della proprietà invitata a spostare l'analisi dal concetto di “*appartenenza*” a quello della “*funzione*”, non risulta più in linea con una realtà multiversante, fluida e cangiante.

Schmitt¹⁴⁹ parlava del “*nomos della terra*”, ma oggi nella dimensione digitale non è più dato distinguere il “*dove di posizione*” e il “*dove di applicazione*”: il diritto è scosso da due potenze atopiche che sono la tecnica e l'economia.

Secondo il Professore Natalino Irti¹⁵⁰, tali potenze si sono alleate, divenendo potenze della sconfinatezza: non conoscono il dove, ma il “dovunque”. “*Come può il diritto regolamentare la sconfinatezza della “tecnoeconomia”? Il diritto, se non lascia la genesi della terra, non può seguire tali potenze atopiche*”. “Anomia e atopia”: sono questi i due termini che descrivono il mondo digitale.

Non è un caso che i Trattati istitutivi dell'Unione Europea parlino non di territorio, ma di “spazio comune europeo”. “*Il mio esterno*” diceva Kant¹⁵¹, precisando che il fondamento del diritto di proprietà non è di ordine empirico o sensibile, ma intellegibile e razionale scaturendo dalla stessa ragion pratica.

Il “*possesso intelligibile*” distinto dal “*possesso empirico*”, “*possessio phoenomenon*” e “*possessio noumenon*”: la proprietà come esercizio spaziale, la presa di terra fattuale “*landnahme*” come base del diritto di proprietà.

Il tema della proprietà privata era stato ampiamente dibattuto nella *Repubblica* di Platone, che lo ricollegava alle questioni di giustizia e di stabilità sociale (funzione sociale della proprietà affermata anche nell'art. 42 della nostra Costituzione).

Altra concezione della proprietà era quella di Aristotele legata al concetto di progresso.

Ancora oggi, l'indice di sviluppo umano (*Human Development Index*), elaborato annualmente dalle Nazioni Unite, è strettamente correlato all'indice di proprietà privata (*Property Right Index*).

In una visione Neokeynesiana, quale è quella che si sta affermando nel periodo della pandemia in corso, il tema della proprietà, anche nella dimensione digitale, pone l'annosa questione dell'intervento pubblico nell'economia (si ricorderà la diversa concezione tra Weber e Schmitt) volto ad accompagnare gli *assets* strategici del paese attraverso provvedimenti in *equity* di uno Stato *player* che affianca ed aiuta la proprietà privata di tipo produttivo ed imprenditoriale.

Se spostiamo tali considerazioni filosofiche sul piano dell'applicazione pratica del diritto, quale scienza storica e scienza applicata, ci rendiamo conto che la proprietà

¹⁴⁸ La distinzione tra le proprietà e la proprietà, S. PUGLIATTI, “*La proprietà nel nuovo diritto*”, 1964.

¹⁴⁹ C. SCHMITT, “*Il nomos della terra nel diritto internazionale dello «Jus publicum europaeum»*”, Adelphi, 2011.

¹⁵⁰ N. IRTI, “*Il diritto nell'età della tecnica*”, Editoriale Scientifica, 2007.

¹⁵¹ I. KANT, “*Principi metafisici della dottrina del diritto*”, 1797.

oggi non è strettamente correlata alla materialità, prevale la c.d. “*cultura dell’immateriale e dell’adiacente possibile*”.

Di recente, il premio Nobel per la fisica Giorgio Parisi chi ha ricordato che anche la «*materia è un fenomeno dinamico*», definendo il concetto di caos e di “*sistemi complessi*” su scala atomica e planetaria.

Oggi, il diritto deve confrontarsi con l’immateriale e regolarlo.

Per poter regolare occorre, però, capire i fenomeni digitali: il giurista deve sviluppare oggi delle “competenze trasversali” che gli consentano di comprendere la complessità.

Di seguito capiremo in che modo e in quali settori.

Capitolo X

Hate speech: un fenomeno incontrollabile?

La tecnologia e gli strumenti digitali ci impongono ormai di riflettere su un nuovo orizzonte di senso dell'uomo, sullo stesso concetto di valore (*Wertbegriff*) della persona umana, che purtroppo viene colpito profondamente quando, tramite lo strumento digitale, le persone esprimono la c.d. negatività del pensiero e della parola. Come è noto, uno degli aspetti negativi e più diffusi della comunicazione digitale è la reiterazione di attività denigratorie o lesive di vario tipo, che se talvolta sono l'opera di un singolo soggetto, altre volte, invece, convergono in vere e proprie campagne di diffamazione digitale¹⁵².

Ne è un paradigma l'emergente fenomeno delle campagne d'odio (il c.d. *hate speech*), strettamente connesso a quello della diffamazione *online*¹⁵³.

A questo riguardo, è rilevante come la diffusione delle piattaforme digitali stia determinando la frequenza e la pervasività di queste condotte.

La necessità di strumenti di azione più efficaci ha determinato l'avvio di alcune iniziative del Parlamento. Eppure, gli unici risultati raggiunti sono stati quelli in materia di diffusione di immagini a contenuto sessualmente esplicito, inizialmente con l'introduzione nell'ordinamento dell'art. 612-ter c.p., e successivamente con la predisposizione del nuovo art. 144-bis del Codice Privacy.

Il tema ricorrente nell'ambito della diffamazione *online*, presente anche nei casi di diffamazione in generale, è che la persona offesa è molto spesso più interessata, inizialmente, a ristabilire la verità dei fatti, piuttosto che al risarcimento dei danni e alla cessazione della condotta lesiva. Eppure, la verità dei fatti rimane spesso sullo sfondo: generalmente gli elementi di maggiore rilevanza e importanza, ai fini della decisione, insieme a quello della eventuale rilevanza pubblica della notizia diffusa, sono quello della continenza e quello della verità putativa.

Insomma, la realtà dei fatti per come si sono realmente svolti, molto spesso, resta fuori dal processo e la relativa domanda di giustizia è destinata a non essere soddisfatta dal giudice. Si tratta di un profilo di grande interesse, che deve essere segnalato, da un lato,

¹⁵² Il sociologo *Georg Simmel* nella sua opera "*La socievolezza*" evidenzia che nella dimensione digitale deve essere recuperata l'importanza del comportamento, che è la sintesi di un processo di razionalizzazione delle emozioni e dei sentimenti individuali. Il rispetto di tale galateo digitale realizzerebbe quello che *Simmel* definiva estetica che si fa etica. Allo stesso modo, *Norbert Elias* nella sua opera "*La civiltà delle buone maniere*" sottolinea l'importanza del rispetto dell'altro inteso come *kindness*, ossia come gentilezza delle forme comunicative. Il concetto della gentilezza comunicativa rientra nel più grande concetto di *paideia* digitale.

¹⁵³ Si veda la recente opera di E. DHAWAN, "*Digital body language. How to build trust & connection no matter the distance*", 2021, sull'importanza della correttezza e della misura del linguaggio digitale. L'autrice sottolinea l'importanza del linguaggio digitale nel mondo del lavoro per evitare il c.d. "*distancing effect*" e realizzare il c.d. "*water cooler effect*", ossia un linguaggio informale collaborativo nel mondo del lavoro.

al fine di tenere sotto osservazione la casistica in materia, e dall'altro, allo scopo di favorire la ricerca di possibili soluzioni.

Partiamo dal presupposto che il fenomeno del c.d. “*hate speech*” non è una novità degli ultimi tempi, anche se è inevitabilmente recente l'attenzione verso i c.d. “discorsi d'odio”. Infatti, il loro impatto sugli individui e l'introduzione di discipline e misure che consentano di arginare il fenomeno, sono cresciuti di gran lunga negli ultimi anni. La causa di ciò è da rinvenirsi certamente nell'avvento di Internet e dei *social network*¹⁵⁴, che hanno agito come amplificatori. Il tentativo di regolamentare questo fenomeno si scontra inevitabilmente con la necessità di garantire un equo e corretto *trade-off* tra gli interessi in gioco, i diritti e le libertà; vengono in rilievo l'onore, la reputazione, la dignità della persona, ma anche la libertà di espressione, di critica e di cronaca, fino ad arrivare alla libertà di iniziativa economica e di associazione.

In ambito europeo, è già da qualche anno che si sono prese delle misure per arginare comportamenti illegittimi: l'intervento forse più rilevante è stato l'adozione, da parte della Commissione, insieme a diversi *players* del settore (primi fra tutti, Google e Facebook), di un *Codice di Condotta*, che impone ai gestori dei siti e dei *social network* di intervenire attraverso la rimozione dei contenuti illeciti. Per quanto riguarda l'ordinamento interno, invece, sono stati mossi soltanto i primi passi, tanto sul piano giurisprudenziale, quanto su quello legislativo.

Per quanto riguarda il primo profilo, è fondamentale l'analisi delle due pronunce del Tribunale di Roma¹⁵⁵ – relative ad alcune controversie che hanno visto rispettivamente protagoniste le forze politiche *Forza Nuova* e *Casapound Italia* contro Facebook –

¹⁵⁴ Il 10 dicembre 2021, ricevendo il Premio Nobel per la pace, la giornalista filippina Maria Ressa ha lanciato un forte messaggio contro i colossi tecnologici americani, colpevoli, secondo lei, di aver lasciato che l'avidità alimentasse sentimenti negativi sui *social network*. La giornalista Ressa, cofondatrice del sito *Rappler*, che ha vinto il premio insieme al collega russo Dmitry Muratov, ha attaccato le società di internet americane che «hanno permesso a un virus di bugie di infettare ognuno di noi, mettendoci l'uno contro l'altro, facendo emergere le nostre paure, la rabbia e l'odio. Ciò che accade sui social media non rimane sui social media. La violenza online è la violenza del mondo reale. I fatti e la verità sono al centro della risoluzione delle maggiori sfide che la società deve affrontare oggi. Senza fatti, non c'è verità. Senza verità non c'è fiducia. Senza fiducia non abbiamo realtà condivisa, nessuna democrazia e diventa impossibile affrontare i problemi esistenziali del nostro mondo: clima, coronavirus, battaglia per la verità». Ressa – il cui sito web è molto critico nei confronti del Presidente filippino Rodrigo Duterte – è oggetto di 7 cause legali nel suo paese che, secondo lei, rischiano di metterla in prigione per 100 anni. Attualmente in libertà vigilata, in attesa di appello dopo essere stata condannata per diffamazione lo scorso anno, ha dovuto chiedere a 4 tribunali il permesso di viaggiare e di ritirare di persona il suo Nobel per la pace.

¹⁵⁵ Tribunale di Roma, ordinanza del 23/02/2020, resa nell'ambito del procedimento cautelare ex art. 700 c.p.c. (R.G. 64894/2019) e Tribunale di Roma, ordinanza del 14/02/2020, resa nell'ambito della causa n. 80961/19, entrambe commentate e reperibili su <https://www.iusinitinere.it/liberta-di-espressione-facebook-e-movimenti-di-estrema-destra-provvedimenti-a-confronto-27066>, “Libertà di espressione, Facebook e movimenti di estrema destra: provvedimenti a confronto”, di E. PALAZZOLO, 2020.

emesse successivamente alla decisione del famoso *social network* di chiudere alcune pagine ad esse collegate, nonché vari *account* personali riconducibili a loro militanti e gestori. Le due vicende hanno avuto esito diametralmente opposto: la prima si è conclusa con la conferma, da parte del Tribunale, della legittimità della decisione di Facebook; la seconda, invece, con l'accoglimento delle domande presentate dai ricorrenti. Questo duplice e diverso esito ci porta a fare alcune considerazioni.

L'importanza e la delicatezza del tema emergono anche se si esamina l'interesse politico sull'argomento, interesse che ha portato alla presentazione di diverse proposte di legge al riguardo. Da ultimo, è stato presentato alla Camera il c.d. DDL Boldrini, ispirato anche dalla riforma tedesca, il cui aspetto più rilevante risiede nell'introduzione di diversi meccanismi volti sia alla responsabilizzazione dei gestori dei siti internet, sia a fornire agli individui degli strumenti concreti di difesa, soprattutto tramite l'attribuzione di nuove prerogative e poteri in capo al Garante per la privacy. E proprio quest'ultimo ha dimostrato di apprezzare la proposta, e ciò, congiuntamente all'impegno e alle azioni intraprese dall'AGCOM sul tema, dimostra l'importanza del ruolo svolto dalle Autorità garanti.

Il nostro ordinamento, a differenza di altri, non ha una normativa completa e specifica finalizzata a disciplinare il fenomeno del c.d. "*hate speech*".

Secondo la definizione proposta dall'OCSE nel 2003, con questo termine si vogliono intendere le "*manifestazioni di pensiero che esprimono disprezzo nei confronti di individui appartenenti a determinate categorie o nei confronti di determinate categorie di persone*"; manifestazioni di pensiero da tenere comunque distinte dalla più grande e generale categoria degli "*hate crimes*" (i "*crimini d'odio*"), i quali ricomprendono tutti i reati che condividono la matrice del pregiudizio¹⁵⁶.

Comunque, bisogna tenere a mente che, tuttora, manca un'unica definizione.

Il tema è diventato centrale a causa all'avvento della rete e delle comunicazioni tecnologiche, ed in particolare a seguito della diffusione dell'utilizzo dei vari *social network*, i quali ormai veicolano ininterrottamente messaggi, video, audio e immagini fra una moltitudine di persone, con tempi brevissimi e senza confini geografici.

¹⁵⁶ Per una puntuale ricostruzione delle alternative definitorie concernenti gli *hate crimes*, v. da ultimo L. GOISIS, "*Hate Crimes: perché punire l'odio. Una prospettiva internazionale, comparatistica e politico-criminale*", in RIDPP, 2018, 2021 s. Secondo B. PERRY «il crimine d'odio (...) comporta atti violenti ed intimidatori, generalmente diretti verso gruppi già oggetto di marginalizzazione e stigmatizzazione. Così inteso, è un meccanismo di potere e di oppressione, teso a riaffermare le precarie gerarchie che caratterizzano un dato ordine sociale (...)» in B. PERRY, "*In the Name of Hate: Understanding Hate Crimes*", Londra, 2001, 1 e 10. Ancora, secondo N. CHAKRABORTI, i crimini d'odio vanno individuati in quegli «atti di violenza, intimidazione e ostilità diretti verso persone a causa della loro identità o della loro percepita diversità», in N. CHAKRABORTI, J. GARLAND, "*Hate Crime. Impact, Causes, and Responses*", Los Angeles-Londra, 2015, 5. Da ultimo, F. LAWRENCE definisce l'*hate crime* – o meglio il *bias crime* – come un «*crimine commesso per un motivo di pregiudizio (bias) contro una "caratteristica protetta", propria di un gruppo*», in F. M. LAWRENCE, "*Punishing Hate. Bias Crimes under American Law*", Cambridge, 1999, 9.

Si è fatta strada, così, la necessità di garantire maggiori tutele a favore degli utenti di internet, la cui dignità, nonché libertà personale, sono messe in serio pericolo dal continuo verificarsi di condotte illecite *online*.

Il tema è, inevitabilmente, molto complesso. Anzitutto, per la necessità di contemperare ogni esigenza di tutela degli utenti *online* con il rispetto di altri diritti fondamentali che vengono ugualmente in rilievo, come, ad esempio, il diritto alla libertà di espressione, di cronaca e critica. E poi, per la mancanza di una vera e propria regolamentazione della rete: infatti, sia a livello interno che sovranazionale, si è posto il problema relativo al se e in che misura sia necessario introdurre nuove regole e norme valide per l'Internet, e quali obblighi debbano essere imposti ai principali attori del mondo digitale, ossia ai gestori delle grandi piattaforme.

In risposta a tali quesiti, alcune delle maggiori piattaforme recentemente hanno sia introdotto strumenti di autoregolamentazione, che proposto alcune novità anche sul piano legislativo, sotto l'influenza dell'Unione Europea e di altri Paesi (come, ad esempio, la Germania) che si sono già mossi verso questa direzione. Inoltre, nel maggio del 2016, è stato adottato un Codice di Condotta dell'Unione Europea¹⁵⁷, tramite il quale non solo l'Unione e gli Stati Membri, ma anche i *social media* e le altre piattaforme digitali si impegnano a condividere “la responsabilità di promuovere e favorire la libertà di espressione nel mondo online” e di “vigilare affinché Internet non diventi un ricettacolo di violenza e odio liberamente accessibile”.

Il Codice è stato presentato congiuntamente dalla Commissione europea e da quattro grandi piattaforme digitali (*Facebook*, *Microsoft*, *Twitter* e *YouTube*), cui si sono successivamente aggiunte *Google+*, *Instagram*, *Snapchat*, *Dailymotion* e *Webedia*.

Il Codice impone ai gestori delle piattaforme di effettuare, entro 24 ore dalla segnalazione, una valutazione dei contenuti e di eseguire la rimozione di *post* o commenti discriminatori costituenti *hate speech*.

In base alla Direttiva 2000/31/CE, relativa agli aspetti giuridici dei servizi della società dell'informazione¹⁵⁸, tuttavia, la Corte di Giustizia ha affermato che i prestatori di servizi di *hosting* non sono soggetti ad un obbligo *generale* di sorveglianza sulle informazioni trasmesse o memorizzate, né ad un obbligo di ricerca attiva di contenuti illeciti, tranne in alcuni casi specifici in cui l'*host provider* è obbligato a prevenire una violazione ed evitarne di nuove.

Per quanto concerne il livello nazionale, la giurisprudenza si è tradizionalmente orientata nel senso di ritenere che l'*hate speech* non possa rientrare nell'ambito di tutela della libertà di manifestazione del pensiero, dato che questa libertà non può estendersi andando a negare i principi fondamentali ed inviolabili dell'ordinamento¹⁵⁹, come

¹⁵⁷ Accessibile da https://ec.europa.eu/commission/presscorner/detail/it/IP_19_805.

¹⁵⁸ Disponibile su <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:02000L0031-20000717&qid=1495727154628&from=IT>.

¹⁵⁹ Per un approfondimento sulla ricostruzione dei reati di opinione come fattispecie consistenti nella manifestazione di un pensiero critico, dove la condotta comunicativa viene incriminata perché idonea a turbare i valori morali sovra-individuali riconducibili a un'intera collettività, si veda A. SPENA, “Libertà di espressione e reati di opinione”, in *RIDPP*, 2007, 692 ss.

appunto il rispetto della dignità umana e il divieto di ogni tipo di odio e discriminazione.

A livello europeo, è maturata una certa consapevolezza sulla necessità di contrastare efficacemente il fenomeno dell'incitamento all'odio e sulla stretta correlazione esistente tra la sua diffusione e il ruolo preminente che viene oggi assunto dalle piattaforme digitali, consapevolezza che evidentemente si manifesta sia nelle norme contenute all'interno delle nuove proposte di regolamentazione dei mercati digitali presentate a dicembre 2020 dalla Commissione, che nel testo del *Digital Services Act*, ossia il Regolamento che ha come scopo quello di andare a modificare alcuni aspetti dell'attuale Direttiva *e-Commerce*.

In particolare, il Considerando 12 del Regolamento chiarisce un elemento fondamentale, ossia che cosa debba intendersi per “*contenuti illegali*”, dato che, se è vero che le piattaforme digitali non hanno un obbligo generale di sorveglianza, esse sono comunque tenute a provvedere alla rimozione di tali contenuti qualora vengano loro segnalati o comunque ne abbiano conoscenza.

Ebbene, il Regolamento espressamente include, tra i contenuti illegali, quelli qualificabili come “*hate speech*”.

Il Comitato europeo per la protezione dei dati ha formulato un parere su questo profilo, in particolare in merito ai meccanismi di moderazione dei contenuti utilizzati dalle piattaforme.

All'interno dell'Opinione 1/2021¹⁶⁰ è, infatti, specificato che non tutti i meccanismi in questione presuppongono il trattamento di dati personali e che, per rispettare il principio di *data minimisation*, il Regolamento dovrebbe evidenziare in maniera più precisa e dettagliata le condizioni specifiche in presenza delle quali il trattamento dei dati personali nella moderazione dei contenuti risulta ammesso.

Ad ogni modo, la piattaforma dovrà dimostrare la necessità e la proporzionalità delle misure adottate. È importante evidenziare che, comunque, oltre che per la tutela dei dati personali, l'implementazione di tali meccanismi rappresenta un rischio anche per la libertà di espressione.

In quest'ottica, nella proposta di DSA è previsto che la Commissione europea incoraggi e favorisca l'adozione, a livello europeo, di codici di condotta che aiutino a garantire una migliore applicazione del Regolamento e a gestire i rischi derivanti dalla diffusione di contenuti illeciti, tenuto conto soprattutto dei profili che riguardano la concorrenza e la protezione dei dati personali.

Il nuovo orientamento giurisprudenziale italiano, legato ad alcuni casi di rimozione di contenuti *online* da parte di Facebook, e ispirato anche ai dettami della Corte Edu¹⁶¹, si

¹⁶⁰ Accessibile da https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf.

¹⁶¹ Corte Europea dei Diritti dell'Uomo, sez. I, sent. 16/01/2020 Magosso-Brindiani c/ Italia, Ricorso 59347/11; Corte Europea Diritti dell'Uomo, sez. III, 22/06/2021, ric. n. 5869/17, Erkizia Almandoz c. Spagna.

va ad inserire all'interno di questo quadro normativo, relativo ai limiti che possono, in maniera legittima, essere imposti alla libertà di espressione in relazione a messaggi d'odio o discriminatori.

Per cominciare, la giurisprudenza della Corte è conforme nel ritenere che gli atti di istigazione all'odio non necessitino della presenza di violenza o delitti consumati. Bisogna soffermarsi anche sull'identificazione, in concreto, dell'incitamento alla violenza, che deve essere valutato basandosi su diversi elementi, tra i quali rientra il modo in cui viene effettuata una data comunicazione, il linguaggio in concreto utilizzato, il contesto specifico, il numero di persone a cui l'informazione è rivolta, la posizione e la qualità ricoperte dall'autore, nonché la posizione di debolezza o meno del destinatario della dichiarazione.

In altri termini, si può ammettere una compressione della libertà di manifestare il proprio pensiero in rete solamente se le manifestazioni d'odio raggiungono un livello tale da dirsi funzionali alla compressione dei principi di uguaglianza e libertà¹⁶².

L'Unione Europea, d'altronde, già nel 2008 aveva adottato la decisione-quadro 2008/913/GAI¹⁶³ sulla lotta contro alcune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, tramite l'inserimento, tra i reati di stampo razzista o xenofobo, dell'*"istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica"* e dell'*"apologia, la negazione o la minimizzazione grossolana dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra"*, come sono definiti agli articoli 6, 7 e 8 dello Statuto della Corte penale internazionale.

Sotto questo aspetto, il primo caso rilevante riguarda la chiusura di diverse pagine Facebook riconducibili ad alcune articolazioni territoriali del noto partito politico *Forza Nuova*, ed alla diretta sospensione degli *account* personali di alcuni suoi esponenti, amministratori delle pagine richiamate.

In particolare, con l'ordinanza resa nell'ambito del procedimento cautelare ex art. 700 c.p.c. (R.G. 64894/2019) in data 23/02/2020¹⁶⁴, il Tribunale ha rigettato il ricorso

¹⁶² Sul tema v. anche L. GOISIS, *"Libertà di espressione e odio omofobico. La Corte europea dei diritti dell'uomo equipara la discriminazione in base all'orientamento sessuale alla discriminazione razziale"*, in RIDPP, 2013, 418 ss.; L. GOISIS, *"Omosessualità, hate crimes e diritto penale"*, in GenIus, 2015, 44 ss. Sul tema specifico, A. PUGIOTTO, *"Aporie, paradossi ed eterogenesi dei fini nel disegno di legge in materia di contrasto all'omofobia e alla transfobia"*; M. PELISSERO, *"Omofobia e plausibilità dell'intervento penale"*; L. IMARISIO, *"Il reato che non osa pronunciare il proprio nome. Rettenze e limiti nel c.d. disegno di legge Scalfarotto"*; M. CAIELLI, *"Punire l'omofobia: (non) ce lo chiede l'Europa. Riflessioni sulle incertezze giurisprudenziali e normative in tema di hate speech"*; L. MORASSUTTO, *"Omofobia e medioevo italiano"*, contributi pubblicati in GenIus, 2015, 6 ss.

¹⁶³ Il testo della decisione quadro è accessibile da <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32008F0913&from=IT>.

¹⁶⁴ L'ordinanza è reperibile su <https://www.questionegiustizia.it/data/doc/2345/ordinanza-rg-648942019-forza-nuova-art700.pdf>, ed è commentata da I. M. LO PRESTI, *"CasaPound, Forza Nuova e Facebook. Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e social network"*, in Forum di Quaderni Costituzionali, 2, 2020,

presentato contro il *social network* Facebook, volto a contestare il su citato provvedimento di sospensione e chiusura delle pagine, aderendo quindi alla tesi della piattaforma *social*.

Nella pronuncia romana, che si rifà alla definizione di “*hate speech*” predisposta dall’OSCE, i Giudici sottolineano la natura di Facebook quale *soggetto privato*, evidenziando che, nonostante la rilevanza sociale dell’attività svolta da quest’ultimo, il rapporto tra le due parti è comunque regolato dalle condizioni contrattuali a cui queste aderiscono al momento dell’iscrizione al *social network*.

Tramite la sottoscrizione di tali condizioni, in effetti, l’utente assume il precipuo impegno di “*non usare Facebook per scopi illegali, ingannevoli, malevoli o discriminatori*” e di non “*pubblicare ed eseguire azioni che non rispettino i diritti di terzi o le leggi vigenti*”.

Tra l’altro, nell’ipotesi di violazione delle suddette condizioni, Facebook si riserva, inoltre, il diritto di rimuovere tali contenuti e di interrompere la fornitura del suo servizio.

Viene poi previsto che, nel caso in cui il fruitore del servizio digitale violi *chiaramente, seriamente o reiteratamente* le condizioni o normative – ed in particolare gli *Standard della Community* – Facebook potrebbe arrivare a sospendere o disabilitare in modo *permanente* l’accesso dell’utente al proprio *account*, fermo restando che le misure in concreto adottate dipendono, in ogni caso, dalla gravità della violazione e dalle precedenti condotte dell’utente-fruitore. Queste stesse regole si applicano anche alle “*pagine social*”, e l’utente è in tal senso tenuto a garantirne la conformità non solo rispetto agli *Standard della Community*, ma anche a leggi, regolamenti e altre normative vigenti.

Gli *Standard* cui ci si riferisce riguardano in particolare i contenuti e le attività dell’utente su Facebook e prevedono specificatamente il divieto di divulgare contenuti che possano essere interpretati come discorsi di incitazione all’odio e che in alcuni casi possono addirittura portare ad incoraggiare episodi di violenza reale.

Facebook definisce i discorsi d’odio come “*un attacco diretto alle persone sulla base di aspetti tutelati a norma di legge, quali razza, etnia, nazionalità di origine, religione, orientamento sessuale, casta, sesso, genere o identità di genere e disabilità o malattie gravi*” e aggiunge che “*forniamo anche misure di protezione per lo status di immigrato. Definiamo l’attacco come un discorso violento o disumanizzante, dichiarazioni di inferiorità o incitazioni all’esclusione o alla segregazione*”.

Al tempo stesso, viene vietata la divulgazione di contenuti che possano esprimere supporto o elogio ai gruppi o leader coinvolti nell’odio organizzato. Viene, inoltre, definita come organizzazione che incita all’odio “*qualsiasi associazione di almeno tre persone organizzata con un nome, un segno o simbolo e che porta avanti un’ideologia, dichiarazioni o azioni fisiche contro individui in base a caratteristiche come razza,*

credo religioso, nazionalità, etnia, genere, sesso, orientamento sessuale, malattie gravi o disabilità”, specificando di non consentire “la condivisione sulla nostra piattaforma di simboli che rappresentano una delle organizzazioni o degli individui di cui sopra se non ai fini di condanna o discussione. Non consentiamo contenuti che elogiano le organizzazioni e gli individui di cui sopra o atti da loro commessi. Non consentiamo il coordinamento del supporto a qualsiasi organizzazione o individuo di cui sopra o agli atti da loro commessi”.

Tornando al caso di specie, Facebook ha provveduto a risolvere il contratto, chiudendo poi le pagine riconducibili a Forza Nuova, qualificando la stessa come “*organizzazione che incita all’odio*” alla luce della definizione sopra riportata. L’organizzazione, infatti, svolge una serie di attività di propaganda razzista, xenofoba e antisemita, ostentando il fatto di essere un movimento neofascista e utilizzando simboli del fascismo nel corso delle proprie manifestazioni.

Le pagine oggetto della decisione di Facebook – insieme ai profili privati dei loro amministratori – erano utilizzate per la divulgazione di contenuti di propaganda in favore dell’organizzazione, facendo uso di simboli fascisti e razzisti che, a parere di Facebook, incitavano all’odio e alla discriminazione.

Nella parte motiva del provvedimento di rigetto del ricorso presentato da Forza Nuova nei confronti di Facebook, il Tribunale romano ha, per prima cosa, richiamato il programma politico dell’organizzazione, che risulta agli occhi di tutti in contrasto con alcuni principi del nostro ordinamento, primo fra tutti il divieto, valido per tutte le forze politiche, di rifarsi esplicitamente all’ideologia fascista o nazista, al razzismo, alla xenofobia e di proclamare idee discriminatorie (ad esempio, Forza Nuova vorrebbe espressamente l’abrogazione delle leggi Scelba e Mancino, definendo le stesse come leggi liberticide).

Secondo il parere dell’organo giudicante, tenuto conto dei numerosi episodi che testimoniano la stretta vicinanza di Forza Nuova al fascismo, alla luce sia della normativa interna e sovranazionale, che del Codice di condotta sottoscritto da Facebook insieme alla Commissione europea, è stata assolutamente legittima la decisione di addivenire alla risoluzione del contratto e alla sospensione del servizio, dal momento in cui è senza dubbio possibile ascrivere il partito entro la definizione di “*organizzazione d’odio*”.

Ma i giudici si spingono oltre, asserendo che Facebook aveva il *dovere giuridico* di agire in tal senso, rischiando altrimenti di incorrere in responsabilità. A ciò devono essere aggiunti i diversi episodi in cui vari esponenti di Forza Nuova si sono resi protagonisti di veri e propri discorsi d’odio o hanno comunque supportato o elogiato l’attività del partito, circostanza che secondo la Corte legittima la contestuale sospensione dei loro *account* privati, in quanto tali comportamenti si pongono anche in aperto contrasto con gli *Standard della Community* sopra richiamati.

Il Tribunale di Roma si è espresso anche in merito alla proporzionalità della misura adottata, asserendo che, poiché prima di giungere alla rimozione totale delle pagine e

degli *account*, vi era stata reiteratamente da parte di Facebook la rimozione di singoli contenuti, la misura della sospensione si presentava come necessaria e adeguata.

Segue lo stesso orientamento anche un'ordinanza del Tribunale di Siena¹⁶⁵, pronunciata nell'ambito di un ricorso ex artt. 669-bis e ss. e 700 c.p.c., anch'essa riguardo alla rimozione dell'*account* privato di un utente e della "pagina tematica" ad esso connessa. Anche in questo caso i contenuti divulgati erano attinenti allo svolgimento di attività politica e sono stati considerati in contrasto con gli *Standard della Community*, tanto da Facebook quanto dal Tribunale, che ha rigettato l'istanza del ricorrente.

Risulta di diverso avviso, invece, il Tribunale di Roma – sia in prima fase che in sede di reclamo – nell'ordinanza resa in data 14.02.2020 (nell'ambito della causa n. 80961/19¹⁶⁶), a seguito del ricorso promosso da parte di *Casapound Italia* contro Facebook, che aveva rimosso la pagina dell'Associazione e del profilo personale di uno dei suoi esponenti.

Il Collegio giudicante, sebbene abbia ritenuto – in difformità rispetto a quanto affermato dall'ordinanza reclamata – che il rapporto fra le parti vada inquadrato tra i contratti ordinari di diritto civile e che, di conseguenza, la legittimità dell'esercizio del diritto di recesso da parte del contraente debba essere valutata alla luce dell'accordo negoziale stipulato fra le stesse, ha tuttavia puntualizzato che risulta preclusa all'autonomia privata la possibilità di limitare i diritti costituzionali di una delle parti. In altri termini, il rispetto dei diritti fondamentali – in questo caso, la libertà di iniziativa economica privata, ex art. 41 Cost. e la libertà di manifestazione del pensiero e di associazione, rispettivamente riconosciute dagli artt. 21 e 18 Cost. – si pone quale limite invalicabile dell'autonomia privata.

Nello specifico, i giudici hanno respinto il reclamo presentato da Facebook sulla base dell'assunto che quest'ultimo, avente natura di *soggetto privato*, non sia legittimato ad esprimersi sulla liceità o meno dell'Associazione in quanto tale, potendo limitarsi esclusivamente a contestare la violazione delle regole contrattuali che ne disciplinano il reciproco rapporto.

In particolare, l'organo giudicante ha evidenziato che Facebook aveva giustificato la chiusura delle pagine e la sospensione dell'erogazione del servizio nei confronti del singolo utente privato, sulla base di valutazioni concernenti il complesso dell'attività politica di *Casapound*, ed in particolare l'esplicito richiamo di questa all'ideologia fascista. A parere di Facebook, ciò costituiva, infatti, una forma di sostegno a "*politiche*

¹⁶⁵ Testo accessibile su <https://dirittodiinternet.it/wp-content/uploads/2020/01/OrdinanzaSiena.pdf>.

¹⁶⁶ Il testo è disponibile su <https://media2-col.corriereobjects.it/pdf/2019/politica/sentenzacpifb.pdf>, con nota di I. M. LO PRESTI, "*CasaPound, Forza Nuova e Facebook. Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e social network*", cit.; vedi anche il commento di P. VILLASCHI, "*Facebook come la RAI?: note a margine dell'ordinanza del Tribunale di Roma del 12.12.2019 sul caso CasaPound c. Facebook*", disponibile sul sito https://www.osservatorioaic.it/images/rivista/pdf/2020_2_24_Villaschi.pdf.

incompatibili a quelle del Servizio Facebook”, sufficiente a legittimare la recessione dal contratto da parte dello stesso.

Tuttavia, nonostante il Tribunale ammetta che la compatibilità dell’associazione con le condizioni contrattuali debba essere valutata anche alla luce della sua natura intrinseca, i Giudici sottolineano che la valutazione inerente alla liceità dell’organizzazione vada compiuta con riferimento alla disciplina pubblicistica, assumendo quale riferimento i limiti posti dall’art. 18 Cost., come interpretato dalla giurisprudenza costituzionale e di legittimità, e la successiva normativa a tutela del valore dell’uguaglianza.

Per quanto concerne il richiamo all’art. 18 – a norma del quale la libertà di associazione dei cittadini incontra, quale unico limite, il perseguimento di fini vietati ai singoli dalla legge penale – potrebbe rilevare, nel caso di specie, in virtù del divieto di ricostituzione del partito fascista sancito dal nostro ordinamento.

Senonché, la fattispecie in esame richiederebbe la sussistenza di un pericolo in concreto, attinente alle finalità specifiche e alle modalità di azione della forza politica, non essendo sufficiente il solo richiamo all’ideologia fascista.

Secondo il Collegio, inoltre, nel caso di specie non rileverebbe nemmeno la disciplina che lega l’illiceità dell’associazione all’incitamento all’odio, alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi, poiché, nella prospettazione data da Facebook, tali elementi sarebbero riconducibili all’attività di Casapound esclusivamente sulla base dell’inscindibilità di questi aspetti dall’ideologia e dall’esperienza del fascismo.

Questo è un criterio che, secondo il Tribunale, non può che dirsi arbitrario, costituendo un’inaccettabile estensione dell’applicazione della norma penale – come noto soggetta al principio di tipicità – e un’illegittima limitazione del diritto alla libertà di manifestazione del pensiero.

In altre parole, gli elementi dedotti in giudizio non sono, secondo il Giudice, sufficienti a permettere di affermare che Casapound sia un’associazione illecita secondo l’ordinamento generale, tenuto conto che la valutazione svolta è limitata all’oggetto del giudizio in essere.

Inoltre, nel valutare la sussistenza o meno del *periculum in mora*, il Tribunale ha evidenziato la rilevanza del servizio reso da Facebook in riferimento alla partecipazione al dibattito politico. La gravità del pregiudizio subito da Casapound viene, altresì, rapportata al numero di utenti della piattaforma.

Dal punto di vista politico, la nascita di una Commissione parlamentare competente per il tema dell’incitamento all’odio e la proposizione, nel corso degli ultimi anni, di diversi disegni di legge finalizzati a colmare l’attuale lacuna dell’ordinamento, sono la piena testimonianza del fatto che anche dal punto di vista normativo c’è stata grande attenzione verso il tema dell’*hate speech*.

Nel 2019, infatti, è stato presentato in Parlamento il primo disegno di legge DDL Cirinnà, volto a disciplinare e arginare il fenomeno dell’*hate speech* in Italia,

denominato “*Misure per il contrasto del fenomeno dell’istigazione all’odio sul web*”¹⁶⁷. All’interno della relazione introduttiva, vi è l’illustrazione del quadro normativo europeo e sovranazionale vigente, a dimostrazione del fatto che il legislatore italiano ha come obiettivo quello di garantire coerenza e continuità rispetto a quanto già fatto in materia.

L’art. 1 della proposta di legge, nel definire le finalità del progetto, individuate nella volontà di “*prevenire e sanzionare il fenomeno dell’istigazione all’odio sul web*”, richiama espressamente la decisione quadro 2008/913/GAI e il protocollo addizionale alla Convenzione del Consiglio d’Europa sulla criminalità informativa.

I soggetti destinatari della proposta sono i c.d. “*gestori informatici*”, come vengono definiti dalla legge in materia di *cyberbullismo*, mentre invece, le condotte sanzionate coincidono con quelle previste in materia di discriminazione etnica, razziale e religiosa, ma con esplicito richiamo all’ambito della rete.

Una delle novità più interessanti è quella prevista dall’art. 4, che vorrebbe introdurre, nel nostro ordinamento, lo specifico delitto di istigazione all’odio in rete.

La fattispecie, di nuova introduzione, consentirebbe di sanzionare fenomeni che, sebbene rechino già pregiudizio agli utenti, non sono attualmente rilevanti per la disciplina penale.

Se si prende in esame il tradizionale reato di diffamazione ex art. 595 c.p., infatti, si noterà che esso tutela la reputazione soltanto individuale, escludendo le ipotesi in cui espressioni offensive e lesive siano rivolte ad intere categorie o gruppi di persone, e non ad un soggetto specifico.

La nuova fattispecie, inoltre, troverebbe collocazione fra i delitti contro l’uguaglianza, al fine di garantire la piena tutela a tutte le categorie oggetto di fenomeni di istigazione all’odio.

Si tenga presente che l’art. 5 introduce nuovi obblighi in capo ai gestori dei siti web, in materia di segnalazione e rimozione di *post* dal contenuto illecito. Per prima cosa, questi sono tenuti a mettere a disposizione degli utenti in rete una procedura che sia chiara, semplice e sempre attiva, idonea a formulare le proprie segnalazioni. Quest’ultime saranno, poi, valutate da un organismo di autoregolazione, composto da analisti e periti indipendenti, e, nel caso venga espresso parere positivo, il gestore dovrà provvedere alla rimozione del *post* nel termine di 24 ore dalla segnalazione, salvo che intervenga un diverso accordo con le autorità competenti.

L’art. 6 sancisce, inoltre, l’obbligo per i gestori dei siti web di redigere un rapporto semestrale sulle segnalazioni ricevute, distinguendo le stesse a seconda dell’oggetto e del motivo ed indicando l’esito di ciascuna.

Tale rapporto deve venire poi pubblicato sulla *homepage* del sito, affinché sia facilmente fruibile dagli utenti. Nel caso di violazione di tali obblighi da parte dei gestori dei siti, possono essere irrogate nei loro confronti delle sanzioni amministrative pecuniarie, la cui entità può variare a seconda del tipo di violazione, della gravità e dell’eventuale reiterazione della condotta.

¹⁶⁷ Accessibile da <https://www.senato.it/service/PDF/PDFServer/BGT/01124878.pdf>.

Si evidenzia che, da ultimo, è stato presentato alla Camera il c.d. DDL Boldrini, denominato “*Misure per la prevenzione e il contrasto della diffusione di manifestazioni d’odio mediante la rete internet*”¹⁶⁸.

Si parte, anche qui, dalla considerazione che la rete sia ormai diventata lo strumento di diffusione di idee e messaggi più potente di qualunque altro e che il suo utilizzo errato o distorto si possa concretizzare in severe forme di discriminazione di alcune categorie, soprattutto minoranze, sulla base dell’orientamento sessuale, della razza o del genere. Nel seguire l’esempio di altri Paesi europei, che si sono già dotati di una normativa specifica in materia di *hate speech* (v. *supra* il riferimento alla Germania), lo scopo dichiarato è quello di andare a regolamentare questa fattispecie specifica, che presenta connotati ben diversi rispetto alla tradizionale figura dell’*incitamento all’odio*, proprio in ragione della maggiore invasività del web come strumento di diffusione. Il presupposto di tale ragionamento è che la regolamentazione di Internet sia divenuta non solo cosa possibile, bensì strettamente necessaria.

Il DDL Boldrini, all’art. 1, dichiara in maniera esplicita lo scopo della proposta di legge, ossia la tutela delle dignità, libertà personale e salute psicofisica dei fruitori del web, messe a serio rischio da comportamenti che continuamente incitano, promuovono o incoraggiano l’odio.

Per raggiungere tale precipua finalità, si è optato per una maggiore responsabilizzazione dei gestori dei siti, chiamati a contribuire alla prevenzione e al contrasto di tali fenomeni, anche limitando la diffusione di *fake news*.

È un elemento che si ricollega alla tematica della diffamazione a mezzo *social*¹⁶⁹, di cui si parlerà più avanti.

Il prevalente orientamento giurisprudenziale ritenere che sia sufficiente, affinché il diritto di cronaca/critica prevalga sull’interesse del soggetto diffamato, scriminando la condotta, che sia presente la c.d. *verità putativa*. Questo esplicito riferimento del progetto di legge alla verità dei fatti potrebbe contribuire a modificare tale orientamento nel senso di riconoscere maggiore rilevanza alla dignità della persona e al diritto di quest’ultima di ottenere l’accertamento della realtà.

È anche prevista la modifica di diverse disposizioni del codice penale, allo scopo di favorire la rimozione di contenuti illegali dal web.

Anche qui, come nel DDL Cirinnà, è riconosciuto agli utenti del servizio web il diritto di segnalare la presenza di contenuti manifestamente illeciti, per ottenerne la rimozione.

¹⁶⁸ Il testo è disponibile su <http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.2936.18PDL0133410.pdf>.

¹⁶⁹ Sul tema v. anche M. PELISSERO, “*La parola pericolosa. Il confine incerto del controllo penale del dissenso*”, in *QuestG*, 2015, 38; L. ALESIANI, “*I reati di opinione. Una rilettura in chiave costituzionale*”, Milano, 2006; C. CALVERT – J. BROWN, “*Video Voyeurism, Privacy and the Internet: exposing Peeping Toms in Cyberspace*”, in *Cardozo Arts Entertainment Law Journal*, 2000, 469 ss.; J. CLOUGH, “*Principles of Cybercrime*”, Cambridge, 2010, 388 ss.; D. ORMEROD, “*Voyeurism: Elements of Offence-Privacy-Reasonable Expectation of Privacy*”, in *CrimLawReview*, 2008, 12 ss.

Il gestore del sito web è obbligato a mettere a disposizione dei fruitori una procedura semplice, chiara e trasparente per effettuare la segnalazione. Anche in questo caso, inoltre, l'esame della segnalazione è rimesso ad un organismo di autoregolamentazione, di cui fanno parte *“esperti dotati di ampie e diverse competenze e di esperienza, che non presentino cause di conflitto di interessi tali da comprometterne l'indipendenza del giudizio e delle decisioni prese”*.

Il gestore del sito internet deve farsi carico degli oneri di gestione del suddetto organismo, mentre la definizione dell'ambito e della struttura delle verifiche è rimessa a norme procedurali ispirate ad un codice etico di comportamento, trasparente e accessibile agli utenti.

Se il parere dell'organismo risulta negativo, è ammesso il ricorso al Garante per la protezione dei dati personali.

Il gestore del sito è, in ogni caso, legittimato a segnalare la presenza di un contenuto manifestamente illecito direttamente, in assenza di specifica segnalazione da parte dell'utente, ed è tenuto a garantire che il medesimo contenuto non venga nuovamente caricato o condiviso.

I gestori dovranno, inoltre, redigere un resoconto delle segnalazioni pervenute, con specifici obblighi nel caso in cui il numero di queste ultime sia particolarmente elevato.

Il Garante per la privacy può anche irrogare sanzioni – la cui entità è commisurata alla gravità della violazione – in caso di violazione degli obblighi in materia di segnalazione, oscuramento, rimozione o blocco di contenuti illeciti e resoconto da parte dei gestori.

Per quanto concerne l'art. 8, esso interviene sul diritto all'oscuramento, alla rimozione o al blocco della diffusione dei propri dati o immagini personali nella rete, ampliandone la portata rispetto alle fattispecie di cui all'art. 167 del D.lgs. n. 196/2003 e includendovi anche ipotesi escluse dall'art. 4 del medesimo disegno di legge o da altre norme incriminatrici.

È, infatti, riconosciuto a chiunque (ivi compresi i soggetti di minore età; se ultraquattordicenni, i minori possono agire personalmente) il diritto ad ottenere, in qualsiasi momento, l'oscuramento, la rimozione o il blocco di propri dati o immagini ritenuti offensivi o lesivi della propria dignità, identità e libertà personale, tramite istanza presentata al titolare del trattamento.

Nel caso in cui questo dia tempestivamente seguito alla richiesta o non sia possibile identificarlo, l'istanza può essere presentata direttamente al Garante della Privacy. La legittimità della richiesta di rimozione del contenuto può altresì essere contestata innanzi al Garante, le cui decisioni sono suscettibili di ricorso innanzi al giudice ordinario. Il Garante ha il potere di irrogare sanzioni amministrative pecuniarie nei confronti del gestore sul web, il cui ammontare può variare da 500.000 a 5.000.000 euro, sulla base della gravità e della reiterazione della condotta.

Il meccanismo di tutela appena descritto coincide con quanto già previsto in materia di diritto all'oblio e *cyberbullismo*, ed è stato richiamato e lodato dal Presidente del Garante della Privacy, il Professor Pasquale Stanzone, nel corso dell'audizione

tenutasi il 13 luglio 2021¹⁷⁰, il quale lo ha definito un utile strumento di tutela dei diritti della personalità *online*, capace di conciliare l'esigenza di rimozione dei contenuti con la riserva all'autorità pubblica della decisione di ultima istanza, in linea con il difficile bilanciamento di interessi da svolgere secondo le indicazioni della CGUE e della Corte EDU. È interessante evidenziare che il coinvolgimento del Garante è funzionale al rispetto delle libertà fondamentali, sottratte a valutazioni compiute esclusivamente da soggetti privati, arginando il rischio di comportamenti arbitrari e abusivi.

Il Presidente, inoltre, si è espresso in senso favorevole all'ampliamento dell'ambito di applicazione dell'art. 167 del Codice Privacy, che si occupa del delitto di trattamento illecito di dati personali: si suggerisce la reintroduzione del consenso tra i requisiti di illiceità speciale (come prima della riforma di cui al D.lgs. 101/2018; la disciplina attuale ha infatti limitato la fattispecie alle sole attività di *telemarketing*).

Si sta andando verso la stessa direzione di quella emersa in ambito europeo, come dimostrato dal c.d. *Digital Services Act*¹⁷¹, la proposta di Regolamento presentata dalla Commissione nel dicembre 2020. La proposta italiana va ad imporre, infatti, degli specifici obblighi in capo ai gestori delle piattaforme digitali, mirando alla responsabilizzazione di questi ultimi, proprio con riferimento alla rimozione di contenuti illegali, fra i quali rientrano senz'altro i contenuti di *hate speech*. Non è un caso, infatti, che già nel corso dei lavori di preparazione della bozza di provvedimento – anch'esso fortemente influenzato dalla nuova normativa tedesca – sia emersa la rilevanza di tali disposizioni nel contesto dell'*hate speech*.

Per quanto concerne la responsabilità dei gestori e la prevenzione di comportamenti illeciti, è importante anche il parere espresso dall'AGCOM in merito all'utilizzo dell'Intelligenza Artificiale come strumento di monitoraggio. Viene, in tal caso, incoraggiato lo sfruttamento delle nuove tecnologie, che deve avvenire non in sostituzione dell'attività umana, bensì in suo supporto.

L'approccio sin qui delineato potrebbe contribuire, senza dubbio, ad agevolare l'adempimento degli obblighi che s'intende imporre in capo ai gestori dei siti.

L'Autorità garante delle comunicazioni ha già aderito al progetto *ISMyPP*¹⁷², il quale vuole arrivare allo sviluppo di tecniche per la *rilevazione automatizzata* dei discorsi d'odio, che assume particolare rilevanza nell'ambito del recepimento della Direttiva (UE) 1808/2018 (Direttiva SMAV)¹⁷³, con la quale viene esteso l'ambito di applicazione delle norme in materia di contrasto all'*hate speech* anche alle piattaforme di *video sharing*.

Tuttavia, poiché la rimozione di contenuti dal web costituisce comunque una limitazione del diritto alla libertà d'espressione, ammissibile solo in presenza di

¹⁷⁰ V. <https://www.garanteprivacy.it/home/attivita-e-documenti/documenti/audizioni>.

¹⁷¹ Accessibile da <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0825&from=en>.

¹⁷² Disponibile su <https://www.agcom.it/956>.

¹⁷³ V. <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018L1808&from=pl>.

specifiche circostanze, si è diffusa la tendenza che vuole escludere che i processi di monitoraggio siano totalmente automatizzati, dovendo comunque essere garantito il controllo umano volto ad evitare errori eventuali.

Una delle decisioni assunte dall'*Oversight Board* istituito da Facebook, un Comitato interno alla società e preposto a valutare l'adequatezza delle decisioni concernenti la rimozione dei *post*, è rilevante in tal senso.

Trovatosi ad affrontare la questione a seguito della cancellazione di un *post* per la sensibilizzazione sul tumore al seno, raffigurante foto di donne che avevano subito operazioni, il Comitato ha sostenuto che la decisione assunta dall'algoritmo era sbagliata: non era stata rilevata correttamente la descrizione dell'immagine, nella quale si chiariva lo scopo del *post*. Il Comitato, dunque, si è espresso proprio nel senso di ribadire la necessità di un controllo umano rispetto alle decisioni algoritmiche, a tutela delle libertà fondamentali dell'individuo.

Per quanto riguarda la partecipazione dell'AGCOM, bisogna segnalare che l'Autorità ha già approvato un proprio Regolamento, rivolto in primo luogo ai fornitori di servizi media audiovisivi e radiofonici¹⁷⁴, invitati a promuovere i temi dell'inclusione, della coesione sociale, della promozione della diversità e dei diritti fondamentali¹⁷⁵.

Ebbene, l'AGCOM ha avviato delle interlocuzioni con le maggiori piattaforme (come Google e Facebook), proprio alla luce della crescente rilevanza della diffusione dei contenuti sulla rete e del potere riconosciuto all'Autorità di promuovere, mediante procedure di co-regolamentazione, l'adozione da parte delle piattaforme di misure volte a contrastare la diffusione sui *social* di contenuti lesivi della dignità umana.

È evidente che l'Autorità punta a raccogliere informazioni sui criteri e le procedure già in essere per la segnalazione e la rimozione dei contenuti d'odio, volendo raggiungere l'obiettivo di favorire l'adozione di misure ulteriori (es. codici di condotta).

Al fine di assicurare l'efficacia di tali misure, l'AGCOM ha anche avviato un'indagine conoscitiva¹⁷⁶, volta a valutare l'impatto delle piattaforme sull'economia e sulla società, classificando i servizi offerti da queste ultime e valutandone le potenzialità, le problematiche e gli effetti.

¹⁷⁴ Accessibile da <https://www.agcom.it/documents/10179/539471/Delibera+607-10-CONS/13bf547f-48e6-4f22-94f4-b82a46bb41e3?version=1.0&targetExtension=pdf>.

¹⁷⁵ Si segnala che lo stesso impegno era già stato richiesto anche ai *social media* e ai *servizi online*, proprio in ragione dell'interazione fra i diversi mezzi di comunicazione; tuttavia, a differenza di quanto previsto per i *media* tradizionali, si trattava esclusivamente di un invito all'autodisciplina.

¹⁷⁶ Disponibile su <https://www.agcom.it/documents/10179/5041493/Delibera+309-16-CONS/7f6d711a-ac5d-48b1-9b30-faa27d6a1ecb?version=1.0>.

Capitolo XI

La figura degli *influencer*

Il mondo dei *social media*, e soprattutto il modo in cui questi vengono utilizzati dai c.d. *influencer*, sta avendo un grande impatto anche per quanto concerne la materia relativa alla tutela dei marchi e della pubblicità occulta.

L'AGCM, consapevole della portata della questione, ha mostrato una grande attenzione verso quest'ultima fattispecie, scegliendo di modificare il proprio approccio nell'ultimo periodo. Piuttosto che limitarsi a pronunce di *soft law*¹⁷⁷, sono state recentemente avviate, infatti, vere e proprie indagini istruttorie nei confronti delle imprese digitali, con lo scopo di spronarle all'adeguamento alla disciplina vigente.

Dal momento che l'attività del c.d. *influencer marketing*¹⁷⁸ ricade nell'ambito di applicazione del Codice del Consumo, non è raro che si vadano a configurare ipotesi di pubblicità occulta a danno del consumatore.

Per ovviare a tale pericolosa situazione, è stato necessario l'intervento dello IAP, che ha reso pubblica la *Digital Chart*¹⁷⁹, che consiste in un documento – condiviso anche dall'AGCM – con cui sono fornite delle precise indicazioni per quanto riguarda le misure che gli *influencer* devono adottare al fine di rendere esplicita la finalità commerciale delle loro comunicazioni *social* (*posts, stories*), a seconda del tipo di contenuto che viene pubblicato e della natura del rapporto che lega l'*influencer* al titolare del marchio. Ed è sulla base di questa più limpida regolamentazione che l'Autorità Garante della Concorrenza e del Mercato ha iniziato ad intervenire. Si pensi ai casi che hanno coinvolto Alitalia e Barilla: sono la testimonianza dell'attenzione dell'Autorità anche verso le più recenti evoluzioni del fenomeno.

Per quanto concerne la tutela dei marchi, invece, vengono in rilievo anzitutto le questioni legate all'utilizzo degli *hashtag*; si pensi, ad esempio, alla possibilità di applicare a questi ultimi la disciplina propria dei segni distintivi.

Recentemente, la giurisprudenza si è espressa sui marchi celebri, in un caso che ha visto protagonista la Ferrari¹⁸⁰. La pronuncia in questione ha suscitato grande interesse,

¹⁷⁷ Le prime pronunce di “*moral suasion*” dell'AGCM risalgono alle estati del 2017 e del 2018, con riferimento rispettivamente agli *influencer* più noti e ai c.d. *micro-influencer*.

¹⁷⁸ Di *influencer marketing* si parla già in un articolo di G. SATELL, “3 Reasons to Kill Influencer Marketing”, su *Harvard Business Review*, 2014; v. anche S. SARDELLA, “*Influencer marketing e Fashion Law*”, su *iusinitinere.it*, 19 aprile 2020.

¹⁷⁹ Per la disciplina del Regolamento *Digital Chart* si veda M. RACO, “*La Digital Chart: una prima regolamentazione dell'influencer marketing*”, su *iusinitinere.it*, 5 maggio 2020; v. anche C. PAPPALARDO, “*Influencer e Autodisciplina pubblicitaria – prime applicazioni della Digital Chart*”, su *DeJure*.

¹⁸⁰ Il caso è sorto a seguito di un reclamo cautelare presentato dalla Ferrari S.p.A. contro un famoso stilista tedesco, accusato di aver pubblicato, sul suo profilo *social* di Instagram, numerosi *post* e *stories* pubblicizzando calzature accanto al cofano della nota auto di lusso che porta il marchio Ferrari. Il Tribunale di Genova, con ordinanza n. 15949 del 30 gennaio 2020, pubblicata il 4 febbraio, ha

da un lato perché si tratta di una delle primissime applicazioni del Codice della Proprietà Industriale al nuovo e specifico contesto dei *social network*, dall'altro perché vi si trova una grande estensione della tutela riconosciuta al titolare del marchio, al di là della funzione distintiva propria dello stesso.

Più in generale, la diffusione di casi in cui il marchio celebre altrui è utilizzato non in funzione distintiva, bensì di agganciamento, è un tema che sta suscitando molto interesse. In alcuni casi, addirittura, il marchio viene utilizzato in maniera occulta, in funzione della presentazione di prodotti di concorrenti (ad esempio nei *marketplace* e nei *recommender system*).

Sul tema, per quanto concerne l'ambito europeo e la legislazione europea, il riferimento obbligato è al “*Social media discussion paper*”, rilasciato dall'Ufficio dell'UE per la Proprietà Intellettuale (EUIPO), il quale ha evidenziato ed esaminato le violazioni di diritti IP in cui è possibile incorrere attraverso l'utilizzo dei *social media*; contestualmente, è stata suggerita l'adozione di alcune *good practices* allo scopo di impedire – o quantomeno arginare – gli effetti negativi che ne potrebbero derivare.

Anche la Corte di Giustizia è intervenuta sul tema relativo alle regole procedurali applicabili nel caso di azioni civili promosse per la contraffazione di marchi europei e nazionali, in cui siano parti due o più Stati Membri.

Non è una novità, dunque, che l'avanzare dell'utilizzo di Internet, e soprattutto la diffusione dei *social network*, stiano modificando, rivoluzionandolo del tutto, il mondo della pubblicità e della tutela dei marchi.

Anzitutto, è necessario volgere lo sguardo alle problematiche poste dalla pubblicità occulta e dalla tutela degli utenti-consumatori.

Nel nostro ordinamento, è in particolare il Codice del Consumo a fornire le direttive che devono essere seguite nell'ambito delle attività pubblicitarie. Le regole ivi contenute, infatti, tutelano il consumatore tramite la predisposizione di norme finalizzate a garantire la massima trasparenza; è necessario, come prima cosa, assicurarsi che il destinatario del messaggio pubblicitario sia posto nella facoltà di discernere la natura commerciale di una data comunicazione, attraverso l'inserimento di appositi *disclaimer*.

Per applicare questa disciplina è stato inevitabile un confronto con l'evoluzione delle tecnologie e dei mezzi di comunicazione, dapprima con riferimento alle opere audiovisive e, da ultimo, ai *social network*.

Per quanto riguarda quest'ultimo profilo, con l'espressione “*influencer marketing*”¹⁸¹ si intende – secondo una definizione condivisa dall'Autorità Garante per la Concorrenza e per il Mercato – “una modalità consolidata di comunicazione,

ritenuto che il marchio fosse da considerarsi notorio, e che lo stilista *influencer* lo abbia utilizzato in maniera scorretta (v. *infra*).

¹⁸¹ Per un'analisi del fenomeno dell'*influencer marketing*, v. anche J. CIANI, M. TAVELLA, “La riconoscibilità della natura pubblicitaria della comunicazione alla prova del digital: native advertising tra obbligo di disclosure e difficoltà di controllo”, in “*Social media e diritto. Diritti e social media*” della Rivista Informatica e Diritto, 2017.

consistente nella diffusione su blog, vlog e social network (come Facebook, Instagram, Twitter, YouTube, Snapchat, Myspace) di foto, video e commenti da parte di blogger e influencer che mostrano sostegno o approvazione (endorsement) per determinati brand, generando un effetto pubblicitario”.

Differentemente dal caso dei tradizionali canali di pubblicità, l’AGCM ha rilevato che la condivisione da parte degli *influencer*, sul proprio profilo privato, genera nell’utente-consumatore la sensazione di una maggiore credibilità del messaggio, poiché questo è inserito “*in un flusso che dà l’impressione di una narrazione privata della quotidianità dell’influencer, che coinvolge i destinatari nel proprio racconto*”.

Il fenomeno in esame è talmente diffuso che, ormai, si assiste anche ad una sua evoluzione, che può essere ravvisata nel coinvolgimento sempre maggiore di soggetti che non godono di un numero di *followers* così elevato (si tratta dei c.d. *microinfluencer*).

Analizzando la disciplina del Codice del Consumo, agli artt. 22 e 23 in materia di pubblicità occulta – che sicuramente trovano applicazione anche qui – notiamo che le norme impongono l’adozione di specifici accorgimenti che consentano al consumatore di identificare in maniera chiara la presenza di un messaggio pubblicitario.

Nel caso specifico dei messaggi pubblicitari veicolati attraverso i *social network*, è interessante analizzare l’intervento dell’Istituto di Autodisciplina Pubblicitaria (IAP). L’istituto ha pubblicato la “*Digital Chart*”¹⁸², un importante documento che riporta le regole e le misure che tutti gli *influencer* sono obbligati a rispettare affinché l’attività di pubblicizzazione dei prodotti delle loro imprese digitali soddisfi il requisito della c.d. “*riconoscibilità*”. Si tratta della necessità che, al di là dello strumento utilizzato per porre in essere la comunicazione commerciale, se ne deve sempre garantire la piena riconoscibilità. La *Digital Chart*, che nell’ambito dell’accordo-quadro stipulato fra l’AGCM e l’Istituto¹⁸³ ha trovato anche l’approvazione dell’Autorità, distingue varie ipotesi, a seconda del tipo di contenuto condiviso sui *social*.

La *prima ipotesi* analizzata è quella del c.d. “*endorsement*”, che si sostanzia nell’attività di chi accredita un prodotto per persuadere il pubblico al suo acquisto¹⁸⁴. All’interno di questa fattispecie, bisogna ulteriormente distinguere due casi: il caso in cui il rapporto fra il titolare del *brand* e l’*influencer* sia un rapporto di committenza e il diverso caso in cui il rapporto abbia natura meramente occasionale (es. invio gratuito di prodotti o dietro modico corrispettivo).

¹⁸² Regolamento *Digital Chart* sulla riconoscibilità della comunicazione commerciale diffusa attraverso internet, emanato nel 2016 dall’Istituto di Autodisciplina Pubblicitaria, disponibile qui <https://www.iap.it/wp-content/uploads/2016/05/Digital-Chart-IAP-VERSIONE-ONLINE.pdf>; sul tema vedi anche E. NUNZIANTE, “*Influencer e pubblicità, quale trasparenza: che fare*”, su *agendadigitale.eu*, 30 ottobre 2019; G. IOZZIA, “*Influencer marketing e quadro normativo*”, su *altalex.com*, 17 luglio 2019.

¹⁸³ Il testo dell’accordo è disponibile su <https://www.iap.it/wp-content/uploads/2018/06/Accordo-quadro-AGCOM-IAP-amc.pdf>.

¹⁸⁴ Vedi anche R. MAZZUCCONI, “*L’influencer marketing e il rapporto di endorsement tra aziende e influencers: profili giuridici e derive illecite*”, su *cyberlaws.it*, 21 maggio 2020.

Nel caso di rapporto di committenza, è necessario che la natura commerciale della comunicazione *social* sia resa esplicita tramite l’inserimento – nella *caption* che accompagna il *post* o le *stories* (in modo tale che la dicitura sia ben visibile rispetto agli elementi promozionali) – di diciture quali “Pubblicità/Advertising”, o “Promosso da...brand/Promoted by...brand” o “Sponsorizzato da...brand/Sponsored by...brand”, o “in collaborazione con...brand/In partnership with...brand”; e/o nel caso di un post entro i primi tre *hashtag*, purché di immediata percezione, una delle seguenti diciture: “#Pubblicità/#Advertising”, o “#Sponsorizzato da...brand/#Sponsored by...brand”, o “#ad” unitamente a “#brand”.

Se il rapporto tra il *brand* e l’*influencer* ha natura meramente occasionale, invece, è sufficiente che l’*influencer* inserisca un *disclaimer* del tenore di “prodotto inviato da...brand”, o equivalente. La particolarità, qui, è che l’inserzionista è in ogni caso tenuto, al momento dell’invio del prodotto, ad informare l’*influencer* riguardo quest’ultimo obbligo.

Allo stesso modo, anche nella *seconda ipotesi*, ossia nel caso in cui la comunicazione commerciale sia diffusa sul web mediante un video¹⁸⁵, bisogna distinguere a seconda della natura del rapporto giuridico esistente fra le parti. Se fra inserzionista e *influencer* esiste un rapporto di committenza, la *Digital Chart* richiede che sia la descrizione del video che le scene iniziali dello stesso debbano riportare delle avvertenze scritte che ne rendano chiara ed esplicita la natura commerciale; si precisa che, nei video in *streaming*, queste avvertenze devono essere ribadite nel corso della trasmissione. I *disclaimer* devono altresì comparire alla fine del video, nonché ogni volta che siano inquadrati in maniera specifica i prodotti inseriti a fini commerciali.

Nel caso in cui, invece, le parti siano legate da un rapporto meramente occasionale, l’*influencer* può limitarsi ad inserire in apertura del video un *disclaimer*, che può essere sia in forma verbale che in forma scritta, del tenore di “questo prodotto mi è stato inviato da...”; in questo caso, resta ferma la responsabilità dell’inserzionista di informare l’*influencer* sull’esistenza di tale obbligo.

A causa della violazione di queste ultime regole, l’AGCM potrebbe irrogare una sanzione nei confronti dei cantanti Fedez, Orietta Berti e Achille Lauro per il videoclip caricato su *Youtube* del brano musicale “Mille”¹⁸⁶.

Lo scorso settembre, infatti, è pervenuta una segnalazione del Codacons, e l’Autorità ha aperto un’indagine istruttoria per verificare la configurabilità di pubblicità occulta in favore del marchio Coca-cola. Secondo il comunicato stampa diffuso dal Codacons,

¹⁸⁵ Per un accurato approfondimento del *Product Placement* si veda M. RACO, “Product placement ai limiti della pubblicità occulta: Baby K e Chiara Ferragni per Pantene”, su *iusinitinere.it*, 3 gennaio 2021; P. F. CARBALLO-CALERO, “Pubblicità occulta e product placement”, Cedam, 2004; vedi anche V. D’ANTONIO e D. TARANTINO, “Il product placement nell’ordinamento italiano: breve fenomenologia di uno strumento pubblicitario”, in *Comparazione e Diritto Civile*, 2011.

¹⁸⁶ V. “Pubblicità occulta alla Coca Cola nel video di “Mille”: Fedez rischia una multa di 5 milioni dall’Antitrust”, su *codacons.it*, 5 settembre 2021; E. SIMIONATO e M. E. ORLANDINI, “Fedez, Mille e Coca Cola: è davvero pubblicità occulta?”, su *iusinitinere.it*, 8 luglio 2021.

il motivo della contestazione non sarebbe tanto il testo del brano musicale, libera espressione dell'artista, quanto il video promozionale dello stesso, che non reca indicazioni sufficienti a chiarire la natura commerciale della comunicazione, mostrando durante l'intero video, in più occasioni, il marchio della nota bevanda.

Per quanto riguarda la *terza ipotesi*, si tratta della fattispecie in cui la promozione del prodotto avvenga esclusivamente mediante l'invito dell'*influencer* a partecipare ad un determinato evento. Poiché la fattispecie dà luogo ad un rapporto occasionale, secondo la disciplina della *Digital Chart* l'*influencer* deve solamente informare il pubblico, dal momento in cui fa pubblicità dei contenuti riguardanti l'evento, che la propria partecipazione è legata ad invito da parte del professionista (il quale comunque rimane obbligato ad informare in tal senso).

Per quanto concerne i contenuti generati dagli utenti (c.d. "*user generated content*"), è parimenti richiesta l'adozione di una delle misure su indicate per precisare la natura della comunicazione. A tal proposito, si segnala che l'Autorità Garante ha recentemente avviato un'indagine istruttoria¹⁸⁷ dopo che alcuni noti *influencer* avevano pubblicato *post* e *stories* chiedendo ai propri *followers* di ripubblicare (c.d. *repost*) loro contenuti con l'utilizzo di specifici *tag* e *hashtag* riconducibili alla promozione del prodotto *Glo Hyper*.

In questo caso viene in rilievo, più che altro, il problema relativo all'attività pubblicitaria posta in essere *indirettamente* dagli utenti, e i quesiti che ci poniamo sono i seguenti: qual è la natura degli ulteriori *post* pubblicati dagli utenti? Qual è, inoltre, l'impatto che ne deriva sugli altri utenti?

È normale che sia molto più complicato, in questo caso, riconoscere in maniera lampante la natura commerciale delle comunicazioni. Non a caso, nel comunicato stampa divulgato dall'AGCM il 21 maggio 2021, si legge: "*L'intervento si inserisce nell'ambito di un filone di indagine che, seguendo le evoluzioni delle tecniche di marketing adottate sui social media, punta a colpire le comunicazioni apparentemente neutrali e disinteressate ma in realtà strumentali a promuovere un prodotto e, come tali, in grado di influenzare le scelte del consumatore*".

Secondo la nuova disciplina, occorre inserire *disclaimer* anche in altri casi riconducibili alle seguenti ipotesi: "*In-feed units*" (ossia contenuti redazionali), "*paid search units*" (risultati di ricerca sponsorizzati), "*in App advertising*" (app con contenuto pubblicitario), "*recommendation widgets*" (contenuti raccomandati) e "*advergame*" (giochi promozionali).

Bisogna ora porre l'attenzione sull'evoluzione che l'approccio adottato nei confronti degli *influencer* dall'Autorità Garante della Concorrenza e del Mercato ha avuto negli ultimi anni.

¹⁸⁷ Accessibile da <https://www.agcm.it/media/comunicati-stampa/2021/5/PS12009>; v. E. SIMIONATO, "AGCM e pubblicità occulta: aperto il procedimento istruttorio nei confronti di BAT e Stefano De Martino, Cecilia Rodriguez e Stefano Sala", su iusinitinere.it, 1° giugno 2021.

In passato, l'approccio dell'Antitrust si è sempre limitato all'adozione di decisioni di *moral suasion*: si trattava di strumenti di *soft law*, di meri inviti, diretti alle imprese digitali, volti a far adeguare gli *influencer* alle disposizioni della *Digital Chart* e del Codice di autodisciplina dell'IAP.

Ultimamente, invece, l'Autorità ha avviato diverse indagini per pubblicità occulta, a causa dell'importanza assunta da questo fenomeno sul mercato e sulla concorrenza. E proprio tramite varie pronunce adottate dall'Autorità nell'ambito di questi procedimenti, sono state elaborate vere e proprie linee-guida, che permettono ad aziende e *influencer* di avere un punto di riferimento per adeguarsi alle misure e per adottare i giusti accorgimenti, al fine di evitare l'insorgenza di violazioni e l'irrogazione di sanzioni.

Uno dei primi casi in cui si è pronunciata l'Autorità è quello relativo all'indagine per pubblicità occulta scaturita dalla pubblicazione, sui profili Instagram di diversi *influencer*, di post raffiguranti immagini di capi firmati da Alberta Ferretti in cui appariva inquadrato il logo di Alitalia, indagine conclusasi con l'importante Provvedimento n. 27787/19¹⁸⁸. Si è configurata, nel caso di specie, una possibile violazione degli artt. 22 e 23, comma 1, lett. m) del Codice del Consumo, in quanto nella pubblicazione dei *post* suddetti sembrava chiaro l'intento promozionale, sia considerando la proporzionalità della citazione dei marchi, sia valutando il contesto in cui erano inseriti i *post*. Nonostante ciò, non era possibile, per l'utente consumatore che avesse visionato detti *post*, identificare chiaramente la natura commerciale della comunicazione.

A seguito dell'apertura delle indagini istruttorie, Alitalia ha inoltrato alle imprese digitali coinvolte la raccomandazione ad adeguarsi alla normativa sulle pratiche commerciali scorrette. A ciò si è aggiunto, da un lato, l'impegno ad adottare specifiche linee-guida per definire le regole di condotta che gli *influencer* devono seguire, poiché parte dell'accordo di collaborazione commerciale stipulato con la società, e dall'altro, l'introduzione – nei contratti di *co-marketing* per la concessione della licenza del marchio Alitalia e nei contratti di licenza del marchio a fini promozionali – dell'obbligo per i *partner* commerciali di adottare tutte le misure e le cautele necessarie per evitare che si verificino fenomeni di pubblicità occulta. Se suddetto obbligo viene violato, si attiva una specifica procedura di avvertimento, che potrebbe anche concludersi con l'irrogazione di una penale. Anche la società di riferimento del marchio di Alberta Ferretti, *Aeffe*, ha assunto impegni simili.

Per quanto riguarda gli *influencer* coinvolti, essi si sono specificatamente impegnati a rispettare quanto previsto sull'utilizzo di *hashtag* e diciture varie nella pubblicazione dei *post*, al fine di rispettare la disciplina contenuta nella *Digital Chart*.

¹⁸⁸ Testo del provvedimento disponibile su [https://www.agcm.it/dotcmsCustom/tc/2024/6/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/E6B624BBD0F6A573C12584150049D1EE/\\$File/p27787.pdf](https://www.agcm.it/dotcmsCustom/tc/2024/6/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/E6B624BBD0F6A573C12584150049D1EE/$File/p27787.pdf); v. B. MANCA, "L'Antitrust apre istruttoria su Alitalia e Aeffe di Alberta Ferretti: nel mirino anche le foto di influencer: "pubblicità non riconoscibile", su ilfattoquotidiano.it, 15 dicembre 2018.

Dal momento che gli impegni assunti dalle parti coinvolte sono stati ritenuti idonei, l'istruttoria si è conclusa senza accertamento di infrazione; tuttavia, l'Autorità ha ritenuto di ordinare alle parti suddette di dare attuazione alle misure proposte, avvertendo che, in caso di mancata ottemperanza, sarà applicata una sanzione amministrativa pecuniaria da 10.000 a 5.000.000 euro, nonché la sospensione dell'attività per un periodo non superiore a trenta giorni se l'inottemperanza sarà reiterata.

Il secondo caso interessante da prendere in considerazione è quello relativo alla pubblicizzazione degli integratori alimentari prodotti da *JuicePlus+*. Il procedimento istruttorio – che si è concluso con il Provvedimento n. 27612/2019¹⁸⁹ – ha visto l'azienda protagonista porre in essere attività di divulgazione di informazioni sulle caratteristiche e la natura dei prodotti tramite gruppi segreti di Facebook; alcuni rivenditori dell'azienda portavano i consumatori ad entrare nei gruppi a fini promozionali. I *post* contestati dall'Autorità narravano l'esperienza personale di alcuni consumatori, mentre in alcuni casi l'amministratore della pagina Facebook condivideva esperienze di consumo personale o esperienze di terzi.

I contenuti della pagina erano accomunati da una forte enfattizzazione delle proprietà degli integratori e dei risultati ottenuti. Nell'indagine condotta dall'Autorità è emerso che alcuni dei soggetti che si presentavano come consumatori erano, in realtà, i rivenditori del prodotto. Ciò avveniva anche attraverso i profili privati degli stessi o all'interno di chat private su *Whatsapp*.

Non solo, è emerso anche che le informazioni divulgate erano fuorvianti e inesatte, sia sotto il profilo della qualità e delle proprietà dei prodotti venduti, sia sotto quello della modalità di utilizzo degli stessi.

L'istruttoria ha evidenziato, inoltre, che era stata la stessa azienda ad invitare i venditori a diventare “*brand di se stessi*”, promuovendo l'uso dei prodotti attraverso i propri profili sui *social network* e proponendosi come esempi da seguire nel proprio stile di vita. Il problema è che nelle operazioni e indicazioni dell'azienda non vi era alcun riferimento alla necessità di identificarsi chiaramente dinnanzi agli utenti-consumatori come venditori della stessa. Poiché, dunque, la condotta tenuta dalla società integra una pratica commerciale scorretta ai sensi degli artt. 20, 21, 22, comma 2 e 23, comma 1, lett aa) del Codice del consumo, l'Autorità ha accertato la violazione ed ha irrogato una sanzione amministrativa pecuniaria di 1.000.000 di euro.

Il terzo caso da prendere in considerazione è quello relativo alla società Barilla (Provvedimento n. 28167/2020¹⁹⁰), la cui vicenda pone in luce l'evoluzione del fenomeno dell'*influencer marketing*, facendo venire in rilievo il coinvolgimento dei c.d. *microinfluencer*. Anche in questo caso – relativo alla pubblicazione di *post* della

¹⁸⁹ Accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/PS11050_scorr-sanz_omi.pdf. v. anche l'articolo “*Vendite segrete integratori su Fb, Antitrust multa Juice Plus*” su *adnkronos.com*, 15 aprile 2019.

¹⁹⁰ Testo accessibile da https://www.agcm.it/dotcmsdoc/bollettini/2020/11-20_all.pdf.

linea di prodotti “*Pan di Stelle*” – la contestazione dell’Autorità riguardava la violazione delle norme dettate dal Codice del Consumo in materia di pubblicità occulta¹⁹¹. Ebbene, poiché tutte le parti coinvolte hanno formulato delle proposte di impegni concernenti l’adozione di misure volte a garantire maggiore trasparenza nella divulgazione dei contenuti di natura commerciale, l’istruttoria si è conclusa solamente con la disposizione dell’obbligo di dare attuazione agli impegni formulati, senza alcuna irrogazione di sanzione. Poiché in questo caso peculiare ad essere coinvolti sono stati i c.d. *microinfluencer*, le misure di cui si è proposta l’adozione differiscono leggermente da quelle oggetto del provvedimento di Alitalia, ma rispondono alla medesima *ratio* e alla necessità di trasparenza e tutela del consumatore.

Nell’analisi delle problematiche relative al nuovo mondo digitale, quella relativa al reparto di competenze fra le diverse autorità garanti che operano nel nostro Paese è sicuramente di grande rilievo. Complice la natura intrinsecamente trasversale dei problemi affrontati, urge un approccio sempre più sinergico tra le autorità, anche a causa della difficoltà, se non l’impossibilità, di distinguere nettamente fra le competenze attribuite all’una o all’altra istituzione. Per quanto riguarda, dunque, il fenomeno dell’*influencer marketing*¹⁹², si rileva che, pur riguardando prevalentemente il tema del consumo e ricadendo dunque entro l’ambito di competenza dell’AGCM, ci sono alcuni profili che rendono auspicabile – se non addirittura necessario – il coinvolgimento di altre autorità, prima fra tutte l’AGCOM.

Il commissario dell’AGCOM, Laura Aria, ha analizzato il tema, esaminando quale potrebbe essere l’impatto della Direttiva SMAV (Servizi Media AudioVisivi) e delle proposte della Commissione Europea sui mercati digitali (DMA e DSA), se le stesse fossero approvate. È noto che la crescente importanza delle piattaforme *online* ha portato alla necessità di regolamentare più compiutamente un settore che, fino a poco tempo fa, non era stato adeguatamente studiato nelle proprie peculiarità. Per quanto riguarda la nuova Direttiva SMAV, essa riconosce, per la prima volta, l’equiparabilità delle piattaforme di *video sharing* rispetto ai *media* tradizionali, con tutte le conseguenze che ne derivano in termini di responsabilità. E non solo.

Da tale equiparazione deriva, infatti, la legittimazione dell’AGCOM ad intervenire per svolgere la propria attività di controllo. Ma siccome la Direttiva volge la propria attenzione anche ai pericoli in cui incorrono i consumatori nell’utilizzo delle piattaforme video, l’ambito di competenza dell’autorità deve ritenersi esteso anche a questi profili, soggetti, come noto, al controllo da parte dell’AGCM.

È un profilo molto innovativo; si pensi al fatto che la SMAV prevede anche l’introduzione di meccanismi di risoluzione extragiudiziale delle controversie e di

¹⁹¹ G. DE CRISTOFARO, “*Influencer Marketing: caso ‘Crema Pan di Stelle’*. Come nel caso Alitalia-Ferretti nessuna sanzione. L’Antitrust accetta gli impegni di Barilla e dei Micro-Influencer. tanto rumore per nulla? Non si direbbe: altri spunti utili per inserzionisti e influencer”, su youmark.it, 17 marzo 2020.

¹⁹² Sul tema v. anche S. BARCO, “*Il contratto di Influencer marketing: profili civilistici del rapporto tra brand ed influencer*”, su iusinitinere.it, 28 maggio 2020.

indennizzo nel caso di disservizi a scapito dei consumatori, la cui definizione procedurale potrebbe ragionevolmente spettare proprio all'AGCOM.

Si pensi anche alle proposte della Commissione europea per la regolamentazione dei mercati digitali: esse andrebbero senza dubbio ad incidere sul profilo suddetto.

Il *Digital Services Act* interviene, infatti, sul regime di responsabilità delle piattaforme *online*, qualificate come servizi di *hosting provider*, alle quali verrebbe applicato un sistema che ricalca quello previsto attualmente dall'art. 17 della Direttiva *e-commerce*. Si prevede l'individuazione di una o più autorità competenti all'interno di ciascun Stato Membro, che garantiscano l'effettiva applicazione della disciplina e svolgano attività di controllo: ebbene, una delle possibilità sarebbe quella di attribuire tali poteri proprio all'AGCOM.

Dal canto suo, il *Digital Markets Act* pone, invece, il tema della potenziale concorrenza dell'AGCOM e dell'AGCM quali Garanti per l'applicazione del Regolamento, dato che si includono anche le piattaforme video fra i soggetti potenzialmente qualificabili come “*gatekeeper*” (ossia le piattaforme *online* che controllano gli accessi ai mercati) e quindi destinatari della disciplina ivi prevista.

Oltre al profilo della pubblicità occulta, c'è un altro ambito in cui viene in rilievo l'attività degli *influencer*, ossia quello legato all'utilizzo dei marchi e alla tutela dei diritti di soggetti terzi.

Si pensi, anzitutto, alla possibilità che la promozione dei prodotti mediante l'*influencer marketing* contrasti con il rispetto della disciplina sulla tutela dei dati personali, dal momento che l'immagine di una persona, tale da consentirne l'identificazione, viene considerata un dato personale e, perciò, non è ammissibile la sua divulgazione senza il consenso da parte dell'interessato.

È lecito affermare, dunque, che l'utilizzo di un'immagine di un *influencer* a fini promozionali, se manca uno specifico accordo in tal senso, può integrare gli estremi di una violazione della suddetta disciplina.

Si deve anche avere riguardo della necessità di tutelare i diritti di paternità dell'opera e di natura patrimoniale attribuibili al fotografo che ha realizzato l'immagine.

Si devono considerare, inoltre, le ipotesi nelle quali l'immagine, che si usa per sponsorizzare un dato prodotto, presenti anche marchi ulteriori; in tale circostanza la condotta può portare ad una violazione dei diritti di esclusiva, che sono riservati al titolare del marchio, potendo anche integrare la fattispecie di concorrenza sleale.

Un esempio di violazione della normativa che tutela il marchio da parte di attività di *influencer marketing* è il caso deciso dal Tribunale di Genova che, con l'ordinanza n. 15949/2020¹⁹³, ha applicato per la prima volta l'art. 20, comma 1, lett. c) del Codice della Proprietà Industriale allo specifico contesto dei *social network*.

¹⁹³ L'ordinanza è commentata da S. GIANCONE, “*Influencer e social network: quando l'uso di un marchio altrui è un atto illecito*”, su iusinitinere.it, 8 ottobre 2020.

Si tratta di un caso in cui a venire in rilievo è stato un marchio notorio, e dunque l'articolo, in questi casi, prevede che l'utilizzo di tale marchio è illecito, anche per fini diversi da quello di distinzione di prodotti e servizi, se “*senza giusto motivo consente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio stesso*”. Dunque, l'utilizzo del marchio notorio sui *social network* da parte di terzi è lecito soltanto se non è effettuato a fini commerciali o se è espressamente autorizzato dal titolare del marchio stesso.

Nel caso di specie, l'*influencer* tedesco Philipp Plein aveva pubblicato numerose foto promozionali di un paio di calzature sul cofano di una delle autovetture della nota casa automobilistica Ferrari, inquadrandone chiaramente il marchio, senza godere di alcuna autorizzazione in tal senso.

Il Tribunale, con l'ordinanza del 30 gennaio 2020, pubblicata il successivo 4 febbraio, ha evidenziato che nel caso di specie non fosse riscontrabile alcuno scopo ad esclusione di quello di favorire la pubblicizzazione delle calzature. I giudici hanno, pertanto, considerato illecita la condotta tenuta dall'*influencer*, che è stato condannato a rimuovere i *post* oggetto del contenzioso e, inoltre, è stata imposta l'inibizione a qualsiasi futuro utilizzo del marchio in questione (pena l'irrogazione di una sanzione pari a 20.000 euro per ogni violazione).

Altro profilo che viene in rilievo nel caso di specie è quello che concerne il c.d. offuscamento (o *dilution by tarnishment*), ossia l'ipotesi in cui l'utilizzo da parte di terzi del segno/marchio rechi pregiudizio al titolare, poiché alternativamente rovina l'immagine dello stesso agli occhi del pubblico oppure viene inserito in un contesto che si pone in contrasto rispetto all'immagine promossa in precedenza, vanificando gli sforzi del titolare per promuoverla. Ebbene, in questo caso è stata contestata la pubblicazione sul *social network* di video ritraenti giovani donne in abiti succinti, intente nel lavaggio di un'autovettura della nota casa automobilistica, sul cofano della quale erano collocate le calzature oggetto di promozione commerciale.

È necessario anche analizzare il profilo relativo all'utilizzo degli *hashtag*.

Una domanda che ci si è posti è la seguente: è possibile qualificarli come marchi, riconoscendone la funzione di segno distintivo?¹⁹⁴

Partiamo dal presupposto che la funzione degli *hashtag* è molto diversa: trattandosi di strumenti finalizzati a facilitare le ricerche da parte degli utenti, raggruppano prodotti e servizi simili sotto una stessa dicitura; dunque, gli stessi rispondono ad una *ratio* completamente diversa dai marchi.

In più, bisogna considerare che applicargli la disciplina della tutela dei marchi, limitandone di conseguenza l'utilizzo, rischierebbe di limitare in maniera ingiustificata la libertà di espressione degli utenti. È anche vero, però, che in maniera sempre più diffusa si verificano sui *social* episodi di agganciamento a marchi noti, proprio tramite lo strumento dell'*hashtag*, che ricollega tramite un click un determinato marchio.

¹⁹⁴ Sul tema, v. L. BERTO, “*E' possibile registrare un hashtag come marchio?*”, su *iusinitinere.it*, 13 novembre 2017.

Proprio per questo, è lecito chiedersi se un diritto di registrazione degli *hashtag* come marchi possa esistere, e se questi possano godere o meno dei requisiti necessari per poter essere qualificati come tali, primo fra tutti la capacità distintiva.

Purtroppo, la normativa italiana, come la disciplina europea, non è chiara sul punto, e neanche la giurisprudenza è riuscita a dettare direttive da seguire, potendo essere considerate rilevanti sul punto soltanto le pronunce che sanciscono il divieto di utilizzo non autorizzato del marchio altrui come *AdWords* o *keyword*.

Ebbene, su questo elemento si è espresso il Tribunale di Milano nel 2018¹⁹⁵: i giudici hanno censurato l'utilizzo del marchio da parte di terzi al solo scopo parassitario, per sfruttare la rinomanza del nome del marchio per accreditare i propri prodotti.

Bisogna ribadire, infatti, che il fine delle parole chiave è quello di fornire all'utente la possibilità concreta di scegliere tra le alternative commerciali presenti sul mercato.

Comunque, nel silenzio del legislatore sul punto, in ragione della crescente importanza dell'utilizzo degli *hashtag* sul mercato, molti produttori hanno iniziato a registrarli insieme ai marchi.

L'interesse verso i rischi legati alla tutela dei diritti di proprietà intellettuale, nel contesto emergente dei *social network*, è cresciuto anche in ambito europeo, dove si assiste ad una approfondita analisi della questione da parte dell'EUIPO, in particolare nel documento "*Social Media Discussion Paper*"¹⁹⁶, il cui intento è quello di evidenziare le violazioni che, in particolare, avvengono attraverso i *social*, ma anche quelle violazioni riconducibili esclusivamente al particolare contesto dei *social media*. È anche riportato l'ambito concernente i casi in cui i *social network* non costituiscono di per sé il mezzo con cui avvengono le violazioni dei diritti IP, ma piuttosto rappresentano lo strumento di divulgazione di informazioni concernenti siti che ne sono responsabili.

Nella prima ipotesi, sono ricompresi i servizi come l'*hosting*, lo *streaming* e il *live streaming*. Inoltre, l'utilizzo dei *social media* può portare a sponsorizzare contenuti che violano i diritti di proprietà intellettuale, tramite sponsorizzazioni che rimandano gli utenti-consumatori ad altri siti e pagine esterne.

È importante la distinzione tra questa categoria e quella, diversa, che riguarda più nello specifico l'attività degli *influencer*, che promuovono i prodotti attraverso i propri *account social*.

L'EUIPO ha approfondito il profilo relativo ai possibili casi di contraffazione del marchio. Si fa l'esempio di *influencer* che incoraggiavano i propri utenti-*followers* ad acquistare la versione economica di prodotti noti.

¹⁹⁵ Tribunale di Milano, sentenza n. 830/2018 del 25 gennaio 2018, commentata da E. BADIALI, "*Il caso Barilla e la tutela del marchio rinomato: commento alla sent. n. 830/2018 del Tribunale di Milano*", su *iusinitinere.it*, luglio 2018.

¹⁹⁶ Il testo è accessibile da https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Social_Media/2021_Social_Media_Discussion_Paper_FullR_en.pdf.

Un altro esempio interessante è quello dei c.d. “*burner accounts*”, *account* che vengono utilizzati al fine di attirare gli utenti di siti riconducibili ai legittimi titolari del marchio verso altre pagine, che invece divulgano contenuti illeciti.

Quest’ultima fattispecie va tenuta distinta da quella degli “*scam accounts*” i quali, invece, sfruttano i marchi noti allo scopo di ingannare gli utenti, indirizzando loro verso siti illeciti o, addirittura, per sottrargli dati della carta di credito o simili.

Sul tema della contraffazione del marchio sui *social network*, anche se relativamente ad un profilo diverso, si è espressa pure la giurisprudenza italiana.

Il Tribunale di Milano, nell’ordinanza pubblicata il 15 ottobre 2019¹⁹⁷, ha statuito che l’uso del marchio da parte di terzi sulle piattaforme *social* come Instagram e Facebook, anche se non in funzione distintiva, integri comunque la fattispecie di contraffazione del marchio, in quanto idoneo a creare negli utenti confusione, anche tenuto conto del fatto che le due imprese coinvolte operavano nel medesimo settore merceologico. All’esito del procedimento, l’organo giudicante ha ravvisato la sussistenza del *fumus boni iuris* e del *periculum in mora*, disponendo nei confronti del resistente l’inibitoria all’utilizzo del marchio altrui su tutti i *social network*.

Uno dei caratteri peculiari dei *social network* è la possibilità per gli utenti di comunicare su vari livelli, sia pubblicamente che attraverso gruppi chiusi e accessibili solo a specifici iscritti.

Ebbene, secondo gli esperti, questa seconda funzionalità viene sfruttata allo scopo di eludere l’applicazione della disciplina sulla proprietà intellettuale. I gruppi chiusi creati sui *social* divengono, quindi, strumenti finalizzati a condividere con gli utenti contenuti che violano i diritti IP, oppure link che li rimandano a siti parimenti illeciti, nascosti dall’occhio pubblico. In altri casi ancora, invece, viene sfruttata la criptazione delle chat private, grazie alla quale, per esempio, comunicazioni relative ai pagamenti dei prodotti sono protette.

Il *Social Media Discussion Paper*, nell’individuare le maggiori problematiche poste dalle violazioni dei diritti IP attraverso l’uso dei *social media*, esamina la disciplina vigente a livello europeo, ponendo in evidenza, fin da subito, che uno degli elementi che ne limita maggiormente l’efficacia è la circostanza che, attraverso i *social network*, gli utenti hanno a disposizione funzionalità molto diverse fra loro, tra cui rientrano la diffusione di vari dati e contenuti. Questo fa sì che le regole applicabili divengono svariate, e tale frammentazione del quadro normativo si pone in contrasto con la garanzia di un intervento efficace.

Nel documento, la prima grande distinzione prevista è quella fra contenuti disponibili pubblicamente e contenuti di natura privata.

¹⁹⁷ Pronunciata nell’ambito del procedimento cautelare n. r.g. 23037/2019, disponibile su [https://www.sistemaproprietaintellettuale.it/giurisprudenza/procedimenti-giurisdizionali/merito/17542-tribunale-milano-ord-15-10-2019-marchio-registrato-inibitoria-all-uso-del-marchio-marchio-figurativo-uso-segno-distintivo-di-ramo-di-azienda-acquistato-contraffazione.html?title=Tribunale%20Milano%20\(ord.\),%2015/10/2019](https://www.sistemaproprietaintellettuale.it/giurisprudenza/procedimenti-giurisdizionali/merito/17542-tribunale-milano-ord-15-10-2019-marchio-registrato-inibitoria-all-uso-del-marchio-marchio-figurativo-uso-segno-distintivo-di-ramo-di-azienda-acquistato-contraffazione.html?title=Tribunale%20Milano%20(ord.),%2015/10/2019).

Nel caso di contenuti privati, si pongono le questioni relative alla normativa sulla protezione dei dati personali, con riguardo, da un lato, alla possibilità di divulgare i dati privati dei soggetti responsabili delle violazioni e, dall'altro, alla tutela della riservatezza delle comunicazioni.

Nel caso di contenuti pubblici, invece, trova applicazione la Direttiva *e-commerce*, che limita, ai sensi dell'art. 14, la responsabilità dell'*hosting provider*, precisando che il suo obbligo, nel caso in cui pervenga una segnalazione, è solamente quello di rimuovere tempestivamente eventuali contenuti illeciti, non essendo tenuto ad effettuare alcun controllo preventivo.

Questo è il quadro normativo vigente; eppure, ultimamente, la direzione verso cui si sta andando è quella di coinvolgere maggiormente le piattaforme, promuovendo la cooperazione fra queste e i titolari dei diritti di proprietà intellettuale, allo scopo di arginare il fenomeno della diffusione di contenuti illeciti.

Lungo questa direzione si colloca anche il *Digital Services Act*, ossia la recente proposta di Regolamento presentata dalla Commissione al Parlamento europeo, che, ribadendo l'assenza di un generale obbligo di monitoraggio, vuole introdurre obblighi di *due-diligence*, per facilitare la rimozione dei contenuti illeciti, anche al fine di assicurare maggiore trasparenza.

Si ricorda, peraltro, che la regolamentazione di queste nuove materie è particolarmente complessa, potendo essa incidere direttamente sui diritti e le libertà fondamentali degli individui.

Bisogna ricordare, inoltre, che i *social network* sono soggetti all'applicazione di altre due fonti normative dell'Unione Europea, la Direttiva UE 48/2004¹⁹⁸ sull'applicazione dei diritti di proprietà intellettuale (*IPRED*) e la Direttiva UE 29/2001¹⁹⁹ sull'armonizzazione di alcuni aspetti del *copyright* e altri diritti nella società dell'informazione (*INFOSOC*).

Infine, nel caso in cui i *social media* siano utilizzati per la divulgazione di contenuti tutelati da *copyright*, si applica la Direttiva *Copyright*²⁰⁰.

Passando ai contenuti ed alle chat private, le maggiori perplessità sono sorte riguardo alla possibilità di qualificare le comunicazioni istantanee che avvengono attraverso i *social media* come comunicazioni elettroniche ai sensi della Direttiva *e-Privacy*²⁰¹, garantendo l'applicazione del relativo regime di tutela ivi previsto.

¹⁹⁸ Il testo della direttiva sull'applicazione dei diritti di proprietà intellettuale (*IPRED*) è disponibile su [https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R\(01\):IT:HTML](https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):IT:HTML).

¹⁹⁹ Il testo della direttiva sull'armonizzazione di alcuni aspetti del *copyright* e altri diritti nella società dell'informazione (*INFOSOC*) è accessibile su <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32001L0029&from=IT>.

²⁰⁰ Il testo della direttiva *Copyright* è disponibile su <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L0790&from=RO>; v. anche L. SERRA, "Copyright e diritti nel mercato digitale: attuata la Direttiva UE", su altalex.com.

²⁰¹ Il testo della direttiva *e-Privacy* è accessibile da <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32002L0058&from=IT>.

In passato, infatti, i *social* erano rimasti esclusi da tale nozione, anche se vi erano state alcune pronunce discordanti della Corte di Giustizia, che avevano alimentato il regime di incertezza già presente.

Il quadro è ancora più incerto da quando è entrata in vigore, il 21 dicembre 2020, la Direttiva UE 1772/2018²⁰², contenente il c.d. Codice Europeo delle Comunicazioni Elettroniche, che ha introdotto una nuova definizione di comunicazioni elettroniche, includendovi tutti i servizi di comunicazione interpersonale. Si attendono maggiori chiarimenti sull'applicazione della disciplina con l'entrata in vigore del Regolamento *e-Privacy*, che sostituirà l'attuale Direttiva.

Nel documento, si prende in considerazione il problema legato alla nascita di nuovi *social media*, definiti come “*decentralizzati*”, in quanto basati su tecnologie *peer-to-peer*, come ad esempio la *blockchain*. La novità sta nel fatto che queste nuove realtà vanno a modificare la struttura tradizionale *client-server*, caratterizzata dalla circostanza che i dati e i contenuti degli utenti venissero gestiti e conservati in maniera *centralizzata* da una singola società.

Sono anche evidenziate le principali *good practices*: misure che devono essere prese per arginare il rischio di violazioni e che possono essere distinte in *preventive* e *reattive*. Tra le *misure preventive* rientrano, anzitutto, le condizioni contrattuali, nonché le linee-guida adottate da ogni società per regolare l'utilizzo dei propri servizi da parte degli utenti. Ci si riferisce a quanto esaminato sull'emergente fenomeno dell'*hate speech*, in relazione al quale le principali difese di Facebook si basavano proprio sulla violazione da parte degli utenti delle regole della *Community*.

Per rendere più efficace l'applicazione delle *policy*, bisognerebbe differenziare queste ultime sulla base delle funzionalità e dei servizi a cui s'intende applicarle.

È anche auspicabile che vengano introdotti e utilizzati sistemi di verifica degli *account social*, per garantire che questi corrispondano all'identità reale degli utenti-utilizzatori e per favorire l'identificazione dei soggetti che si rendono responsabili di atti illeciti. Oltre a questa misura, vi è anche l'introduzione, da parte di alcune piattaforme, di strumenti di identificazione più incisivi nei confronti di soggetti che sponsorizzano sui *social*, fornendo agli utenti informazioni utili sulla loro identità ed evitando così il rischio di violazione dei diritti di proprietà intellettuale attraverso l'attività di *influencer marketing*.

Alcune piattaforme, inoltre, usano misure in grado di controllare l'eventuale utilizzo distorto degli *account*: i gestori dei *social media* possono introdurre sistemi che permettono di identificare gli utenti bannati ed impedire loro di creare nuovi *account*, limitando la reiterazione di atti illeciti.

Bisognerebbe, inoltre, intervenire per impedire la creazione di molteplici profili riconducibili al medesimo utente, nonché introdurre dei sistemi di autorizzazione

²⁰² Il testo è accessibile da <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018L1972>; v. anche R. JACCHIA, M. STILLO, “Codice Ue delle comunicazioni elettroniche: la nuova normativa per un mercato più accessibile e sicuro”, su agendadigitale.eu, 30 aprile 2021.

differenziati, precludendo determinate funzionalità (es. l'accesso ai *servizi e-commerce*) agli account di nuova creazione.

Inoltre, i *social media* dovrebbero, da un lato, limitare l'utilizzo di parole chiave (compresi i marchi) all'interno del nome dell'utente; dall'altro, effettuare controlli circa l'identità dell'utente e il possesso da parte di quest'ultimo dei diritti e delle autorizzazioni necessarie all'utilizzo di un dato segno distintivo.

Le *misure reattive* ricomprendono, invece, i cosiddetti meccanismi “*notice and action*”. Si tratta, ad esempio, di specifici canali messi a disposizione dei titolari di diritti di proprietà intellettuale o degli utenti per segnalare presunte violazioni.

Tali strumenti possono risultare efficaci a seconda della presenza o meno di specifici elementi, che ne facilitano l'accesso e la comprensione²⁰³.

Tuttavia, affinché tali strumenti possano risultare pienamente efficaci, bisogna applicarli a tutte le funzioni dei *social media*, compresi i contenuti temporanei (“*stories*”) o gli *hashtag* che, come visto, possono essere utilizzati nella violazione dei diritti di proprietà intellettuale. Non bisogna dimenticare che sono anche i titolari dei diritti IP a dover osservare alcune *good practices*, come ad esempio l'utilizzo appropriato dei meccanismi appena elencati.

L'impiego delle nuove tecnologie (es. IA), inoltre, potrà essere utile per l'introduzione di nuovi e più rapidi sistemi per indagare eventuali violazioni.

Tra le misure di carattere reattivo rientra anche la collaborazione con le autorità pubbliche, competenti ad intervenire per tali violazioni.

Si faccia l'esempio fornito dall'operazione “*Aphrodite*”, condotta congiuntamente dall'EUROPOL, dalla Guardia di Finanza italiana e dalle forze di polizia di diversi Stati Membri, che ha portato al sequestro di 20.000 prodotti contraffatti e alla chiusura di oltre 1.000 conti. È un esempio concreto dell'effetto positivo derivante dalla collaborazione con le autorità, nonché dell'intervento sinergico fra queste ultime.

Il comunicato stampa trasmesso da EUROPOL evidenzia proprio il ruolo giocato dai *social media* nella divulgazione delle offerte di prodotti contraffatti per raggiungere il pubblico.

La tendenza di internet e dei *social media* ad abbattere i confini geografici ha creato non pochi problemi nell'applicazione della disciplina e nell'individuazione delle norme effettivamente applicabili.

Sul tema della contraffazione del marchio, nel caso specifico di contraffazione attraverso l'uso di nomi a dominio e sulle piattaforme *social*, la Corte di Giustizia si è pronunciata in via pregiudiziale per risolvere una questione legata alla litispendenza di azioni civili simultanee, sulla base di marchi nazionali e dell'Unione Europea.

²⁰³ Ad esempio, informazioni chiare sui soggetti legittimati ad effettuare la segnalazione, sugli elementi da includervi ecc; possibilità di segnalare molteplici violazioni mediante un singolo *report*; informare tempestivamente il soggetto segnalante dell'avvenuta rimozione del contenuto illecito.

Nel noto caso (causa C-231/16²⁰⁴) agiva *Merck KGaA*, operante nel settore chimico-farmaceutico e titolare di vari marchi che tutelano il nome “*Merck*”.

La società ha intrapreso contestualmente due azioni diverse, una innanzi alla *High Court of Justice* ed un'altra innanzi al *Landgericht Hamburg* (Tribunale regionale di Amburgo).

Nel primo caso, veniva in rilievo la contraffazione dei marchi nazionali ed internazionali protetti nel Regno Unito, a causa dell'utilizzo in rete del nome “*Merck*”.

Nel secondo caso, invece, si agiva a tutela del marchio UE *Merck*, per il suo utilizzo non solo su internet, ma anche sulle piattaforme Facebook, Twitter e Youtube.

Il giudice di Amburgo ha sollevato una questione sull'interpretazione dell'art. 109, para 1, del Regolamento (CE) n. 207/2009, che dispone: “*Qualora azioni per contraffazione siano proposte per gli stessi fatti e tra le stesse parti davanti a tribunali di Stati membri differenti, aditi rispettivamente sulla base di un marchio [dell'Unione Europea] e sulla base di un marchio nazionale:*

a) *il tribunale successivamente adito deve, anche d'ufficio, dichiarare la propria incompetenza a favore del primo tribunale adito quando i marchi in causa sono identici e validi per prodotti o servizi identici. Il tribunale che dovrebbe dichiarare la propria incompetenza può sospendere il procedimento qualora venga eccepita l'incompetenza dell'altro tribunale;*

b) *il tribunale successivamente adito può sospendere il procedimento quando i marchi in causa sono identici e validi per prodotti o servizi simili, nonché quando i marchi in causa sono simili e validi per prodotti o servizi identici o simili”.*

Con il primo quesito, è stato chiesto all'adita Corte di Giustizia se la locuzione “*stessi fatti*” debba essere intesa nel senso di includere il mantenimento e l'utilizzo in tutto il mondo – e quindi anche in tutta l'Unione Europea – di una pagina internet accessibile in modo identico da qualunque luogo, sotto lo stesso dominio, o, parimenti, di contenuti accessibili in modo identico di volta in volta con il medesimo *username*, sotto il dominio “*facebook.com*” e/o “*youtube.com*” e/o “*twitter.com*”.

Con un altro quesito, è stato poi chiesto alla Corte se il “*tribunale successivamente adito*” avesse l'obbligo di dichiarare la propria incompetenza solo sul territorio dello Stato membro in cui un altro Tribunale era stato adito per primo – a fronte di una violazione commessa mediante una pagina internet accessibile da tutto il mondo sotto lo stesso dominio o attraverso contenuti accessibili da tutto il mondo sotto il dominio “*facebook.com*” e/o “*youtube.com*” e/o “*twitter.com*” con il medesimo *username* – o se, invece, la dichiarazione di incompetenza dovesse estendersi a tutto il territorio dell'Unione Europea.

In primo luogo, la CGUE ha richiamato l'interpretazione relativa all'esistenza di domande aventi “*il medesimo oggetto e il medesimo titolo*”.

La nozione di titolo ricomprende i fatti e la norma giuridica posta a fondamento della domanda. La Corte ha rilevato che, nel caso di specie, la norma fondante la domanda

è coincidente ed individuabile nella tutela di diritti esclusivi derivanti da marchi identici. Non rileva, dunque, il fatto che la prima azione abbia quale fondamento la tutela di un marchio nazionale, mentre la seconda di un marchio europeo. Inoltre, può dirsi soddisfatto il requisito dell'identità dei fatti, dato che entrambe le questioni riguardano l'utilizzo del termine “*Merck*” in nomi di domini e in piattaforme *social* accessibili da tutto il mondo.

La nozione di oggetto, invece, coincide con lo scopo della domanda. Ebbene, mentre l'azione intentata davanti alla *High Court of Justice* mirava a precludere l'utilizzo del marchio sul territorio del Regno Unito, l'azione presentata al Giudice di Amburgo voleva vietarne l'utilizzo su tutto il territorio dell'Unione.

In secondo luogo, sulla base di tali considerazioni, in risposta all'altro quesito, la Corte è giunta alla conclusione che le due azioni possono dirsi aventi il medesimo oggetto solo limitatamente alle contraffazioni avvenute nel medesimo territorio e, di conseguenza, è esclusivamente con riguardo a queste ipotesi che il Tribunale adito successivamente sarà tenuto a dichiarare la propria incompetenza.

Capitolo XII

La commercializzazione dei dati personali: il caso Facebook

La disciplina relativa alla tutela della privacy – che riveste ormai un ruolo centrale nel nostro ordinamento – sembra tuttavia porsi in contrasto rispetto allo sviluppo delle nuove tecnologie e dell’economia c.d. “*data driven*”.

Ormai, lo sfruttamento dei dati è diventato il *core business* delle imprese e, conseguentemente, deve essere riconosciuto il valore economico dei dati personali. Tuttavia, bisogna tenere anche presente gli altissimi rischi per la tutela dei diritti fondamentali dell’individuo.

La riflessione sulla c.d. *commercializzazione dei dati personali* si basa su queste due considerazioni.

Vi sono due tesi fondamentali in contrapposizione tra loro, una favorevole e una contraria; entrambe richiamano argomentazioni di natura etica, economica e sociale.

Il nucleo del dibattito, tuttora aperto, è la possibilità di utilizzare i dati personali come corrispettivo delle prestazioni.

Sul tema, recentemente è intervenuto il D.lgs. di attuazione della Direttiva 770/2019, relativa ad alcuni aspetti dei contratti di fornitura di servizi digitali.

La disciplina vuole estendere le tutele previste per i contratti di consumo anche alle ipotesi in cui il consumatore non si impegni a pagare di una somma di denaro, ma si obblighi a cedere i propri dati personali. Eppure, il profilo economico non esaurisce il novero delle questioni legate alla tutela dei dati personali nel nuovo contesto digitale. Sono state sollevate diverse altre questioni.

Si pensi alla pubblicazione di immagini in assenza del consenso dell’interessato: si tratta chiaramente di illegittima diffusione dei dati personali. Questo specifico tema ha sollevato grandi preoccupazioni, soprattutto con riferimento alla pubblicazione sui *social* e alla diffusione di dati riferibili a soggetti minori.

La giurisprudenza che si è formata sul punto dimostra quanto la delicatezza dei temi che vengono in rilievo renda necessario l’attento bilanciamento degli interessi in gioco. Si pensi, poi, alla diffusione di immagini illegittima non soltanto perché l’interessato non vi ha acconsentito, ma anche per il contenuto delle immagini stesse, quando ad esempio si tratti di immagini a contenuto sessuale.

È il noto – e purtroppo diffuso, soprattutto tra i giovani – fenomeno del c.d. *revenge porn*, contro cui le autorità e i titolari delle principali piattaforme coinvolte stanno cercando di trovare delle soluzioni concrete (v. *infra*).

Le altre questioni interessanti riguardano gli elementi applicativi della disciplina sulla tutela della privacy, la corretta individuazione dei soggetti qualificabili come titolari o responsabili del trattamento in contesti innovativi, i problemi relativi alla c.d. eredità digitale e dunque all’applicazione della disciplina successoria in riferimento ai beni “digitali” del *de cuius*, e tante altre questioni che si pongono oggi al giurista.

Nella nuova economia digitale, i dati hanno un nuovo ruolo di mercato, come d’altronde è stato dimostrato dal cambiamento dei *business model* delle società.

Nell'economia guidata dai dati, infatti, questi sono diventati un vero e proprio *asset* strategico: grazie ai dati, le imprese possono fornire beni e servizi migliori, perché costruiti sulla base delle preferenze dei consumatori.

I dati personali, dunque, giocano un ruolo fondamentale, dato che senza di essi le imprese non sarebbero in grado di acquisire il grande numero di informazioni utili sulle tendenze del mercato.

Tuttavia, l'esigenza economica di sfruttare queste informazioni contrasta con il rispetto del diritto fondamentale alla protezione della privacy e dei dati personali, importante nel panorama europeo e italiano. Si arriva, addirittura, alla constatazione che l'applicazione della relativa disciplina è vista come un ostacolo allo sviluppo dell'economia.

Eppure, tale conclusione appare paradossale se si considera che è lo stesso GDPR a perseguire il rafforzamento del mercato interno quale fine ultimo, come alla fine vale per tutta la legislazione europea. È conseguenza evidente, allora, che nelle intenzioni del legislatore non si vuole porre alcun limite all'esercizio delle attività economiche, bensì solamente evitare inaccettabili violazioni dei diritti fondamentali.

Sulla base di quanto detto, dottrina e giurisprudenza si sono interrogate sul valore effettivo da dare ai dati personali: essendo diventati un vero e proprio mezzo di lucro, deve essere riconosciuto loro, anche dal punto di vista economico-giuridico, un valore diverso?

La questione principale è quella relativa a quei servizi che vengono offerti ai consumatori apparentemente in maniera gratuita, ma che in realtà presuppongono la cessione di dati personali.

L'esempio paradigmatico è quello dei *social network*: per accedere è necessario accettare uno specifico set di termini e condizioni e procedere alla comunicazione di una serie di dati personali quali nome, cognome, data di nascita, indirizzo e-mail, ecc. Non solo, ma durante la fruizione del servizio vengono generati dall'utente dati ulteriori, rilevatori delle proprie tendenze e preferenze; questi dati vengono spesso condivisi dalla società che gestisce i *social* con soggetti terzi, traendone profitto.

Per questo motivo, da tempo si è fatta strada la tesi, per il vero opinabile, sull'equiparabilità dei dati personali alla valuta: l'acquisto di determinati beni o servizi potrebbe avvenire (o, meglio, di fatto avverrebbe già), dietro la "corresponsione" di dati personali. Alcuni, di fronte a ciò, hanno parlato del cambio di dimensione dei dati dalla tradizionale dimensione "*morale*" a quella "*negoziale*".

Chi sostiene questa tesi, invero, pensa che gli individui godrebbero di una maggiore tutela, dal momento che troverebbero contestualmente applicazione tanto la disciplina sulla tutela dei dati personali che quella del consumo, così evitando che il singolo sia, da un lato, tratto in inganno dalla gratuità dell'offerta e perfezioni un acquisto inconsapevole dell'effettivo valore ceduto e, dall'altro, sia privo della possibilità di usufruire dei mezzi di tutela messi a disposizione dall'ordinamento.

Bisogna chiedersi: la strada della c.d. commercializzazione dei dati personali è davvero la via migliore? Sarebbe, da un lato, finalizzata a rendere l'interessato-consumatore

maggiormente consapevole del valore dei propri dati personali (restituendogli un effettivo controllo su di essi come, d'altronde, auspicato dal GDPR).

Dall'altro lato, lo scopo sarebbe quello di mettere a disposizione dell'utente tutte le tutele e gli strumenti già previsti dal Codice del Consumo.

Inoltre, per sostenere la percorribilità di questa strada, si fa generalmente un parallelismo con la disciplina della proprietà intellettuale, che riconosce contestualmente all'autore dell'opera diritti di natura morale (si pensi al riconoscimento della paternità) e diritti di sfruttamento economico (come il diritto di fare copie o riprodurre l'opera).

La tesi contrapposta – tradizionalmente affermata sia a livello europeo che nazionale – sostiene, invece, che, essendo il diritto alla protezione dei dati personali un diritto fondamentale, questo abbia valore assoluto, indisponibile, intrasmissibile e imprescrittibile, non potendo ammettersi in alcun modo la loro commercializzazione. Insomma, si sostiene il contrario di quanto sopra detto, ossia che la commercializzazione dei dati personali – lungi dal garantire una maggiore tutela agli interessati – finirebbe con lo sminuire l'effettivo valore dei dati personali, esponendo gli individui al rischio di subire pregiudizi ulteriori.

La Commissione, nella bozza della Direttiva sui contratti per la fornitura di servizi digitali, ha avanzato per la prima volta la proposta di ammettere l'utilizzo dei dati come corrispettivo. Sembrava opportuno, in particolare, riconoscere ai consumatori il diritto di scegliere tra le due alternative: acquistare un determinato bene mediante la cessione dei propri dati personali o facendo ricorso alla valuta ordinaria.

Sul punto, però, ha espresso subito parere negativo il Garante europeo per la protezione dei dati (EDPS)²⁰⁵, che ha voluto escludere categoricamente la possibilità di equiparare i dati personali al corrispettivo o al denaro, seppur aprendo alla possibilità di applicare le regole di tutela previste per i consumatori anche nel caso di acquisto di servizi generalmente considerati gratuiti.

In Italia, Guido Scorza, membro del Garante per la protezione dei dati, ha espresso le sue perplessità sul tema, evidenziando che in questo modo si creerebbe una discrepanza fra coloro che godono di una migliore condizione economica – e possono, quindi, scegliere effettivamente quale mezzo di acquisto utilizzare – e coloro che, invece, sarebbero maggiormente propensi a cedere i propri dati personali, trovandosi in una situazione peggiore e ignorandone le conseguenze.

La tesi contraria alla commercializzazione dei dati personali sostiene le sue ragioni anche per evitare l'eccessiva profilazione della popolazione, a cui è legato il rischio di possibili discriminazioni. L'obiettivo della tutela si estende, quindi, all'intera collettività.

205

Di recente, sia la giurisprudenza del Consiglio di Stato, che l'Autorità Garante della Concorrenza e del Mercato attraverso le sue pronunce, si sono posti in una posizione più aperta e favorevole all'introduzione di un approccio *negoziale* rispetto alla disciplina dei dati personali.

Si può, preliminarmente, fare l'esempio dell'AGCM che, dichiarando la vessatorietà di alcune clausole contrattuali poste da *Whatsapp*, ha affermato che non assumesse rilevanza alcuna il fatto che l'*App* di messaggistica istantanea venisse offerta agli utenti in maniera gratuita, ai fini della qualificazione del rapporto giuridico instauratosi fra gli stessi e la società come un rapporto consumeristico.

La posizione dell'Autorità poggia sulla considerazione che il valore economico dei dati personali degli utenti ceduti alla società per accedere al servizio di messaggistica dovesse ritenersi, da solo, sufficiente a far sorgere un rapporto consumatore/professionista²⁰⁶.

In realtà, però, l'esempio più lampante di questo nuovo approccio negoziale è da rinvenirsi nel caso che ha visto come parti contrapposte l'AGCM e Facebook, e che è arrivato fino al Consiglio di Stato, davanti al quale le parti avevano presentato ricorso. La vicenda ha inizio il 29 novembre 2018, quando l'AGCM, dopo aver contestato la violazione, da parte di *Facebook Inc.* e *Facebook Ireland Ltd*, della disciplina sulle pratiche commerciali scorrette, irrogava nei confronti delle società una sanzione per un importo complessivo di 10 milioni di euro²⁰⁷.

Sono due le attività scorrette contestate dall'Autorità.

La pratica a), che è stata ritenuta in contrasto con gli artt. 21 e 22 del D.lgs. 206/2005 (Codice del Consumo), consisteva nell'avere tratto in inganno gli utenti, enfatizzando la gratuità del servizio offerto, senza informarli adeguatamente e tempestivamente del fatto che i loro dati personali sarebbero stati utilizzati a fini commerciali. Secondo il parere dell'Autorità, in questo modo gli utenti sarebbero stati "obbligati" ad assumere una decisione commerciale che altrimenti non avrebbero preso.

La pratica b), contestata per violazione degli artt. 24 e 25 del Codice del Consumo – che disciplinano le pratiche commerciali aggressive – è stata ritenuta, come tecnica di acquisizione del consenso degli utenti, una forma di indebito condizionamento degli stessi: questi avevano, infatti, la sola possibilità di deselezionare la pre-impostazione effettuata da Facebook, tramite un meccanismo di *opt-out*. Così – secondo l'Autorità – gli utenti si sarebbero ritrovati, di fatto, costretti a subire, senza avere prestato adeguato consenso in merito, la cessione dei propri dati personali a soggetti terzi per finalità commerciali.

L'AGCM, evidenziando la natura di vero e proprio corrispettivo attribuibile, nel caso di specie, ai dati personali degli utenti, fa espresso riferimento al *business model* della società sanzionata, il che consentirebbe – secondo la stessa Autorità – di ritenere esistente un rapporto di consumo fra la nota società e gli utenti utilizzatori.

²⁰⁶ Il testo del provvedimento è accessibile su https://www.agcm.it/dotcmsDOC/allegati-news/IP278_ch.%20inott.%20%20sanz.pdf.

²⁰⁷ Il testo del provvedimento è accessibile su https://www.agcm.it/dotcmsdoc/allegati-news/PS11112_scorr_sanz.pdf.

Ebbene, da questo rapporto deriverebbe il dovere di dare attuazione agli obblighi di trasparenza e corretta informazione previsti dal Codice del Consumo.

La società si è poi rivolta al TAR²⁰⁸, il quale ha annullato la sanzione con riferimento alla pratica b), perché non ha ritenuto sussistenti elementi sufficienti a dimostrare la natura aggressiva della pratica commerciale; tuttavia, ha confermato il provvedimento dell'Autorità rispetto alla pratica a).

A quest'ultimo proposito, l'argomento portato da Facebook, secondo cui l'AGCM non sarebbe stata competente a pronunciarsi su una questione concernente la disciplina sulla protezione dei dati personali, è stato totalmente respinto dal TAR, che ha motivato tale rigetto esprimendo in modo chiaro la propria posizione in merito alla patrimonializzazione dei dati personali.

I Giudici hanno spiegato che la tesi della società ricorrente, secondo cui i dati personali, in quanto oggetto di un diritto fondamentale, non potessero acquisire la funzione di corrispettivo di una prestazione, non terrebbe adeguatamente conto del valore commerciale degli stessi nel mercato digitale e nel modello di *business* della società stessa.

Il TAR ha concluso, dunque, che debba trovare applicazione la disciplina del Codice del consumo, ed in particolare le norme che impongono i caratteri di chiarezza, competenza e non ingannevolezza delle informazioni fornite.

La vicenda è arrivata al Consiglio di Stato che, nella recente pronuncia n. 2631/2021²⁰⁹, ha colto l'occasione per ribadire l'erroneità della tesi sostenuta da Facebook in merito alla necessità di netta separazione fra la disciplina sulla tutela dei dati personali e quella contrattualistica.

I Giudici del Supremo Consesso amministrativo hanno evidenziato che, dal momento che tutte le azioni umane implicano il trattamento di dati personali, è ammissibile che all'applicazione della relativa disciplina si accompagni contestualmente quella di altre branche del diritto, tra cui rientra sicuramente quella del consumo. Si è parlato, a tal proposito, di “*tutele multilivello*” garantite alle persone fisiche.

Il Consiglio di Stato ha aderito alla posizione secondo la quale, nel caso di specie, le informazioni fornite agli utenti non fossero sufficientemente chiare e adeguate a permettere loro di assumere piena consapevolezza del fatto che i propri dati personali non vengono utilizzati esclusivamente per consentire la fruizione del servizio, ma vengono ulteriormente sfruttati a fini commerciali. Dunque, si conclude nel senso che la pratica è senz'altro da qualificarsi come ingannevole.

²⁰⁸ T.A.R. Roma (Lazio), sez. I, 10/01/2020, n. 260, disponibile su *dejure.it*, commentata da “Facebook, è scorretta la pratica che prevede la cessione a terzi dei dati degli iscritti senza un adeguato consenso”, su *Diritto & Giustizia*, 13 gennaio 2020.

²⁰⁹ Consiglio di Stato, sez. VI, 29/03/2021, n. 2631, disponibile su *dejure.it*; note a sentenza: I. M. ALAGNA, “Abuso dati personali di utenti: respinto in appello il ricorso di Facebook contro l'Antitrust”, *Diritto & Giustizia*, fasc. 74, 2021, pag. 9; V. RICCIUTO, C. SOLINAS, “Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla correttezza del contratto”, *GiustiziaCivile.com*, 18 maggio 2021.

Se è vero che nel *business model* di Facebook i dati vengono utilizzati per fini commerciali, è certamente discutibile la possibilità di attribuire loro la qualificazione giuridica di corrispettivo della controprestazione.

Si consideri che i dati forniti dagli utenti-consumatori sono generalmente raccolti sulla base giuridica di cui all'art. 6, para 1, lett. b) del GDPR, in quanto necessari all'esecuzione del contratto digitale.

Anche ammettendo che tutti i dati raccolti dalla società siano effettivamente indispensabili a tal fine, la loro dazione da parte degli utenti non potrebbe qualificarsi come corrispettivo della prestazione; piuttosto dovrebbe essere considerato come suo presupposto. Allo stesso modo, se i dati raccolti fossero utilizzati per finalità diverse o ulteriori, non potrebbero comunque essere considerati come un corrispettivo, in quanto ciò presuppone che il versamento avvenga consapevolmente.

Viene anche analizzata l'ipotesi del ricorso al consenso come base giuridica. Tuttavia, affinché il consenso sia libero, in assenza di esso non potrebbe comunque essere negata l'erogazione del servizio all'utente.

Ciò porta ad escludere l'ammissibilità della tesi dei dati come corrispettivo.

Si tenga presente che il Governo ha adottato il decreto legislativo 4 novembre 2021, n. 170, pubblicato il 25 novembre scorso, di attuazione della Direttiva 770/2019, che introduce nel Codice del Consumo un nuovo Capo I-bis nella parte IV, Titolo III, volto appunto a regolamentare i contratti aventi ad oggetto contenuti e servizi digitali²¹⁰.

Il testo individua l'ambito di applicazione della nuova disciplina, includendovi le ipotesi in cui *“il professionista fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali al professionista, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dal professionista ai fini della fornitura del contenuto digitale o del servizio digitale [...] o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico”*.

Viene qui richiamato quanto previsto dal Considerando 14 della Direttiva, il quale specifica che quest'ultima non può trovare applicazione nelle ipotesi in cui il professionista sia entrato nella disponibilità dei dati senza che il consumatore glieli abbia forniti “attivamente” (ad es. mediante l'utilizzo di *cookies*).

Le disposizioni di nuova introduzione intervengono, dunque, su un profilo specifico, e puntano ad estendere la tutela prevista dall'ordinamento in favore dei consumatori –

²¹⁰ Il comma 2 contiene le definizioni, stabilendo che, per il Capo I-bis, per “*contenuto digitale*” si intendono i dati prodotti e forniti in formato digitale; per “*servizio digitale*” si intende un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale; oppure un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore e da altri utenti di tale servizio o qualsiasi altra interazione con tali dati; per “*beni con elementi digitali*” si intende qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni del bene. L'intero testo è accessibile su <http://documenti.camera.it/leg18/dossier/pdf/TR0249.pdf>.

quali noti soggetti deboli nel rapporto contrattuale – anche a quei contratti nei quali, pur non essendoci la corresponsione di una somma di denaro, sorge in capo al consumatore un’obbligazione, consistente appunto nella cessione dei propri dati personali.

È essenziale comprendere, però, che ciò non è sufficiente ad affermare che i dati personali abbiano assunto il valore di controprestazione, con tutte le altre conseguenze in tema di sinallagma contrattuale.

Un altro passaggio interessante del decreto riguarda il rapporto fra la disciplina in esame e le disposizioni nazionali e dell’Unione Europea in materia di protezione dei dati personali. Il nuovo Capo I-bis del Codice del Consumo – viene specificato – trova applicazione con riferimento a qualsiasi dato personale trattato in relazione a contratti in cui il professionista fornisce un contenuto digitale o un servizio digitale al consumatore e che, in caso di conflitto, prevalgano le norme in materia di protezione dei dati.

Passando ad esaminare il diritto all’immagine, di rango di diritto fondamentale – ed in quanto tale inalienabile – si ammette la possibilità di cedere il diritto di riproduzione della stessa, previo consenso dell’interessato.

Alla regola del consenso fanno eccezione le ipotesi espressamente previste dalla L. n. 633 del 1941, tra cui vi è il caso dell’esercizio del diritto di cronaca – nel caso in cui la pubblicazione della foto risponda ad esigenze di pubblico interesse e sia comunque necessaria ai fini di completezza e chiarezza della notizia divulgata.

Sul tema, la Corte di Cassazione²¹¹ ha stabilito che è necessario che vi sia uno specifico ed autonomo interesse pubblico alla conoscenza delle fattezze della persona ritratta.

Con la sentenza n. 29583/2020²¹², inoltre, i giudici di legittimità hanno chiarito che la nozione di interesse pubblico deve essere intesa in senso ampio e che la sussistenza del diritto di cronaca, nonché della necessità di rappresentare l’immagine della persona protagonista della vicenda, deve essere comunque valutata alla luce del tipo di pubblicazione e della natura dell’attività giornalistica svolta.

Nel caso che ha dato origine alla pronuncia, infatti, la Corte ha accolto il ricorso contro la sentenza del Tribunale di Milano, che riconosceva l’illiceità della pubblicazione, su un settimanale, di alcune fotografie, nello specifico sette, ritraenti un personaggio pubblico in vacanza alle Maldive. I ricorrenti lesi lamentavano la violazione degli artt. 136 e 137 del Codice Privacy, dell’art. 6 del codice deontologico dei giornalisti, e dell’art. 21 della Costituzione.

²¹¹ Cass. Civ., sez. I, 09/07/2018, n. 18006, disponibile su *dejure.it*, “È censurabile la pratica delle interviste televisive con “riprese occulte”, ovvero tenendo la telecamera accesa all’insaputa del soggetto”, su *Guida al diritto*, 2018, 32, 35.

²¹² Cass. Civ., sez. I, 24/12/2020, n. 29583, disponibile su *dejure.it*, “Pubblicazione di foto a corredo di un articolo in assenza di consenso dell’interessato: condizioni di liceità”, su *Giustizia Civile Massimario*, 2021 e *Rivista di Diritto Industriale*, 2020, 6, III, 414.

La Suprema Corte ha riconosciuto la fondatezza delle argomentazioni addotte da chi faceva valere il suo diritto di cronaca, e ha ritenuto che le circostanze del caso concreto permettessero di applicare l'esimente del diritto di cronaca.

Non poteva, infatti – ad avviso dell'organo giudicante – ravvisarsi alcuna lesione dei diritti fondamentali, dal momento che la pubblicazione delle foto era giustificata da vari elementi quali: la notorietà del soggetto, la tipologia di cronaca, il fatto che i soggetti si trovassero in un luogo pubblico e, soprattutto, la considerazione che la narrazione non avesse travalicato i limiti della continenza, non recando danno alcuno alla reputazione del soggetto ripreso.

I Giudici hanno, dunque, concluso nel senso di ammettere la liceità della pubblicazione, anche se mancava del consenso delle parti.

Per quanto concerne il consenso²¹³, sono diversi gli aspetti da evidenziare, partendo dalle forme con cui può essere prestato, sino alle questioni concernenti la sua validità, alla luce anche di un'eventuale revoca dello stesso.

La succitata legge non richiede che il consenso venga fornito in una forma specifica: infatti, la giurisprudenza²¹⁴ ha ammesso la sua rilevanza anche nelle ipotesi in cui questo fosse soltanto implicito.

La forma scritta è necessaria, infatti, al solo fine di dirimere eventuali controversie concernenti la sussistenza del diritto alla divulgazione dell'immagine conteso fra soggetti diversi.

Ad ogni modo, il consenso alla pubblicazione può essere oggetto di specifico accordo contrattuale fra le parti, e la conseguenza è che una sua eventuale violazione fa insorgere il relativo regime di responsabilità.

La Corte di Cassazione ha affrontato il tema del consenso prestato mediante accordo contrattuale nella sentenza n. 10957/2010, attinente al diritto di sfruttamento commerciale di alcune pose di nudo di un'attrice esordiente da parte di un fotografo. Dal canto suo, l'attrice sosteneva che non vi fosse alcun rapporto contrattuale intercorrente fra le parti, e l'autorizzazione a disporre delle foto fosse stata concessa mediante atto unilaterale recettizio, da intendersi revocato alla luce di una serie di emergenze istruttorie. Della revoca, poi, erano state rese edotte, mediante lettere di

²¹³ Sul tema del consenso dell'avente diritto, v. F. BRAVO, *"Il consenso e le altre condizioni di liceità del trattamento dei dati personali"*, in G. FINOCCHIARO (diretto da), *"Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali"*, Torino, Zanichelli, 2017; S. TORDINI CAGLI, *"Principio di autodeterminazione e consenso dell'avente diritto"*, Bologna, 2008, 165. Più in generale, F. ALBEGGIANI, *"Profili problematici del consenso dell'avente diritto"*, Milano, 1995, 31. Per quanto concerne il dibattito dottrinale in Germania, cfr. C. ROXIN, *"Sul consenso nel diritto penale"*, in *"Antigiuridicità e cause di giustificazione. Problemi di teoria dell'illecito penale"*, a cura di S. MOCCIA, Napoli, 1996, 126; ID., *"Über die mutmassliche Einwilligung"*, in *"Festschrift für Hans Welzel"*, Berlino-New York 1974, 449 ss.; per un quadro di sintesi, G. FORNASARI, *"I principi del diritto penale tedesco"*, Padova, 1993, 289 ss.

²¹⁴ Cfr. Cass. Civ., sez. III, 06/05/2010, n. 10957, disponibile su *dejure.it*; con nota di A. NATALINI, *"Diritto all'immagine e pubblicazione di foto non autorizzata: per essere risarcita è la parte lesa che deve provare il pregiudizio economico"*, su *Diritto & Giustizia*, fasc. 0, 2010, pag. 193.

diffida, altre due società convenute in giudizio, responsabili dell'ulteriore diffusione delle immagini sulla base del diritto di disposizione delle stesse, acquisito dal predetto fotografo. La Corte di Cassazione, pronunciandosi sulla sussistenza e sulla validità o meno del consenso prestato dall'attrice, ha per prima cosa ribadito quanto detto sopra in merito alla rilevanza del consenso anche se prestato solo tacitamente.

Inoltre, si è chiarita la disciplina del consenso, che sarà volto esclusivamente a delineare le condizioni e i limiti entro i quali il suddetto diritto potrà legittimamente essere esercitato – specificando che anche nell'ipotesi in cui il diritto di disporre dell'immagine divenga oggetto di un rapporto contrattuale fra le parti, il consenso rimane comunque elemento esterno rispetto a tale rapporto.

Conseguenza di ciò è che il contratto ha il consenso quale suo presupposto e che, una volta stipulato, *“questo non possa di norma essere revocato fino a che l'utilizzazione entro i limiti stabiliti dal rapporto contrattuale sia possibile e/o non sia ancora stata realizzata”*.

Nel caso di specie, questo rileva in quanto la cessione del diritto di disposizione delle immagini a soggetti terzi era stata oggetto di contestazione. Per giustificare la legittimità di tale condotta, si sarebbe dovuta dimostrare non soltanto l'esistenza di un rapporto contrattuale, ma anche il fatto che questo disciplinasse il profilo della cessione a terzi del diritto.

È necessario porre l'accento su quel *“di norma”* utilizzato dalla Corte nella succitata pronuncia, dal momento che un orientamento più risalente²¹⁵ aveva stabilito che il consenso alla pubblicazione della propria immagine, in quanto negozio unilaterale, fosse *“revocabile in ogni tempo, anche in difformità di quanto pattuito contrattualmente salvo, in questo caso, il diritto dell'altra parte al risarcimento del danno”*.

Ultimamente, il tema della revoca del consenso è tornato a far discutere, perché una sentenza della Corte d'Appello di Milano²¹⁶ ha ribaltato quanto stabilito dai giudici di primo grado, affermando la revocabilità del consenso in qualunque momento.

Nel caso di specie, riguardante la pubblicazione delle foto di due attori, congiuntamente ad un'intervista sulla loro vita sentimentale, i Giudici hanno richiamato il principio già affermato dalla Cassazione secondo cui la sussistenza del consenso alla pubblicazione della propria immagine, è sempre necessario ed imprescindibile anche al momento della pubblicazione stessa. Quindi, a prescindere dagli accordi contrattuali originariamente raggiunti fra le parti, l'intervento della revoca prima dell'avvenuta pubblicazione fa venire senz'altro meno il presupposto della sua legittimità.

²¹⁵ Si veda Cass. Civ., sez. I, 19/11/2008, n. 27506, disponibile su *dejure.it*; *Giust. civ.* 2009, 2, 313; *Riv. dir. ind.* 2009, 4-5, II, 466; *Foro it.* 2009, 10, I, 2728 NOTA (s.m.) con nota di L. C. UBERTAZZI.

²¹⁶ Si veda la sentenza della Corte di Appello di Milano, n. 21043 del 2021.

Capitolo XIII

La tutela dei minori e il diritto all'oblio

Anche nei casi in cui l'immagine ritragga soggetti minori viene in rilievo la tutela della reputazione altrui, dovendosi comunque ritenere lecita, qualora sussista una delle ipotesi previste dalla legge e non sia recato pregiudizio alla persona, la pubblicazione in assenza di consenso.

Ciò è stato affermato dalla Corte di Cassazione nella pronuncia n. 8880/2020²¹⁷, che ha concluso che nel caso di specie *“le fotografie che ritraevano le minori (...), le quali partecipavano ad una manifestazione di massa in occasione dell'inaugurazione di uno scivolo gonfiabile, di certo non era lesiva della reputazione o dell'onore, posto che non è disdicevole o disonorevole, o contraria a qualsivoglia disposizione di ordine pubblico o buon costume, l'utilizzo di uno scivolo”*.

Parimenti, può essere affermato che l'elemento dell'interesse pubblico giustifica la pubblicazione dell'immagine di un minore solo se vi è la necessità *“di conoscere le fattezze dei protagonisti della vicenda narrata ai fini della completezza e correttezza della divulgazione della notizia (...)”*²¹⁸.

Tuttavia, la questione diventa più problematica quando, invece che avvenire su una testata giornalistica – trovando così pacificamente applicazione l'esimente del diritto di cronaca – la pubblicazione dell'immagine altrui abbia luogo sui *social network*.

La Corte EDU ha ritenuto che *“la pubblicazione di un'immagine manipolata sul social network Instagram”* integri la violazione dell'art. 8 della Carta Europea sui diritti dell'Uomo, posto a tutela del diritto al rispetto della vita privata, incluso quello alla reputazione. A Strasburgo si è infatti spiegato che la tutela alla reputazione deve essere garantita anche a coloro che subiscono diffamazione sui *social*, dovendosi garantire un equo bilanciamento fra il diritto alla libertà di espressione e la tutela della reputazione privata²¹⁹.

Ovviamente, nei casi in cui ad essere ritratto è un minore, la situazione diviene più delicata; le sempre più numerose pronunce giurisprudenziali al riguardo sono accomunate dalla prevalenza della tutela del minore sulla libertà di espressione altrui. La questione è stata affrontata dal Tribunale di Rieti nel marzo del 2019²²⁰.

²¹⁷ Cass. Civ., sez. III, 13/05/2020, n. 8880, disponibile su *dejure.it*, *Guida al diritto* 2020, 37, 64; *Giustizia Civile Massimario*, 2020; *Rivista di Diritto Industriale*, 2020, 4-05, II, 344.

²¹⁸ Cass. Civ., sez. I, 19/02/2021, n. 4477, disponibile su *dejure.it*, commentata da I. M. ALAGNA, *“L'interesse pubblico alla diffusione di una notizia non legittima la pubblicazione di immagini ritraenti un minore su testate giornalistiche”*, su *Diritto & Giustizia*, fasc. 38, 2021, pag. 6.

²¹⁹ Corte Europea Diritti dell'Uomo, sez. II, 07/11/2017, n. 24703, disponibile su *dejure.it* e *Guida al diritto*, 2018, I, 42.

²²⁰ Tribunale di Rieti, sentenza del 07/03/2019, pronunciata nel procedimento avente r.g. n. 2008/2018, disponibile su *dejure.it*; nota a sentenza di A. SIMEONE, *“La nuova compagna del padre non può pubblicare le foto dei minori senza il consenso della madre”*, su *Ilfamiliarista.it*, luglio 2019.

I Giudici si sono trovati a risolvere una controversia riguardante la liceità della pubblicazione di foto ritraenti soggetti di minore età, nel caso di specie figli di genitori divorziati, da parte della nuova compagna del padre.

Con ricorso ex art. 700 c.p.c., il tribunale è stato adito dalla madre dei minorenni, affinché ordinasse alla nuova compagna del padre l'immediata rimozione dai *social media* delle immagini che ritraevano i propri figli, nonché inibisse la generale diffusione delle medesime foto.

Il ricorso era giunto al Tribunale dopo una preliminare diffida, a seguito della quale il comportamento della convenuta era cessato solo temporaneamente, salvo poi riprendere, tanto che i genitori sono stati costretti a convenire in sede di divorzio che la pubblicazione delle immagini dei propri figli sarebbe stata consentita, sia ai genitori che ai terzi, soltanto previo consenso espresso di entrambi.

L'intervento del tribunale è scaturito dall'inosservanza di tale accordo.

Il collegio giudicante, nella propria argomentazione, ha ripreso il principio che subordina l'utilizzo di un'immagine ritraente un soggetto minorenne al previo consenso degli esercenti la responsabilità genitoriale – richiamando sia le norme nazionali che quelle sovranazionali rilevanti in materia (tra cui rientrano l'art. 10 c.c., gli artt. 4, 7, 8 e 145 del Codice della Privacy e la Convenzione di New York del 20 novembre 1989) – e ha così condannato la convenuta alla rimozione dei contenuti esistenti sui *social*, vietandole altresì di pubblicare ulteriormente simili immagini.

Elemento interessante della pronuncia è stata l'applicazione dell'art. 614-bis c.p.c.: i Giudici hanno fissato in 50,00 euro la somma dovuta per ogni giorno di ritardo nell'esecuzione dell'ordine di rimozione e per ogni successiva violazione dell'inibitoria.

Anche altre pronunce più risalenti si sono espresse sul tema della diffusione di immagini di minori in assenza del consenso dell'esercente la responsabilità genitoriale, in particolare in casi di pubblicazione di immagini, da parte di uno dei due genitori, in assenza del consenso dell'altro.

Ad esempio, nel 2017 il Tribunale di Mantova²²¹, all'interno di un giudizio di separazione, aveva inibito alla madre la diffusione delle immagini dei figli in assenza del consenso del padre. Proprio nello stesso anno, il Tribunale di Roma²²² si è spinto oltre, ordinando contestualmente la rimozione dei contenuti già pubblicati e applicando l'art. 614-bis c.p.c.

Tema interessante è anche quello del diritto all'oblio, riconosciuto agli interessati dall'art. 17 del GDPR, che ha rappresentato, sin dall'entrata in vigore del Regolamento, uno degli aspetti maggiormente problematici nella emergente realtà digitale.

²²¹ Tribunale di Mantova, 19/09/2017, disponibile su *dejure.it*, con nota a sentenza di S. MOLFINO, “Vietato pubblicare le foto dei figli sui social network senza il consenso dell'altro genitore”, su *Ifamiliarista.it*, gennaio 2018.

²²² Tribunale di Roma, sez. I, 23/12/2017, disponibile su *dejure.it*, con nota a sentenza di G. O. CESARO, “Genitore pubblica sui social network foto e notizie del figlio minore: interviene d'ufficio il Giudice”, su *Ifamiliarista.it*, marzo 2018.

Ciò è causato, da un lato, dalla difficoltà di garantirne l'effettività, e dall'altro, dalla necessità di bilanciare correttamente tale diritto con gli altri interessi in gioco.

Il diritto all'oblio può essere esercitato solo nei casi previsti dall'art. 17 e purché sussistano circostanze idonee a dimostrare che l'interessato si trovi in una situazione particolare. Tale diritto è venuto in rilievo nel caso *Google Spain*²²³.

La Corte di Giustizia ha selezionato diversi elementi da tenere in mente quando si procede ad una tale valutazione, elementi che sono stati ampiamente condivisi anche dalla giurisprudenza interna, come emerge dall'analisi delle sentenze più rilevanti degli ultimi anni (es. l'interessato è un personaggio pubblico, i fatti riportati sono inaccurati ecc). Si badi che fra i suddetti elementi figura anche il caso in cui l'informazione riportata sia qualificabile come *hate speech*.

Anzitutto, secondo la Suprema Corte, il diritto all'oblio consiste “*nel non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza*”²²⁴.

La pronuncia rientra nell'ambito di quella che viene considerata, da parte della dottrina, la seconda accezione del diritto all'oblio, concernente la tutela dell'identità personale. In quest'ottica, il bene giuridico tutelato è più ampio rispetto al singolo dato personale, mirando a tutelare nel complesso la dignità della persona.

Ne discende la necessità di contestualizzare le informazioni, valutando l'impatto di queste sull'individuo in relazione alla situazione nella quale egli si trova in un dato momento.

Nella medesima pronuncia, i Giudici affrontano il tema del complesso bilanciamento fra il diritto all'oblio e il diritto di cronaca (e informazione), che rappresenta, forse, l'aspetto più delicato e problematico dell'attuazione di questa disposizione.

A norma dell'art. 17, comma 3, lett. a), l'esercizio della libertà di espressione e di informazione costituisce una delle eccezioni che consentono di escludere l'esercizio del diritto all'oblio, configurando come necessaria un'analisi svolta caso per caso e finalizzata a valutare la prevalenza dell'uno o dell'altro diritto nelle circostanze concrete.

Nel compiere tale valutazione, si deve anzitutto tenere in considerazione il lasso di tempo trascorso fra i fatti verificatisi e la persistenza della pubblicità della notizia.

I Giudici evidenziano, infatti, che il pregiudizio alla reputazione e alla riservatezza dell'interessato possa discendere dalla ripubblicazione “*a distanza di un importante lasso temporale di una notizia relativa ai fatti del passato*”.

In un passo importante, la Corte afferma che il diritto all'oblio può dirsi garantito anche soltanto mediante la deindicizzazione di un articolo dai motori di ricerca, proprio perché il diritto dell'interessato va comunque posto in relazione a quello di cronaca e di conservazione della notizia per finalità storico-sociali.

²²³ Vedi G. RESTA, V. ZENO-ZENCOVICH (a cura di), “*Il diritto all'oblio su internet dopo la sentenza Google Spain*”, Roma Tre Press, Roma, 2015.

²²⁴ Cass. Civ., sez. I, 19/05/2020, n. 9147, disponibile su *dejure.it*; nota a sentenza di M. COCUCCIO, “*Deindicizzare per non censurare: il «ragionevole compromesso» tra diritto all'oblio e diritto di cronaca*”, su *Responsabilità Civile e Previdenza*, fasc. 1, 2021, pag. 175.

Il medesimo concetto è stato ribadito nella sentenza n. 7559 del 2020²²⁵, nella quale è riportato che la deindicizzazione di un articolo risalente nel tempo – nonostante la permanenza di quest’ultimo nell’archivio *online* del giornale – è idonea a garantire un corretto *trade-off* fra il diritto all’oblio dell’interessato e l’interesse della collettività alla permanenza della notizia.

Sul punto bisogna fare almeno due diverse considerazioni.

La prima riflessione riguarda la valutazione di un “*lasso di tempo idoneo*” a far venir meno l’interesse pubblico alla conoscenza della notizia. Tale criterio, infatti, sebbene possa sembrare chiaro nella teoria, non lo è nella pratica; sono moltissimi, infatti, i fattori che il giudice sarà chiamato a valutare nel corretto bilanciamento degli interessi. Ad esempio, la Suprema Corte, nella sentenza n. 13161/2016²²⁶, ha affermato che il periodo idoneo a far venir meno l’interesse per la divulgazione di un fatto di cronaca nera fosse individuabile in due anni mezzo. Tuttavia, ci si chiede come tale criterio possa dirsi indistintamente valido per qualunque circostanza, essendo comunque sempre necessario svolgere un’analisi concreta caso per caso.

La seconda considerazione da fare concerne il fatto che limitare la portata del diritto all’oblio alla sola cancellazione dei dati, significherebbe snaturare ingiustamente la disposizione. Questa, infatti, anche alla luce dell’interpretazione che ne è stata data dalla giurisprudenza, ammette, fra le misure che ne permettono la piena attuazione, la deindicizzazione, l’anonimizzazione dei dati e la loro esatta contestualizzazione.

Si tratta di elementi il cui riconoscimento assume particolare rilevanza proprio in virtù dell’avvento di Internet, dato che assicurare la cancellazione dei dati sul web risulta particolarmente complesso in molti casi, ma è ben possibile garantire la piena tutela dell’interessato all’oblio facendo ricorso a mezzi diversi.

Questo concetto si ricollega anche al tema dell’ampliamento della portata del diritto all’oblio e alla configurabilità di un vero e proprio diritto all’identità, alla quale oggi parte della dottrina si riferisce con l’espressione “*identità dinamica dell’individuo*”.

Si è compreso, in altri termini, che per garantire la tutela dell’interessato non basta prevedere la cancellazione dei dati, bensì è necessario provvedere all’attuazione di misure ulteriori, prime fra tutte il loro continuo aggiornamento e la loro contestualizzazione.

Sul tema, si rimanda alla giurisprudenza della Corte di Cassazione²²⁷, che ha anzitutto riconosciuto all’interessato il diritto di rivolgersi direttamente al sito che manteneva la notizia disponibile *online* e non al motore di ricerca, affermando al contempo che al

²²⁵ Cass. Civ., sez. I, 27/03/2020, n. 7559, disponibile su *dejure.it*; nota a sentenza di V. AMENDOLAGINE, “Il diritto all’oblio tra rievocazione storiografica online e cronaca giudiziaria”, su *GiustiziaCivile.com*, 18 agosto 2020.

²²⁶ Cass. Civ., sez. I, 24/06/2016, n. 13161, disponibile su *dejure.it*; nota a sentenza di D. BIANCHI, “Danno e oblio. Nesso di causalità, principio di proporzionalità e misure di sicurezza Data Protection”, su *Ridare.it*, 19 ottobre 2016.

²²⁷ Cass. Civ., sez. III, 05/04/2012, n. 5525, disponibile su *dejure.it*; nota a sentenza di G. CITARELLA, “Aggiornamento degli archivi online, tra diritto all’oblio e rettifica «atipica»”, su *Responsabilità Civile e Previdenza*, fasc. 4, 2012, pag. 1155.

fine di garantire un corretto bilanciamento fra il diritto d'informazione e il diritto all'oblio, si sarebbe dovuto garantire l'aggiornamento delle notizie riportate.

Tra gli elementi rilevanti nel bilanciamento fra il diritto all'oblio e quello all'informazione, è da tenere in considerazione la notorietà del soggetto interessato.

A tal proposito, deve richiamarsi la pronuncia²²⁸ con cui la Corte di legittimità, ribaltando la decisione della Corte d'Appello, ha riconosciuto il diritto di un imprenditore ad ottenere la deindicizzazione da un motore di ricerca di un articolo nel quale venivano riportate intercettazioni telefoniche di terzi che riferivano di una presunta vicinanza dello stesso a gruppi mafiosi.

Nel caso di specie, i giudici hanno ritenuto prevalente il diritto all'oblio dell'interessato, dato che quest'ultimo non era un personaggio pubblico e godeva di notorietà solo a livello locale. A parere della Corte, negare la deindicizzazione avrebbe infatti comportato una lesione del diritto dell'interessato *“a non vedersi attribuita reiteratamente una biografia telematica, diversa da quella reale e oggetto di notizie ormai superate”*.

La Corte di Giustizia si è, altresì, focalizzata sull'elemento della natura della notizia, affermando che il diritto alla cronaca e all'informazione prevalgono, nonostante il trascorrere di un lungo lasso di tempo, nel caso di notizie relative a procedimenti penali. Il caso di specie esaminato dai giudici di Lussemburgo concerneva la condanna all'ergastolo per omicidio di due cittadini tedeschi: la Corte ha ritenuto che *“gli archivi online di giornali e radio sono un bene da proteggere perché garantiscono il diritto della collettività a ricevere notizie di interesse generale, che non è attenuato dal passare del tempo”*²²⁹.

La giurisprudenza della Cassazione si è pronunciata anche sul contenuto della domanda di deindicizzazione rivolta ai motori di ricerca, sottolineando che, in questo caso, si richiede la precisa individuazione dei risultati della ricerca che l'attore intende rimuovere (generalmente serve l'indicazione di indirizzi telematici o URL).

Non è escluso, comunque, che *“una puntuale rappresentazione delle singole informazioni associate alle parole chiave”* possa bastare a permettere al motore di ricerca di adempiere all'obbligo cui è soggetto²³⁰.

Sul tema della deindicizzazione da parte dei motori di ricerca su richiesta degli interessati, la Corte europea, nella causa C-136/2019, pur ribadendo la sussistenza di tale obbligo, ha evidenziato che questo ha valenza solo per quanto riguarda le versioni

²²⁸ Cass. Civ., sez. I, 31/05/2021, n. 15160, disponibile su *dejure.it*; v. anche *“Diritti alla riservatezza e all'identità personale e bilanciamento con il diritto della collettività all'informazione”*, su *Giustizia Civile Massimario*, 2021.

²²⁹ Corte Europea Diritti dell'Uomo, sez. V, 28/06/2018, n. 60798, disponibile su *dejure.it*; v. anche *“Il diritto all'informazione prevale su quello all'oblio se si tratti di notizie relative a procedimenti penali”*, su *Guida al diritto*, 2018, 30, 24.

²³⁰ Cass. Civ., sez. I, 21/07/2021, n. 20861, disponibile su *dejure.it*; nota a sentenza di R. SETTIMIO, *“Deindicizzazione e diritto all'oblio al vaglio della Suprema Corte”*, su *GiustiziaCivile.com*, 27 settembre 2021.

presenti negli Stati Membri e non tutte quelle sotto il dominio dei gestori. Ciò significa che il motore di ricerca sarà tenuto a deindicizzare solo i dati presenti nei *server* europei. Questo profilo ha assunto una rilevanza sempre maggiore, tanto che lo scorso 7 luglio l'EDPB ha adottato le linee-guida 5/2019²³¹ relative proprio all'esercizio del diritto all'oblio nei casi relativi ai motori di ricerca. In relazione all'art. 17 comma 1, lett. b), che riconosce il diritto dell'interessato di richiedere la cancellazione dei dati nell'ipotesi in cui abbia ritirato il proprio consenso al trattamento, il documento evidenzia il fatto che, normalmente, il consenso è dato al *web publisher* e non al motore di ricerca e, perciò, è al primo che sarà comunicata dall'interessato la volontà di ritirare il consenso. Secondo l'EDPB, in tal caso, è onere del *web publisher* informare tempestivamente il motore di ricerca e ottenere la cancellazione dei dati, ai sensi del comma 2 dell'art. 17 GDPR. L'interessato potrà, tuttavia, esercitare direttamente il proprio diritto, ai sensi dell'art. 17, comma 1, lett. c). La norma consente all'interessato, infatti, di esercitare il diritto all'oblio altresì nell'ipotesi in cui abbia previamente esercitato il diritto di obiezione ex art. 21, comma 1 del GDPR. L'articolo pone a carico del motore di ricerca l'onere di provare la sussistenza di motivi legittimi prevalenti rispetto al diritto di obiezione. Il legame fra le due disposizioni richiamate – come messo in luce dall'EDPB – comporta che nel caso del diritto all'oblio, se il motore di ricerca non è in grado di fornire la prova richiesta, sarà obbligato ad esaudire la richiesta dell'interessato. Per quanto concerne la legittimazione ad agire per il riconoscimento del diritto all'oblio, nell'ipotesi di notizie riguardanti una persona deceduta, i Giudici di legittimità hanno affermato che tale diritto non può essere fatto valere dal congiunto *iure proprio*, ma soltanto nella sua veste di erede²³².

Come si configura il risarcimento del danno derivante dalla lesione del diritto all'oblio? La giurisprudenza è pacifica nel riconoscere la risarcibilità di tutti i danni, patrimoniali e non, riconducibili alla violazione di tale diritto, avendo il diritto all'oblio rango di diritto fondamentale della persona, per cui è azionabile il risarcimento per danno da fatto illecito ex art. 2043 c.c. Per vedersi riconosciuto il danno non patrimoniale, chi agisce in giudizio deve, tuttavia, allegare e provare tale danno²³³. Sotto il profilo della quantificazione, il danno è calcolato perlopiù in via equitativa ex art. 1226 c.c.²³⁴.

²³¹ Accessibili da https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_it.

²³² Si veda Cass. Civ., sez. I, 27/03/2020, n. 7559, cit.

²³³ Cass. Civ., sez. III, 19/07/2018, n. 19137, disponibile su *dejure.it*; nota a sentenza di I. PIETROLETTI, “Nessun risarcimento per l'avvocato se non prova i pregiudizi concreti ricollegabili all'attività”, su *Diritto & Giustizia*, fasc. 128, 2018, pag. 10 e Cass. Civ., sez. I, 23/05/2018, n. 12855, disponibile su *dejure.it*; nota a sentenza di F. VALERINI, “La familiarità della minore con i social network non salva Yahoo.it dal risarcimento del danno per la pubblicazione della foto”, su *Diritto & Giustizia*, fasc. 92, 2018, pag. 21.

²³⁴ È utile richiamare la giurisprudenza della Cassazione relativa al risarcimento del danno da reputazione, la cui *ratio* trova applicazione anche nel contesto che qui interessa. A proposito, la Corte ha ribadito che il giudice è “*tenuto a dare conto delle circostanze considerate nel compimento della valutazione equitativa e del percorso logico che lo ha condotto a quel determinato risultato*” (Cass. Civ., n. 11039/2006, disponibile su *dejure.it* e *Giust. civ. Mass.* 2006, 5).

Capitolo XIV

L'“eredità digitale”

Infine, molto interessante è anche il tema dell'accesso e del trasferimento dei dati di una persona deceduta (c.d. “*eredità digitale*”), questione emersa con l'avvento e la diffusione della società digitale. L'esigenza principale che pone la questione è quella di stabilire quali sono i soggetti che abbiano – e a quali condizioni – il diritto di accedere ai dati personali *online* di una persona deceduta.

Il fenomeno della c.d. “*digitalizzazione*” dell'economia ha comportato che i beni immateriali e gli *asset* intangibili sono entrati a far parte della massa ereditaria, creando il problema relativo all'individuazione delle regole di ripartizione della stessa. Inoltre, soprattutto a causa dell'avvento dei *social media*, un'enorme quantità di dati personali resta disponibile *online* sul web anche durante la fase *post mortem*, facendo sorgere anche la problematica concernente il controllo di tali dati. Il fulcro della questione è che i dati vengono affidati all'intermediario professionista (ossia la piattaforma), in virtù di accordi contrattuali che, tuttavia, in molti casi prevedono espressamente la loro *intrasmissibilità mortis causa*, in contrasto con la disciplina in materia di successioni. Inoltre, un altro problema è quello legato all'eterogeneità dei beni qualificabili come facenti parte dell'eredità digitale. Infatti, oltre ai dati presenti sui *social media*, vi rientrerebbero, ad esempio, i documenti digitali *offline* e quelli conservati grazie a servizi di *cloud computing*, i profili *online*, sia professionali che personali, i dati relativi a giochi virtuali, gli *accounts*, le criptovalute, i nomi di dominio. Per fare chiarezza sulla questione, si possono suddividere tutti questi elementi in almeno due categorie. Da un lato, vi sono i beni a connotazione prettamente patrimoniale (es. le criptovalute) e dall'altro, quelli di carattere personale (es. profili *social*).

Da questa distinzione deriverebbe l'applicabilità di regole diverse per l'una e l'altra categoria, individuate sulla base delle caratteristiche dei beni.

È una distinzione apparentemente semplice in teoria, ma più complicata da effettuare nella pratica, dal momento che in molti casi vi è una sovrapposizione dei caratteri.

Si aggiungono gli ormai noti problemi legati al carattere transnazionale delle questioni. Con il D.lgs. n. 101 del 2018, che ha novellato il Codice della Privacy, il legislatore italiano è intervenuto sul tema introducendo l'art. 2-terdecies²³⁵.

²³⁵ Art. 2-terdecies Codice Privacy (“Diritti riguardanti le persone decedute”)

“1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

È una norma molto rilevante, anche perché il Considerando 27 del GDPR afferma chiaramente che il Regolamento non si applica ai dati delle persone decedute, lasciando agli Stati membri la possibilità di introdurre regole proprio su questo profilo.

La norma non chiarisce se i soggetti legittimati all'esercizio dei diritti del *de cuius* agiscano in virtù di un acquisto *mortis causa*, oppure se godano di una legittimazione *iure proprio*.

Gli aspetti più rilevanti sono che, anzitutto, la norma include fra i diritti esercitabili *post mortem* dell'interessato anche il diritto alla portabilità dei dati.

Poiché la *ratio* della norma risponde sia all'esigenza di garantire il pieno controllo sui dati personali che a quella di tutelare il mercato concorrenziale, si deve dedurre che la legittimazione all'esercizio di tale diritto deve essere riconosciuta solo ai soggetti che agiscono a tutela dell'interessato e non anche a chi vanta un proprio interesse.

Il mandatario è incluso tra i soggetti legittimati all'esercizio dei diritti *post mortem*. Questo, per l'esigenza di prendere atto della prassi sempre più diffusa di affidare la gestione dei propri *account* e profili *social*, soprattutto professionali, a soggetti terzi.

Il compimento da parte di tale soggetto di atti giuridici in nome dell'interessato – e per espressa volontà di quest'ultimo dopo la sua morte – è compatibile con il nostro diritto successorio solo nella misura in cui attenga a quei beni che sono stati definiti di carattere “personale”. In caso contrario, infatti, s'incorrerebbe nella violazione del divieto di patti successori.

I commi successivi dell'articolo prevedono che l'esercizio dei diritti possa essere precluso per espressa volontà dell'interessato, consegnata o comunicata al titolare del trattamento, ma solo per quanto concerne l'ambito dei servizi della società dell'informazione.

Tale volontà deve avere queste caratteristiche: risultare in modo non equivoco, essere specifica, libera e informata.

La previsione deriva dalla consapevolezza dell'asimmetria informativa e dello squilibrio che caratterizza i rapporti contrattuali fra i soggetti privati e le grandi piattaforme e vuole tutelare l'integrità delle scelte compiute dai primi.

Ad ogni modo, i terzi non possono subire alcun pregiudizio rispetto ai diritti patrimoniali derivanti loro dalla morte dell'interessato, nonché rispetto al diritto di difendere in giudizio i propri interessi.

Di questa disposizione, ha fatto di recente applicazione il Tribunale di Milano²³⁶, con una sentenza in cui si è affermato che l'accesso e il trasferimento dei dati delle informazioni memorizzate sull'*account* di una persona deceduta o sincronizzate *online*

4. *L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.*

5. *In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.*”

²³⁶ Tribunale di Milano, sez. I, 09/02/2021, disponibile su *dejure.it*; v. nota a sentenza di S. CIARDO, “Privacy e tutela dei dati personali memorizzati nell'*account* della persona deceduta”, su *Ridare.it*, 20 aprile 2021.

su *iCloud* è consentito, ai sensi dell'art. 2-terdecies del Codice, ai terzi legittimati, soltanto nell'ipotesi in cui sussistano ragioni familiari meritevoli di protezione e se non espressamente vietato dall'interessato.

Alla società di informazione, titolare del trattamento, è vietato frapporre ostacoli all'esercizio di tale diritto, se non in adempimento della disciplina nazionale ed europea.

Con la pronuncia cautelare in esame, il giudice ha ordinato d'urgenza ad una società del gruppo *Apple* di consentire ai genitori di un ragazzo venuto a mancare in un incidente stradale di accedere ai dati dell'*account i-cloud* del figlio.

L'intervento della società si è rivelato necessario, poiché il telefono del ragazzo defunto era andato distrutto. Ebbene, alla prima richiesta di accesso rivolta dai genitori alla società, questa aveva risposto che avrebbe provveduto in tal senso soltanto su ordine del Tribunale, avente specifici contenuti.

Gli interessati, dunque, si erano rivolti al Tribunale di Milano, affinché emettesse – con decreto *inaudita altera parte* o con ordinanza – i provvedimenti necessari in via cautelare, ex artt. 669-bis e 700 c.p.c. Quanto alla sussistenza del *fumus boni iuris*, i ricorrenti sostenevano la ravvisabilità dei requisiti previsti dall'art. 2-terdecies del Codice Privacy. Relativamente al *periculum in mora*, si faceva presente che l'*Apple* aveva comunicato loro che i dati dell'*account* sarebbero stati automaticamente distrutti una volta decorso un determinato periodo di inattività dello stesso. Il Tribunale, nel caso di specie, ha ritenuto che la richiesta dei genitori, giustificata dal tentativo di cercare di colmare il senso di vuoto e il dolore causati dalla perdita del figlio, integrasse perfettamente le “ragioni familiari meritevoli di protezione” richieste dall'art. 2-terdecies e che fosse altresì sussistente il requisito del *periculum in mora*, concludendo dunque con l'ordine rivolto ad *Apple* di consentire ai ricorrenti l'accesso all'*account*.

Altro elemento interessante dell'ordinanza è la considerazione fatta dai giudici sui requisiti che – ai sensi delle condizioni contrattuali previste da *Apple* – l'ordine del Tribunale dovrebbe possedere per vincolare la società.

Secondo la Società, l'ordine deve specificare:

- a) che il defunto fosse proprietario di tutti gli account associati all'ID *Apple*;
- b) che il richiedente fosse l'amministratore o il rappresentante legale del patrimonio del defunto;
- c) che questo agisse come “agente” del defunto e la sua autorizzazione costituisca un “consenso legittimo”;
- d) che l'ordine imponesse ad *Apple* di fornire assistenza nel recupero dei dati personali degli account, che avrebbero potuto contenere anche informazioni o dati personali di terzi.

Il Tribunale di Milano ha, tuttavia, evidenziato alcune criticità della richiesta, dovute soprattutto al fatto che questa si basasse sul diritto statunitense, piuttosto che su quello italiano. Ad esempio, è noto che nel nostro ordinamento non esiste la figura dell'amministratore, del rappresentante legale o dell'agente del *de cuius*. Parimenti, la disciplina interna non prevede alcuna autorizzazione o consenso legittimo all'attività di tali soggetti.

Alla luce di ciò, il Tribunale ha dichiarato illegittima la pretesa di *Apple* di subordinare l'esercizio di un diritto riconosciuto dall'ordinamento giuridico italiano a condizioni estranee a quest'ultimo. Infine, il Tribunale ha respinto la tesi di *Apple* che legittimava il proprio rifiuto ad accogliere la richiesta invocando la “*sicurezza dei clienti*”, affermando che ai sensi dell'art. 6, para 1, lett. f) del GDPR il trattamento dei dati è possibile se necessario per il perseguimento del legittimo interesse del titolare o di terzi. Secondo i giudici di Milano, essendo la richiesta avanzata dai genitori basata su “*ragioni familiari meritevoli di protezione*”, sussisterebbe in questo caso il legittimo interesse.

Capitolo XV

Il fenomeno del c.d. *Revenge porn*

Il fenomeno del c.d. *revenge porn*, concernente la diffusione di immagini a contenuto sessuale, senza il consenso della persona interessata è, purtroppo, sempre più frequente nell'era dei *social media* e della divulgazione *online* di foto e video²³⁷, ponendosi in stretta correlazione con la tutela dei dati personali, poiché che le immagini diffuse rientrano pienamente nella nozione di dato personale fornita dalla legge.

Il Garante per la Privacy, per contrastare la diffusione di questo fenomeno, ha cercato di fornire uno strumento specifico per tutelare le vittime di *revenge porn*, e così ha formulato un accordo con Facebook, introducendo un meccanismo di segnalazione, agevolmente accessibile attraverso il sito del Garante, attraverso il quale chiunque abbia modo di temere che le proprie immagini possano essere illegittimamente diffuse attraverso i canali *social* forniti dal *social network*, può richiedere che la piattaforma intervenga in maniera preventiva, proteggendo le immagini mediante un codice *hash* ed impedendone così la divulgazione.

Sul tema del *revenge porn*, è intervenuta la Corte di Cassazione, con la pronuncia n. 3050/2020²³⁸, in particolare sull'argomento relativo all'applicabilità della disciplina dettata dal Codice della Privacy alle condotte ascrivibili a tale fenomeno in espansione. Nello specifico, è venuta in rilievo la continuità normativa fra il vecchio e il nuovo articolo 167, comma 2 del Codice, da cui discende la rilevanza penale o meno della condotta.

La pronuncia trae origine da una vicenda che ha visto la diffusione – da parte dello stesso indirizzo riconducibile alla vittima – di diciotto e-mail, con allegati video raffiguranti atti e rapporti sessuali fra il soggetto che aveva divulgato i messaggi e la vittima di *revenge porn*, nonché foto intime ritraenti la figlia minorenni di quest'ultima.

Il ricorrente lamentava la falsa applicazione dell'art. 167 del Codice della Privacy, ritenendo escluse, sulla base della nuova formulazione dell'articolo, le condotte di *comunicazione e diffusione dei dati*.

²³⁷ Sul tema v. G. M. CALETTI, “*Revenge porn e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane*”, in *DirPenCont* 2018, 65 ss.; D. CITRON – K. FRANKS, “*Criminalizing Revenge Porn*”, in *Wake Forest Law Review*, 2014, 347; M. KAMAL – W. NEWMAN, “*Revenge Pornography: Mental Health Implications and Related Legislation*”, in *The Journal of American Academy of Psychiatry and the Law*, 2016, 362 ss.; B. SANDYWELL, “*On the globalisation of crime: The internet and the new criminality*”, in “*Handbook of Internet Crime*”, a cura di Y. JEWKES – M. YAR, Milton, 2010, 46, che inserisce il “*revenge porn*” all'interno delle «*traditional criminal activities that are generalised and radicalised by the internet*».

²³⁸ Cass. Pen., sez. V, 17/12/2020, n. 3050, disponibile su *dejure.it*; nota a sentenza di F. BRIZZI, “*Diffusione illecita di immagini o video sessualmente espliciti: tra tutela della privacy e revenge porn*”, su *Ilpenalista.it*, 30 Marzo 2021.

Si sosteneva, pertanto, che il giudice dell'esecuzione, ritenendo sussistente la continuità normativa rispetto alla vecchia versione del codice, avesse fatto un'applicazione della norma *in malam partem*, data la mancanza dei presupposti normativi o giurisprudenziali in tal senso.

I giudici della Cassazione hanno accolto tale tesi, sostenendo l'erroneità della conclusione formulata dal giudice dell'esecuzione, dato che, alla luce dell'intervenuta riforma del Codice Privacy, non si può ritenere che la condotta sia ascrivibile alla figura di reato a cui si era fatto riferimento.

Leggendo la norma, infatti, si nota che essa si riferisce soltanto alle ipotesi in cui la condotta sia posta in violazione dell'art. 9, par. 1 del GDPR, concernente i trattamenti necessari per motivi di interesse pubblico rilevante, o degli artt. 2-septies, 2-octies e 2-quinquedecies del Codice Privacy, concernenti rispettivamente le misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, i principi relativi al trattamento dei dati relativi a condanne penali e reati e il trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico.

Non vi rientrerebbe, dunque, la diffusione di dati appartenenti a categorie particolari, come nel caso di specie.

I Giudici di legittimità hanno rilevato che non è stata neanche posta la questione di continuità con l'art. 612-ter c.p., concernente, nello specifico, la condotta illecita di chi fa diffusione di immagini o video sessualmente espliciti.

L'epilogo della vicenda ha visto l'annullamento dell'ordinanza, e ciò ci dà l'occasione per riflettere sull'importanza del corretto inquadramento giuridico delle fattispecie, sia ai fini della punibilità che del contrasto effettivo di fenomeni come quello esaminato.

La Suprema Corte ha affermato il seguente principio: il giudice di merito, chiamato ad interpretare la portata dell'art. 167-bis del Codice Privacy, deve interrogarsi circa la sussistenza di continuità normativa fra tale norma ed altre disposizioni normative, anche non appartenenti al Codice Privacy.

Rilevante, sul tema, è stata la modifica al Codice prodotta dal recente D.L. n. 139/2021 (c.d. "Decreto Capienze"), il quale introduce l'art. 144-bis, rubricato, appunto, "*revenge porn*", con cui viene riconosciuto alle vittime del reato, ivi inclusi i minori ultraquattordicenni, il diritto di presentare reclamo o segnalazione innanzi al Garante della privacy nell'ipotesi in cui vi sia il fondato timore che una delle condotte descritte dall'art. 612-ter c.p. possa essere realizzata.

Il potere di intervento del Garante è quello ai sensi dell'art. 58 del GDPR: egli può, ad esempio, ordinare l'interruzione del trattamento o la rimozione dei contenuti illeciti. Lo scopo della norma è quello di *anticipare* la tutela riconosciuta alle vittime, dando loro la possibilità di invocare l'intervento dell'Autorità già prima che il reato sia effettivamente commesso; dunque, non viene ampliato il novero di strumenti *correttivi* di cui può servirsi l'Autorità.

Gli strumenti che l'interessato può utilizzare sono il reclamo e la segnalazione, accessibili gratuitamente e meno onerosi dei classici rimedi giurisdizionali.

La speranza è che l'introduzione di questa nuova disposizione, ossia la previsione di un sistema di tutela anticipato e parallelo rispetto a quello tradizionale, possa – se non eliminare – quanto meno arginare il più possibile il fenomeno.

È fisiologico che il sistema giuridico si debba adattare alle nuove tecnologie, con un necessario ripensamento rispetto alle fattispecie esistenti, data la repentina diffusione dei mezzi di comunicazione di massa cui stiamo assistendo.

Il mondo digitale, se da un lato moltiplica le occasioni di contatto, dall'altro aumenta in maniera proporzionale le incertezze in merito alla liceità del comportamento sul web, i cui limiti non sono ancora definiti.

Gli utenti pagano le più aspre conseguenze, e i loro diritti costituzionalmente tutelati rischiano seriamente di essere messi a repentaglio con una lesività maggiore rispetto al passato.

I comportamenti illeciti sulla rete sono sempre più difficilmente identificabili, e anche gli eventuali rimedi sembrano essere spesso insufficienti.

La Dichiarazione dei diritti in *internet* del 2015, tuttavia, precisa che i diritti fondamentali di ogni persona sono garantiti anche sul web, e devono essere interpretati in modo da assicurarne l'effettività, nel pieno rispetto della dignità, libertà, uguaglianza e diversità di ognuno (art. 1).

Pertanto, il compito dell'ordinamento è quello di reinterpretare le norme esistenti in modo aperto e realizzare tale obiettivo.

L'art. 9 della Dichiarazione, inoltre, riconosce il diritto a non veder rappresentata erroneamente la propria identità in rete.

Questo tema è caro alla giurisprudenza, la quale si è pronunciata svariate volte cercando di adattare il contenuto dell'articolo 595 c.p. al web e temperarlo con la tutela della libertà di cui all'art. 21 Cost.

Una delle domande che ogni giurista si è posto è quella relativa all'estensibilità della nozione di stampa ai periodici telematici, soprattutto allo scopo di accertare la legittimità, per questi ultimi, del sequestro preventivo a scopo cautelativo.

Ci si è interrogati, inoltre, sulla possibilità di aggravamento della pena in caso di diffamazione tramite *social network*, *forum* e *blog*, in ragione della maggiore diffusività del mezzo.

È stata considerata, inoltre, la responsabilità a carico a chi ha la possibilità di avere accesso ai contenuti in rete e sono state analizzate le politiche perseguite dalle piattaforme *online* in materia.

I maggiori problemi sono legati al fatto che non è prevista una garanzia *ex ante* per gli utenti che usufruiscono della rete, i quali sono costretti a beneficiare unicamente di rimedi riparatori e mai di inibitorie preventive a causa dell'eccessiva onerosità che questo comporterebbe per i *provider*.

Tuttavia, sarebbe auspicabile un equo bilanciamento tra gli interessi coinvolti e sarebbe opportuno adottare soluzioni tecniche, anche automatizzate, finalizzate alla prevenzione di quella maggiore lesività della condotta veicolata dalla rete.

Lo sviluppo e la diffusione degli strumenti informatici hanno favorito l'utilizzo sempre più frequente di *blog*, *chat rooms*, *forum*, periodici *online*, *social networks*, *mailing-list* e *newsgroup*.

Frequente è il superamento, da parte degli utenti che utilizzano queste piattaforme, dei confini della libertà di espressione, della critica ovvero della cronaca, ledendo il diritto all'altrui reputazione (es. *hate speech*)

Come sostenuto da autorevole dottrina, i diritti della personalità di una persona corrispondono alle sue qualità, che devono essere tutelate nel rapporto con gli altri. Tra questi diritti personali assoluti di esclusione vi è anche il diritto all'onore; questi diritti trovano la loro fonte nella personalità dell'uomo ed alcuni sono "*la causa prima*" di tutti gli altri diritti particolari²³⁹.

Secondo la Corte Costituzionale, è l'art. 2 Cost.²⁴⁰ a riconoscere il diritto all'identità personale, inteso come diritto ad essere se stessi con le proprie idee, esperienze, convinzioni ideologiche e religiose, tutti elementi che qualificano un dato individuo²⁴¹. Leggendo insieme tale disposizione con le altre norme che riconoscono e garantiscono le singole libertà dell'individuo, si possono desumere gli ulteriori diritti della personalità, come ad esempio il decoro e l'onore, la rispettabilità, la riservatezza, l'intimità e la reputazione.

Per quanto riguarda la previsione costituzionale del diritto di manifestare il proprio pensiero, non si tratta di una tutela incondizionata, essendo essa temperata dall'esistenza di interessi diversi che sono ugualmente garantiti. Vi rientra l'onore, insieme al decoro e alla reputazione, in quanto diritti inviolabili della persona umana²⁴². Questi diritti ricevono tutela dall'ordinamento ai sensi dell'articolo 595 c.p., il quale punisce qualsiasi espressione diffamatoria dell'altrui onore e decoro, indipendentemente dal mezzo con cui la stessa sia perpetuata. Come noto, affinché il reato si configuri, è necessario che tale messaggio sia percepito come tale da una pluralità di soggetti. La diffamazione è punita più severamente in presenza di determinate aggravanti; si pensi a quella prevista nel comma 3, concernente l'utilizzo del mezzo della stampa o di altro mezzo di pubblicità.

La domanda che si è posta la giurisprudenza è quella relativa alla configurabilità o meno di tale aggravante nei casi di diffusione del messaggio diffamatorio tramite giornale *online*, *blog*, *social networks* e *forum*.

²³⁹ G. ALPA, "Alle origini dei diritti della personalità", in *Riv. Trim. di Dir. Proc. Civ.*, 3, 2021, p. 567.

²⁴⁰ Art. 2 Cost.: "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*".

²⁴¹ Cfr. I diritti fondamentali nella giurisprudenza della Corte Costituzionale, 2006, p. 8., Corte Costituzionale, sent. n. 98/1979.

²⁴² *Idem*. Tale limite è espressamente riconosciuto dall'articolo 10 della CEDU: "*L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica [...] alla protezione della reputazione o dei diritti altrui*".

Bisogna partire dal presupposto che, nel caso del giornale *online*, la sua configurabilità come “stampà” è stata storicamente esclusa da numerose pronunce della Cassazione²⁴³. L’impossibilità di estensione era collegata alla definizione di “stampà” contenuta nell’art. 1 della l. 47/1948, che ricomprende le riproduzioni tipografiche o ottenute con mezzi meccanici o fisico-chimici in qualsiasi modo destinate alla pubblicazione.

È chiaro che una tale interpretazione storica della norma limiti l’applicabilità delle garanzie riservate ai periodici unicamente alla “*carta stampata*”.

Tuttavia, successivamente, le Sezioni Unite della Cassazione²⁴⁴ si sono pronunciate sul tema del sequestro preventivo tramite oscuramento di una pagina telematica, in un caso che riguardava la diffamazione *online* sulla pagina di un noto quotidiano.

Ebbene i giudici, dopo aver dichiarato l’idoneità di tale misura cautelare, hanno però chiarito che non è ammissibile il sequestro preventivo di un periodico *online* fuori dai casi previsti dalla legge poiché, sulla base dell’equiparazione, a certe condizioni, delle testate telematiche alla stampa cartacea, vi è la conseguente applicabilità delle garanzie costituzionali di cui all’art. 21 Cost.

La Cassazione si è discostata dall’esegesi letterale del dettato normativo, privilegiando una interpretazione estensiva ed evolutiva dello stesso, consapevole che in senso figurato la definizione di stampa su richiamata, fa riferimento ai giornali come mezzo elettivo di informazione a prescindere dalla digitalizzazione di cui si ignorava l’esistenza quando una simile norma fu elaborata.

La Corte ci dice che un prodotto editoriale propriamente inteso possiede dei requisiti ontologici e teleologici, quali una “testata”, la periodicità regolare delle pubblicazioni, la finalità informativa e diretta al pubblico, oltreché un generico interesse alla pubblicazione, ossia alla diffusione dell’informazione.

C’è, inoltre, il requisito del direttore responsabile e quello relativo alla registrazione delle testate presso la cancelleria del competente Tribunale.

Alla luce di ciò è evidente che tali requisiti, pacificamente appartenenti alla stampa, non sono menzionati nell’articolo 1 della l. 47/1948, ancorata invece alle tecnologie dell’epoca.

Comunque, la Corte ha sostenuto che non ci sono ostacoli alla possibilità di accreditare il giornale telematico come stampa alla luce dei progressi tecnologici e in presenza dei

²⁴³ Cass. Pen., sez. V, 16/07/2010, n. 35511, disponibile su *dejure.it*; nota a sentenza di S. PERON, “Internet, regime applicabile per i casi di diffamazione e responsabilità del direttore”, su *Responsabilità Civile e Previdenza*, fasc. 1, 2011, pag. 85; Cass. Pen., sez. V, 28/10/2011, n. 44126, disponibile su *dejure.it*; nota a sentenza di D. PETRINI, “Il direttore della testata telematica, tra horror vacui e prospettive di riforma; sperando che nulla cambi”, su *Riv. It. Dir. e Proc. Pen.*, fasc. 4, 2012, pag. 1611; Cass. Pen., sez. V, 05/11/2013, n. 10594, con nota di C. MELZI D’ERIL, “La Cassazione esclude l’estensione ai siti internet delle garanzie costituzionali previste per il sequestro di stampati”, in *Dir. Pen. Uomo*, 2014.

²⁴⁴ Cass. Pen., Sez. Un., 17/07/2015, n. 31022, disponibile su *dejure.it*; nota a sentenza di L. DIOTALLEVI, “La Corte di cassazione sancisce l’“equiparazione” tra giornali cartacei e telematici ai fini dell’applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di “scivolamento” dalla “nomofilachia” alla “nomopoiesi”?”, su *Giurisprudenza Costituzionale*, fasc. 3, 2015, pag. 1062.

requisiti sopra elencati. Invero, l'elemento caratterizzante dell'attività giornalistica è il *fine informativo*, dunque, in presenza di esso, i periodici telematici possono essere assimilati ontologicamente e funzionalmente alla pubblicazione cartacea.

Conclusione rilevante, soprattutto perché in tal modo alla testata telematica vengono applicate le disposizioni costituzionali e ordinarie che disciplinano l'attività di informazione diretta al pubblico e, nel caso di specie, non è attuabile il sequestro preventivo, poiché la diffamazione a mezzo stampa non rientra tra i casi al ricorrere dei quali la legge lo consente.

La pronuncia, inoltre, chiarisce la differenza di trattamento ed inquadramento normativo tra testate e ulteriori mezzi di informazione quali *blog*, *social network* e *forum*, ugualmente rientranti nell'ambito dell'art. 21 Cost., quali strumenti attraverso cui manifestare liberamente la propria opinione, ma che *non rientrano* nel concetto di stampa. Infatti, nei vari siti, *blog*, *forum* ecc., diversi dai periodici *online*, ci sono pagine web che consentono uno scambio di opinioni e commenti, in forma sia privata che pubblica, che difettano dei requisiti di assimilabilità alla stampa.

Per inquadrare correttamente il fenomeno è necessario che il giornale *online* possenga i requisiti di cui all'art. 2, l. 47/1948.

Per parlare di “stampato” è necessario che siano indicati il luogo e l'anno di pubblicazione, il nome e il domicilio dello stampatore e, se esiste, dell'editore. Solo per quanto concerne i giornali, le agenzie di informazioni e i periodici è necessario aggiungere i dati identificativi del proprietario e del direttore (o vice) responsabile.

Perché si possa parlare propriamente di giornale o periodico, bisogna inoltre registrare lo stesso presso la cancelleria del tribunale, nella cui circoscrizione debba effettuarsi la pubblicazione, ai sensi dell'articolo 5, l. 47/1948. Ciò sia nel caso in cui l'editore intenda ottenere contributi statali ovvero preveda di avvalersi di giornalisti professionisti, pubblicisti e praticanti.

Per i periodici web di piccole dimensioni, quest'ultimo obbligo non è imprescindibile, perché se si tratta di giornali realizzati unicamente su supporto informatico e diffusi unicamente per via telematica ovvero *online*, i cui editori non abbiano fatto domanda di contributi o agevolazioni pubbliche e che conseguano ricavi annui inferiori a 100.000 euro, questi non sono soggetti alla registrazione di cui all'art. 5 (art. 3-bis, l. 103/2012).

Al contrario, l'art. 3 della l. 103/2012 impone dei parametri per valutare la periodicità di testate giornalistiche di grandi dimensioni che offrano contenuti anche *online*, parametri che riguardano l'accessibilità *online* della testata, anche a titolo non oneroso, la garanzia di un'informazione quotidiana composta da informazione autoprodotta per almeno dieci articoli al giorno, con un aggiornamento pari ad almeno 240 giorni per i quotidiani, 45 per i settimanali e plurisettimanali, 18 uscite per i quindicinali e 9 per i mensili. In più, qualora la testata sia pubblicata sia in edizione cartacea sia in edizione digitale, con lo stesso marchio editoriale, l'impresa non è tenuta all'iscrizione di entrambe le testate, ma solo a dare apposita comunicazione al registro degli operatori di comunicazione (art. 3, l. 103/2012).

Concludendo, per le testate giornalistiche *online* non è configurabile un obbligo di registrazione ai fini dell'equiparazione degli stessi alla nozione di stampa.

La giurisprudenza successiva alle Sezioni Unite del 2015 si è uniformata all'orientamento secondo cui i periodici *online* sarebbero assimilabili alla stampa, contrariamente ai *social, forum, blog* e *newsletter* i quali, pur essendo tutelabili ai sensi dell'art. 21 Cost., non godrebbero tuttavia delle garanzie costituzionali di cui ai commi successivi al primo, non essendo soggetti alla normativa e tutela accordata alla stampa. Per quanto riguarda l'applicabilità dell'aggravante di cui al comma 3 dell'articolo 595 c.p., si è scelto di ricomprendere nell'ambito del “*qualsiasi altro mezzo di pubblicità*” i *social network, blog* o *forum* in cui si perpetuava il reato di diffamazione²⁴⁵.

L'aggravante in questione si applica ai *social network* anche in virtù del costante orientamento volto a considerarli come strumenti idonei a raggiungere una pluralità di persone, determinando quella maggiore diffusività dell'offesa che giustifica un trattamento sanzionatorio più severo²⁴⁶.

Nulla osta, ai fini della configurabilità dell'aggravante, la pubblicazione del contenuto diffamatorio nella bacheca *Facebook* della persona offesa, poiché la maggiore diffusività è comunque configurabile.

Da parte di alcuni, in effetti, era stato sostenuto che, nel caso in esame, non si integrasse la pubblicazione, con conseguente diffusione, del messaggio diffamatorio, poiché potevano agire i meccanismi di privacy impostati dalla persona sulla cui bacheca era pubblicato il messaggio.

Contrariamente a questa tesi, la Cassazione ha deciso sia per l'applicabilità dell'aggravante sulla base dell'idoneità del mezzo (*Facebook*) a consentire un'ampia e indiscriminata diffusione della notizia, sia per l'idoneità della bacheca a tal fine, indipendentemente dalle impostazioni della privacy; e ciò “*sia perché, per comune esperienza, bacheche di tal natura racchiudono un numero apprezzabile di persone (senza le quali la bacheca Facebook non avrebbe senso), sia perché l'utilizzo di Facebook integra una delle modalità attraverso le quali gruppi di soggetti socializzano le rispettive esperienze di vita, valorizzando in primo luogo il rapporto interpersonale, che, proprio per il mezzo utilizzato, assume il profilo del rapporto interpersonale allargato ad un gruppo indeterminato di aderenti al fine di una costante socializzazione*”²⁴⁷.

²⁴⁵ Cfr. Cass. Pen., sez. I, 28/04/2015, n. 24431, disponibile su *dejure.it* e su *Ilpenalista.it*, 4 settembre 2015, con nota di V. SPAZIANI TESTA; Cass. Pen., sez. V, 25/01/2021, n. 13979, disponibile su *dejure.it* e su *Responsabilità Civile e Previdenza*, 2021, 4, 1341.

²⁴⁶ Cfr. Cass. Pen., sez. I, 28/04/2015, n. 24431, cit.

²⁴⁷ Cfr. Cass. Pen., sez. I, 28/04/2015, n. 24431, cit. Un'altra interessante pronuncia da prendere in considerazione è la recente sentenza n. 27939 del 13 ottobre 2021, con cui la Corte di Cassazione, confermando la decisione della Corte d'Appello di Roma, ha rigettato definitivamente il ricorso contro un licenziamento di un ex dipendente TIM, statuendo che il lavoratore che insulta i propri responsabili sui *social network* può incorrere nel licenziamento per giusta causa. Il caso ha preso le mosse dalla diffusione – tramite tre e-mail e un post sulla propria pagina Facebook – di diverse frasi rivolte ai propri superiori, gravemente offensive e diffamatorie, cui è seguito il licenziamento del dipendente per giusta causa, in applicazione dell'art. 2119 c.c., per la grave insubordinazione posta

Nel caso in cui la portata diffamatoria del messaggio non emerga direttamente, ma derivi da una discussione nei commenti ad un post all'interno di un gruppo Facebook, la Corte ha optato per un bilanciamento con il diritto di libera espressione del pensiero, escludendo la fattispecie nel caso dell'azione di chi abbia inteso condividere una critica nei confronti della persona offesa, ma nel farlo sia rimasto entro i limiti dell'esercizio del proprio diritto di manifestazione del pensiero, senza condividerne le forme illecite usate da altri.

La Corte ha stabilito, infatti: *“che l'imputato condividesse o meno i presunti insulti che altri avrebbero postato è infatti circostanza irrilevante nella misura in cui la sua condotta materiale non evidenzia oggettivamente alcuna adesione ai medesimi, rilanciandoli direttamente o anche solo indirettamente. [...] La condotta contestata potrebbe assumere in astratto rilevanza penale soltanto qualora potesse affermarsi che con il proprio messaggio l'imputato aveva consapevolmente rafforzato la volontà dei suoi interlocutori di diffamare”*²⁴⁸.

Dunque, i giudici di legittimità escludono che sia integrato il reato di diffamazione nel caso in cui il discorso o l'espressione configurino una semplice condivisione di un *post* nel suo complesso, e qualora il commento non abbia carattere esplicitamente diffamatorio.

Alla luce di quanto detto, non dovrebbe configurarsi la fattispecie in questione qualora il contenuto diffamatorio venga semplicemente condiviso o si esprima un gradimento allo stesso, attraverso i c.d. *likes* ai *post* o ai commenti.

Questo perché, pur manifestando la persona un'adesione al contenuto offensivo, non ne si condividono le modalità illecite; dunque, la condotta non sarebbe manifestamente diffamatoria²⁴⁹.

in essere attraverso i mezzi di comunicazione citati. Secondo il lavoratore, i post sulla pagina Facebook erano da considerarsi riservati, in quanto la pagina era destinata alla comunicazione esclusiva con i propri “amici”. Tuttavia, secondo i Giudici, la tutela della libertà e della segretezza della corrispondenza non può trovare applicazione dal momento che lo strumento utilizzato non integra le caratteristiche della corrispondenza o di “ogni altra forma di comunicazione”, ovvero l'attualità, la determinatezza o determinabilità del destinatario e la segretezza della comunicazione. Viene in questo caso in rilievo il concetto di “*bacheca Facebook*”, alla quale possono accedere gli utenti considerati “amici” dal titolare dell'account. Ebbene, se da una parte tale elenco di “amici” non comprende la totalità degli utilizzatori del *social network*, dall'altra parte l'elenco è sempre modificabile tramite l'accettazione o la rimozione di ulteriori “amicizie” da parte dell'utente, comportando perciò l'impossibilità di avere un numero di destinatari determinato o determinabile; emerge, quindi, l'elemento della pluralità, previsto nella fattispecie della diffamazione. V. A. DE LUCIA, “*Offese su Facebook: la Cassazione conferma la legittimità del licenziamento*”, su *altalex.com*.

²⁴⁸ V. Cass. Pen., sez. V, 29/01/2016, n. 3981, con nota di A. ALÌ, “*Diffamazione via Facebook: condividere post offensivi non è reato*”, su *altalex.com*, 2016.

²⁴⁹ La Corte d'Appello dell'Aquila, con la sentenza 1659 del 9 novembre 2021, si è espressa sul rapporto contrattuale che si instaura tra utente e *social network*, concludendo che l'utente ingiustamente bannato da un *social* ha diritto di ottenere il risarcimento del danno subito a causa della sospensione delle proprie relazioni sociali. La pronuncia ha preso le mosse dal ricorso presentato da un utente che, dopo aver pubblicato foto didascalie e commenti sulla figura di Mussolini, mostrando

Capitolo XVI

La diffamazione tramite chat privata o *mailing list*

Quid iuris nel caso di un messaggio lesivo dell'onore e della reputazione di un soggetto, trasmesso tramite chat di gruppo o *mailing list*, ovvero posta elettronica indirizzata a più destinatari in cui partecipava la persona offesa? Si può configurare il reato di diffamazione?

Partiamo dal presupposto la Cassazione²⁵⁰ ha ritenuto che la *mailing list* rientri nell'alveo "*dell'altro mezzo di pubblicità*" di cui si è detto, poiché configura un mezzo di comunicazione in cui si condividono informazioni utili, ad un numero anche ampio di destinatari, circa le quali è possibile esprimere condivisione, commentare e discutere. Eppure, la questione principale sollevata dalla *mailing list* è quella relativa alla configurabilità stessa del reato di diffamazione, data la partecipazione del soggetto offeso alla conversazione diffamante.

Di recente, nell'Aprile del 2021, la Corte di Cassazione è stata investita della questione in un caso in cui il ricorrente lamentava l'errata qualificazione del fatto come diffamazione e la configurabilità, al contrario, della fattispecie depenalizzata di cui all'articolo 594 c.p. (ingiuria), poiché la persona offesa avrebbe partecipato "in tempo reale" alla conversazione. I giudici hanno respinto tale obiezione.

Non è facile adattare le norme al contesto digitale: in effetti, è lecito il dubbio circa la "presenza" della persona offesa come circostanza che renderebbe applicabile l'illecito depenalizzato dell'ingiuria, al massimo configurabile come aggravato dalla comunicazione a distanza, ovvero dalla presenza contestuale di altre persone, come attualmente previsto dai commi 2 e 4 dell'articolo, abrogato con il D.lgs. n. 7 del 2016. Tale norma consente di operare un discrimine con la diffamazione, che si configura allora, secondo la Corte, nel caso dell'offesa "a distanza" della comunicazione lesiva, qualora indirizzata anche ad altri soggetti oltre che all'offeso (fermo restando che

la propria appartenenza politica, era stato sospeso da Facebook per oltre quattro mesi per violazione degli «*standard della comunità*». I Giudici di prime cure hanno condannato Facebook a un risarcimento di 15 mila euro a titolo di danno morale e il *social network* ha impugnato la decisione. La Corte d'Appello, nel decidere la questione, è partita dal fatto che il contratto tra le parti è un contratto a titolo oneroso e a prestazioni corrispettive, dove il "prezzo" pagato dall'utente è rappresentato dalla concessione dei propri dati personali a fini commerciali. Dunque, se è vero che ogni *social network* può introdurre clausole con poteri di rimozione dei post degli utenti e di sospensione degli *account*, è anche vero che i *social* devono fare attente valutazioni prima di attivare poteri di sospensione o rimozione. Nel caso di specie, i giudici hanno ritenuto lecite le prime due sospensioni dell'*account*, effettuate per commenti lesivi dell'altrui reputazione (l'utente aveva definito "*stupido*" un altro utente); tuttavia, ha considerato che le successive sospensioni fossero illegittime, poiché «*la mera pubblicazione di una foto con un commento che si limita all'espressione del proprio pensiero (...) non si ritiene sufficiente a violare gli standard della comunità*». In appello si è quindi ridimensionato il risarcimento dovuto, in 3 mila euro.

²⁵⁰ Cfr. Cass. Pen., Sez. Un., 17/07/2015, n. 31022, cit.

l'offesa riguardante un assente comunicata ad almeno due persone, presenti o distanti, integra sempre la diffamazione).

È quindi nata la necessità di riempire il significato di “*presenza*”, alla luce di mezzi quali *mailing list*, videoconferenze o audio conferenze. Negli ultimi due casi, e nelle situazioni equivalenti, in cui cioè ci si trovi alla presenza anche virtuale dell'offeso unitamente ad altri soggetti che possono interagire in audio, video o scrivere istantaneamente – quindi di fatto in una riunione virtuale – si configurerebbe l'ingiuria²⁵¹.

Invece, nel caso di *mailing list*, è difficile – se non impossibile – parlare di presenza virtuale, perché le e-mail sono considerate delle lettere in formato elettronico, indirizzate a persone che non sono contestualmente presenti. Per tale ragione, nonostante il fatto si compia con un unico gesto, la trasmissione effettiva del messaggio si realizza attraverso una pluralità di atti di cui l'agente ha coscienza e volontà.

In sostanza, la Corte²⁵² considera integrato il reato di diffamazione nel caso in cui il fatto è compiuto tramite l'invio di e-mail di contenuto offensivo, sebbene tra i destinatari del messaggio vi sia la persona offesa.

Tale orientamento non è però pacifico: in altri casi, la “*presenza*”, da remoto o virtuale, dell'offeso, ha guidato i giudici verso un'interpretazione rigida del dettato normativo, e si è optato per l'applicazione dell'art. 594, ultimo comma c.p.²⁵³

Passando ad esaminare l'esimente del diritto di critica, si può iniziare col dire che il diritto della persona a non veder leso il suo onore e la sua reputazione non è configurato come assoluto nel nostro ordinamento, potendo essere limitato dall'altrettanto legittima libertà di manifestazione del pensiero, anche in rete, di cui all'art. 21 Cost.

²⁵¹ Cfr. Cass. Pen., sez. V, 25/02/2020, n. 10905, disponibile su *dejure.it* e su *Responsabilità Civile e Previdenza* 2020, 4, 1306. Si veda anche la recente sentenza 2 dicembre 2021, n. 44662, della Quinta Sezione Penale della Corte di Cassazione, commentata da M. MARTORANA, “*L'offesa su Facebook non è reato se l'insultato è online*”, su *altalex.com*, febbraio 2022. Nel caso di specie, i giudici della Corte d'Appello di Catanzaro avevano confermato la condanna di un soggetto per diffamazione per aver pubblicato commenti e insulti su una *chat* con la persona offesa. La Corte di Cassazione, tuttavia, ha accolto il ricorso dell'imputato, che richiedeva di qualificare la fattispecie come ingiuria e non come diffamazione. In sostanza, la Corte ha ribadito l'importanza del requisito della presenza della vittima per la distinzione tra ingiuria e diffamazione, presenza che secondo i giudici può essere anche “virtuale” e non necessariamente fisica o telefonica. Poiché nel caso di specie il destinatario delle offese in *chat* era *online* e, dunque, riceveva i messaggi in tempo reale, la fattispecie che si è configurata è quella dell'ingiuria, con esclusione del reato di diffamazione e della rilevanza penale della condotta. La Corte, richiamando la precedente sentenza n. 10905/2020, ha chiarito che anche laddove gli insulti fossero stati proferiti durante una riunione da remoto tra più individui compreso l'offeso si sarebbe trattato di ingiuria commessa alla presenza di più persone, anch'essa depenalizzata.

²⁵² Cass. Pen., sez. V, 02/02/2017, n. 12603, disponibile su *dejure.it* e su *Cassazione Penale* 2017, 9, 3312 e *CED* Cass. pen. 2017; Cass. Pen., sez. V, 06/07/2018, n. 34484, disponibile su *dejure.it* e su *Diritto & Giustizia*, 23 luglio 2018; Cass. Pen., sez. V, 04/03/2021, n. 13252, disponibile su *dejure.it*; nota a sentenza di A. IEVOLELLA, “*Offeso con una e-mail inviata a lui e ad alcuni colleghi: è diffamazione*”, su *Diritto & Giustizia*, fasc. 73, 2021, pag. 7.

²⁵³ V. Cass. Pen., sez. V, n. 10905/2020, cit.

Il diritto di critica, quindi, come il diritto di cronaca o di satira, può, a determinate condizioni, moderare la portata del diritto all'onore.

La critica si esprime in un giudizio soggettivo, che non può certamente essere asettico o obiettivo, ma affinché si applichi l'esimente è necessario che il fatto di cui si stia trattando sia corrispondente a verità, per cui non dovrebbe essere arbitrariamente inventato o elaborato esorbitando da quello che è il nucleo essenziale, come specificato dal Tribunale di Firenze con la pronuncia n. 1502 del 2019. Dunque, è necessario che la verità sia quanto meno putativa in ragione di una verifica sulle fonti da cui proviene o sul contesto all'interno del quale il fatto è avvenuto.

Oltre a questo requisito della verità, devono sussistere anche la continenza espositiva e l'interesse sociale alla notizia. Quest'ultimo è connesso alla necessità che la critica soddisfi l'interesse di un pubblico alla notizia e alla sua interpretazione critica, che non sia, dunque, mera curiosità pur potendo riguardare la vita privata di un soggetto (c.d. principio di pertinenza). Per quanto riguarda la continenza espressiva, questa non esclude la possibilità di un linguaggio più colorito o pungente, purché esso sia strumentalmente collegato alla manifestazione di un dissenso ragionato dall'opinione o dal comportamento preso di mira, tanto che, in ultima analisi, il giudizio in questione deve essere accompagnato da una motivazione in merito al disvalore attribuito, dato che la critica non può risolversi in una aggressione gratuita, come evidenziato dalla giurisprudenza²⁵⁴.

Allorquando non possa trovare applicazione l'art. 51 c.p. – che esclude la punibilità nei casi in cui il fatto sia commesso nell'adempimento di un dovere o nell'esercizio di un diritto (chiaramente quello di cui all'art. 21 Cost.) – è possibile invocare l'*exceptio veritatis*, nei limiti di quanto previsto dall'art. 596 c.p.²⁵⁵

Si tratta di una disposizione volta a considerare la verità dei fatti come causa di esclusione della punibilità qualora la stessa sia accertata per fatti determinati, nei casi di accordo tra offensore ed offeso per il deferimento dell'accertamento ad un giuri d'onore, ovvero nei casi di cui al comma 3 dello stesso articolo.

Per escludere la punibilità serve che la prova del fatto sia completa, e non parziale, ai fini di una perfetta aderenza dei fatti di causa con quelli realmente accaduti: non devono essere riportate inesattezze non marginali, idonee a modificare l'assetto sostanziale degli eventi²⁵⁶. Comunque, anche qualora la verità sia provata, se i modi usati sono

²⁵⁴ Si vedano le sentenze Tribunale di Firenze, 15/05/2019, n. 1502, disponibile su *dejure.it* e su *Redazione Giuffrè 2019*; Corte di Appello di Taranto, 27/01/2021, n. 84, disponibile su *dejure.it* e su *Guida al diritto 2021*, 23; Cass. Civ., sez. III, 26/10/2017, n. 25420, disponibile su *dejure.it*; note a sentenza di I. ALAGNA, "Diffamazione a mezzo stampa: il reato sussiste anche in assenza di esplicita indicazione del nome", su *Ridare.it*, 18 dicembre 2017 e A. VILLA, "Il diritto di critica ancorché contenga giudizi soggettivi deve fondarsi su fatti che debbono corrispondere a verità perlomeno putativa", su *Diritto & Giustizia*, fasc. 171, 2017, pag. 11; Tribunale di Milano, sez. I, 15/07/2020, n. 4250, disponibile su *dejure.it* e *Redazione Giuffrè 2020*; Cass. Civ., sez. III, 29/10/2019, n. 27592, disponibile su *dejure.it* e *Giustizia Civile Massimario 2019*.

²⁵⁵ Vedi Cass. Pen., sez. V, 16/06/2016, n. 41414, disponibile su *dejure.it* e *CED Cass. pen. 2016*.

²⁵⁶ Cass. Pen., sez. V, 18/11/2019, n. 7008, disponibile su *dejure.it* e *CED Cass. pen. 2020*.

stati diffamanti, secondo una valutazione conforme al principio di continenza espositiva, non è automatica l'esclusione della punibilità per il reato di diffamazione. In realtà, sembrerebbe che una disposizione come quella esaminata voglia sancire il divieto dell'*exceptio veritatis*, che non si applica che nei casi previsti dall'art. 596 c.p. e nell'esercizio di un diritto, ex art. 51 c.p. (all'interno del quale è pacificamente ricomprensibile il diritto di critica). In definitiva, dunque, in determinate circostanze, viene temperato il diritto a non veder leso il proprio onore con l'interesse alla verità oggettiva o putativa che sia, che si dimostra, però, inidonea, da sola, ad escludere la punibilità. Resta fermo che l'assenza di uno dei criteri richiamati (verità, interesse pubblico, continenza espressiva) determina la carenza dell'esimente del diritto di critica, per cui il diritto di manifestare liberamente il proprio pensiero non è giustificato ma punibile, e dunque risarcibile. Se accade il contrario, la condotta è da considerare lecita.

Passando ad esaminare il profilo del danno, nel caso in cui la fattispecie si perfeziona, questo pregiudizio si può considerare, anzitutto, come una lesione di un interesse giuridicamente apprezzabile; in secondo luogo, come un effetto economico negativo; in terzo luogo, come liquidazione pecuniaria dell'evento economico negativo²⁵⁷.

Il danno ex art. 2043 c.c. è un danno *non iure e contra ius*, perché generato da un comportamento non giustificato dall'ordinamento e che lede un interesse giuridicamente tutelato. Ovviamente, grava sulla parte che si dichiara lesa provare la sussistenza del nesso di causalità tra l'azione ed il danno ingiusto derivatone, nonché l'imputabilità soggettiva a carico del presunto offensore²⁵⁸.

È interessante notare che nei casi di diffamazione perpetuata in internet, è stato registrato che in luogo dell'azione penale si è preferita quella civile del risarcimento del danno²⁵⁹ ed inoltre, stante la difficoltà di provare il danno patrimoniale, ai sensi dell'articolo 2043 c.c., si è preferito ricorrere al danno di cui all'articolo 2059 c.c.

Molto spesso, infatti, il fatto illecito genera comunque un turbamento, una sofferenza interiore, con conseguenze pregiudizievoli risarcibili.

Al riguardo, deve essere illustrato brevemente il contributo delle Sezioni Unite della Cassazione che, con le c.d. sentenze gemelle del 2008, hanno ridefinito i confini del danno non patrimoniale. La Corte ha, infatti, ricondotto ad unità fenomenica e giuridica il danno non patrimoniale, sancendo l'unitarietà del pregiudizio le cui differenti denominazioni (danno morale, danno biologico, danno da perdita del rapporto parentale) sono semplicemente descrittive.

²⁵⁷ M. BIANCA, "Diritto civile", Milano, 2011, 123.

²⁵⁸ Cass. Civ., Sez. Un., 26/01/1971, n. 174, in *Resp. Civ. Prev.*, 1971, 67 ss.

²⁵⁹ Solo nel biennio 2011-2012, su un campione di 112 sentenze emesse dal Tribunale di Milano, sono state registrate richieste risarcitorie per un ammontare pari a €766.511,93; cfr. *New Tabloid*, 3, 2013, 32 ss., come riportato da S. PERON, "Il risarcimento dei danni da diffamazione: analisi e riflessione sui criteri orientativi proposti dell'Osservatorio sulla Giustizia civile di Milano" (edizione 2018), in *filodiritto.it*, 2018.

Se il fatto illecito si configura come reato, dunque, è risarcibile il danno non patrimoniale sofferto dalla persona offesa nella sua più ampia accezione di danno determinato dalla lesione di interessi inerenti alla persona, non connotati da rilevanza economica²⁶⁰. Nel caso di diffamazione, quindi, qualora non si possano riscontrare degenerazioni patologiche della sofferenza, si verificherà il danno morale, ove sia allegato il turbamento dell'animo o il dolore intimo sofferti²⁶¹.

Il giudice di merito deve accertare l'effettiva consistenza del pregiudizio allegato, a prescindere dal nome attribuitogli, individuando quali ripercussioni negative sul valore-uomo si siano verificate e provvedendo alla loro integrale riparazione.

La prova del danno è a carico sulla parte lesa, che potrà però servirsi anche di mezzi di prova presuntivi che testimonino che lo scritto offensivo abbia ingenerato una ripercussione dolorosa nella sfera personale. I danni così provati non potranno che essere liquidati in via equitativa²⁶².

Molteplici sono i parametri di quantificazione del danno adoperati dalla giurisprudenza con specifico riferimento alla liquidazione del danno da diffamazione a mezzo di comunicazione di massa.

Anzitutto rileva la diffusività della notizia, con riguardo alla notorietà del diffamante; poi è importante un'eventuale reiterazione della condotta; si guarda anche alla collocazione della notizia/commento (se in una posizione rilevante rispetto ad altre²⁶³); al mezzo (se sia o meno idoneo ad una più capillare diffusione); è importante, inoltre, la risonanza mediatica suscitata dalle notizie diffamatorie. Ma non solo. Si guarda anche alla posizione sociale ricoperta dal diffamato, senza però distinguere tra reputazione professionale e personale, poiché la rilevanza è data alla complessiva diminuzione del valore della persona.

Certamente rileva l'*animus diffamandi*, quindi la presenza o meno degli elementi esimenti richiamati. Infatti, pur bastando l'elemento della colpa, l'intensità dell'elemento psicologico certamente rileva nella quantificazione del danno. Ancora rilevano le conseguenze dell'azione diffamatoria: in senso favorevole al diffamante acquisiscono importanza alcuni comportamenti quali la ratifica delle dichiarazioni ovvero la pubblicazione della sentenza in uno o più quotidiani.

In base alle decisioni risarcitorie della giurisprudenza, sono state previste cinque categorie di diffamazione, sulla base del grado di lesività dell'offesa complessivamente

²⁶⁰ Punto 2.1, Cass. Civ., Sez. Un., 11/11/2008, n. 26972, disponibile su *dejure.it*; nota a sentenza di M. ROSSETTI, "Post nubila phoebus, ovvero gli effetti concreti della sentenza delle sezioni unite n. 26972 del 2008 in tema di danno non patrimoniale", su *Giustizia Civile*, fasc. 4-5, 2009, pag. 930.

²⁶¹ Punto 4.8, Cass. Civ., Sez. Un., 11/11/2008, n. 26972, cit.

²⁶² In tema di risarcimento del danno causato da diffamazione a mezzo stampa, la liquidazione del danno morale va necessariamente operata con criteri equitativi, il ricorso ai quali è insito nella natura del danno e nella funzione del risarcimento, realizzato mediante la dazione di una somma di denaro compensativa di un pregiudizio di tipo non economico (v. Cass. 05/12/2014, n. 25739; v. anche Cass. 16/07/2002, n. 10268, secondo cui la liquidazione del danno morale conseguente alla lesione dell'onore o della reputazione è rimessa alla valutazione equitativa del giudice).

²⁶³ A tal proposito, è stato ritenuto che anche solo il titolo di un articolo giornalistico sia idoneo ad integrare la fattispecie, cfr. Cass. Civ., sez. III, 07/08/2013, n. 18769.

considerata²⁶⁴. Le fasce sono le seguenti: tenue gravità, modesta gravità, media gravità, elevata gravità ed eccezionale gravità; la collocazione del fatto di reato dipenderà certamente dalla posizione ricoperta dal diffamato, ma parimenti dal grado di diffusività della notizia.

Ebbene, ci chiediamo se le categorie sopra rappresentate sono o meno idonee a trovare applicazione nel mondo di internet: nel grado di elevata gravità, oltre all'intensità dell'elemento soggettivo o alla gravità del discredito, si fa riferimento alla risonanza mediatica. Sulle piattaforme *social* è già intrinseca questa risonanza mediatica, indipendentemente dalla gravità dell'offesa o dall'intensità del dolo. Inoltre, se si guardano i rimedi risarcitori, solo una deindicizzazione della notizia o la rimozione della stessa possono dare "soddisfazione" all'offeso, ma neanche in quel caso si potrà avere la certezza che il contenuto sia rimosso dalla rete, o comunque che la condotta non sia reiterata. La domanda che ci si è posti è: la condotta diffamatoria tramite il web è da considerare sempre come di "elevata gravità"?²⁶⁵. Accogliendo questa interpretazione, si dovrebbero ridefinire tutte le altre categorie prospettate, perché al più elevato grado di lesività corrisponde un più elevato *quantum* risarcitorio²⁶⁶: potrebbe allora sembrare sproporzionato un tale rimedio, nonostante la diffusività, rispetto, ad esempio, alla diffamazione tramite Facebook.

Tema interessante è quello del *locus commissi delicti*: qual è il luogo di consumazione del reato in caso di diffamazione *online*? Ciò vale per tutti i reati informatici, per i quali bisogna chiedersi quale sia il luogo in cui si perfeziona la fattispecie – se il luogo in cui il contenuto è caricato in rete ovvero il luogo in cui si ha la percezione dello stesso. Partiamo dal presupposto che il reato di diffamazione si consuma nel momento della percezione del contenuto lesivo della reputazione altrui da parte di terzi, per cui rientra pacificamente tra i reati di evento. Sono, dunque, ipotizzabili due distinti momenti: da un lato, quello dell'immissione del contenuto sul web, dall'altro, quello della percezione dello stesso da parte di terzi. È pacificamente configurabile l'ipotesi del tentativo: si pensi al caso in cui il diffamatore scriva il messaggio ma questo non venga caricato correttamente per mancanza di rete o altre motivazioni. È anche configurabile il reato impossibile, quando l'azione risulti in concreto inidonea a produrre i suoi effetti in quanto, ad esempio, l'agente fa uso di uno strumento difettoso, che solo in modo apparente gli consente l'accesso ad uno spazio web, mentre in realtà il suo messaggio non è stato mai caricato in rete²⁶⁷.

²⁶⁴ Elaborazione dell'Osservatorio per la giustizia civile di Milano nell'anno 2018.

²⁶⁵ Per completezza, l'Osservatorio di Milano ha stimato che l'importo medio matematico liquidato tra i casi analizzati sia pari a €26.290.

²⁶⁶ Attualmente prospettato intorno a €40.000.

²⁶⁷ Cass. Pen., sez. V, 17/11/2000, n. 4741, disponibile su *dejure.it*; nota a sentenza di E. PERUSIA, "Giurisdizione italiana anche per le offese on line su un sito straniero", su *Cassazione Penale*, fasc. 6, 2001, pag. 1835.

Ne deriva che la giurisdizione appartiene al giudice italiano, ai sensi della c.d. teoria dell'ubiquità, sia che la condotta sia posta in essere nel territorio nazionale, sia che sia solo stata percepita da terzi nel territorio italiano²⁶⁸.

Il giudice territorialmente competente per i reati informatici è, invece, frutto di una presunzione: si ritiene che la percezione del contenuto lesivo si abbia nel luogo di residenza, domicilio o dimora della persona offesa, ossia il luogo dove il soggetto vive e, in quanto tale, in cui svolge la sua personalità. È un criterio elaborato dai Giudici di legittimità, per evitare di rendere indefinito il luogo in cui è sorta l'obbligazione ovvero il luogo in cui il danno si è verificato. Non sostenibile appare, invece, la tesi di chi individua tale luogo in quello presso cui il contenuto sia stato caricato sulla rete, *in primis*, perché il soggetto agente ben potrebbe essere in movimento durante il caricamento, e poi perché i *server* dell'ISP potrebbero essere locati in qualsiasi luogo, rendendo così quasi impossibile per la vittima risalire al *server* su cui sia stata caricata la notizia. Non è plausibile nemmeno la tesi di chi sostiene che la lesione del diritto si possa verificare in tutti i luoghi in cui avviene la diffusione della notizia, poiché in tal modo si andrebbe ad incidere sulla situazione processuale dell'attore, per cui sarebbe impossibile dimostrare, per il risarcimento del danno, che il luogo da lui indicato sia quello della prima visita.

Passiamo ad esaminare la posizione di garanzia *online*.

Nel caso in cui vi sia una fonte di rischio che trovi la causa in un rapporto qualificato tra un soggetto e l'attività da questi esercitata, l'attribuzione di una posizione di garanzia è funzionale a tutelare l'interesse previsto dall'ordinamento.

A fronte del recente incremento dei *cybercrimes*, tra cui rientra la diffamazione *online* appena esaminata, ci si chiede quale possa essere il soggetto cui viene affidata la posizione di garanzia e l'obbligo giuridico di attivarsi per prevenire la commissione di reati *online*.

È diffusa la consapevolezza della necessità di un controllo *online*, eppure è nota la difficoltà dello stesso per l'intrinseca natura del mezzo utilizzato.

Si pensa, comunemente, che il legislatore, piuttosto che prevedere meccanismi di controllo preventivo non percorribili e che potrebbero porsi in contrasto con la natura libertaria della rete, dovrebbe valorizzare modelli di *compliance* e controllo successivo. D'altro canto, è pur vero che l'esigenza comunque sentita di prevenire i reati mette in dubbio questo orientamento.

Ultimamente, è stato il legislatore europeo a riconoscere un obbligo di attivazione in capo ai soggetti che hanno la possibilità di agire sui contenuti *online*, ossia gli *Internet Service Provider* (ISP) che, come noto, rappresentano i principali intermediari dell'offerta digitale²⁶⁹. La Direttiva sul commercio elettronico (2000/31/CE), confluita

²⁶⁸ Cass. Pen., sez. V, 27/12/2000, n. 4741, cit.

²⁶⁹ L'OSCE ha definito gli ISP degli intermediari che danno accesso agli utenti, ospitano, trasmettono, e indicizzano contenuti originati dai *content provider* o forniscono servizi basati su internet a terze parti, *cfr.* G. E. VIGEVANI, O. POLLICINO, C. MELZI D'ERIL, M. CUNIBERTI, M. BASSINI, "Diritto dell'informazione e dei media", G. Giappichelli Editore, Torino, 2019, p. 336.

poi nel Codice del commercio elettronico (D.Lgs. 70/2003), ha introdotto gli artt. 14 ss., che consentono di configurare a carico degli ISP un obbligo di attivarsi qualora venissero a conoscenza della trasmissione di un contenuto illecito. Gli ISP si configurano, dunque, come veri e propri tutori dell'ordine virtuale, collaborando nella attenuazione ovvero eliminazione delle conseguenze dei contenuti illeciti, senza però avere alcun obbligo di verifica preventiva intervenendo esclusivamente *ex post*.

Resta ferma la possibile responsabilità per concorso attivo nel reato commesso dall'utente. Tale sistema di responsabilità indiretta in capo ai *provider* è stato, in parte, modificato dalla c.d. Direttiva *Copyright* (2019/790/UE) che, con riguardo ai contenuti protetti dal diritto d'autore, prevede che gli ISP debbano, in via preventiva, ottenere una licenza per caricare i contenuti, anche qualora condivisi dai propri utenti, costituendo, di fatto, una forma di controllo anche *ex ante* in capo agli ISP, e presupponendo un comportamento attivo degli stessi.

Se questo obbligo di controllo preventivo in capo agli ISP fosse applicato ai contenuti diffamatori o d'odio, ciò sarebbe funzionale alla prevenzione della lesione esaminata fino ad ora. Tuttavia, la disciplina di cui sopra è applicabile unicamente alle violazioni in materia di Diritto d'Autore. Ai sensi dell'articolo 15, comma 1, della Direttiva *e-commerce*, infatti, è vietato agli Stati membri di imporre un obbligo generale di sorveglianza o di ricerca attiva tra i contenuti veicolati dagli ISP²⁷⁰.

Per cui, chi subisce una lesione del proprio onore e della propria reputazione in internet, ha la facoltà di chiedere la disabilitazione all'accesso dei singoli contenuti diffamatori, ma non ne può chiedere una disabilitazione preventiva o generalizzata indipendente dalla sua richiesta.

Nel 2018, però, la Corte di Giustizia è intervenuta con una sentenza rivoluzionaria in materia²⁷¹, perché, pur ribadendo quanto disposto dall'art. 15, ha riconosciuto la possibilità di intimare agli ISP di bloccare l'accesso alle informazioni di contenuto identico ed equivalente²⁷², anche qualora condivisi da utenti terzi.

²⁷⁰ Cfr. sul punto: Sabam c. Netlog, C-360/10; Scarlet Extended c. SABAM, C-70/10.

²⁷¹ La causa C-18/18 ha ad oggetto la domanda di pronuncia pregiudiziale proposta alla CGUE dalla Corte suprema austriaca nel procedimento *Eva Glawischnig Piesczek v. Facebook Ireland*.

Il caso trae origine da un commento diffamatorio ad opera di un utente della piattaforma, che ha accompagnato la condivisione di un articolo di un quotidiano austriaco con un commento lesivo dell'onore e della reputazione della ricorrente.

Le domande proposte sono state tre:

I) Se l'articolo 15, co. 1 della direttiva 2000/31/CE consenta di imporre ad un *hosting provider* di eliminare non soltanto il contenuto dichiarato illecito, ma anche contenuti identici, anche qualora pubblicati da altri utenti e a livello mondiale;

II) In caso di risposta negativa al primo quesito, valga anche per i contenuti equivalenti;

III) Se valga per i contenuti equivalenti, non appena il gestore sia venuto a conoscenza di tale circostanza.

²⁷² Punto 39 della sentenza: “Dalle indicazioni contenute nella decisione di rinvio risulta che, con i termini «informazioni di contenuto equivalente», il giudice del rinvio intende riferirsi a informazioni che veicolano un messaggio il cui contenuto rimane, in sostanza, invariato e quindi diverge molto poco da quello che ha dato luogo all'accertamento d'illiceità”.

Tale riconoscimento deriva dall'applicazione del combinato disposto dell'art. 18 della medesima Direttiva e del Considerando 47, poiché il primo consente di intimare ai *provider* di tenere un comportamento *attivo*, teso a porre fine alle violazioni e a impedire ulteriori danni agli interessi in causa; mentre il secondo, nel rispetto del divieto di sorveglianza generale, ammette una tale possibilità unicamente con riguardo a casi specifici e ben determinati in sede di richiesta del provvedimento²⁷³.

Secondo quest'ottica, l'ingiunzione dovrebbe individuare sia il nome della persona interessata dalla violazione accertata, sia le circostanze in cui è stata accertata tale violazione, nonché un contenuto equivalente a quello dichiarato illecito.

Le differenze nella formulazione di tale contenuto equivalente, rispetto al contenuto dichiarato illecito, non dovrebbero, ad ogni modo, essere tali da costringere il prestatore di servizi di *hosting* interessato ad effettuare una valutazione autonoma di tale contenuto, così che siano bilanciati l'interesse dell'offeso a non veder leso il suo onore, anche *pro futuro*, e la fattibilità tecnica²⁷⁴ della misura inibitoria a carico degli *Internet Service Provider*.

Seguendo quanto tracciato dalla giurisprudenza europea, si potrebbe pensare a strumenti di intelligenza artificiale in grado di discernere i contenuti caricati nelle piattaforme per ottimizzare le procedure di controllo e l'analisi dei contenuti, approccio non del tutto sconosciuto alle piattaforme di grandi dimensioni che si servono già di elementi del genere (ma in via riparativa).

Potrebbe allora essere ripensato l'uso dei sistemi automatizzati in funzione garantista dei contenuti veicolati, ma un tale approccio dovrebbe essere ponderato, sia per quanto riguarda il punto di vista etico che dal punto di vista della responsabilità e, in ultima analisi, anche dal punto di vista di un eventuale controllo umano sulle decisioni della macchina.

Più di recente, la Commissione europea ha elaborato una proposta di regolamento sui servizi digitali, il c.d. *Digital Services Act* (DSA), che si basa sui principi già affermati dalla Direttiva sul commercio elettronico, e tuttavia mira ad assicurare le condizioni migliori per la prestazione dei servizi digitali innovativi nel mercato interno. La proposta vuole contribuire alla sicurezza *online* e alla protezione dei diritti fondamentali, nonché creare una struttura di *governance* solida e duratura per una vigilanza efficace sui prestatori di servizi intermediari.

La proposta di regolamento mantiene il sistema di esonero da responsabilità per i *provider* che non svolgano un ruolo attivo nella trasmissione dei contenuti, tuttavia ne modifica le condizioni, rendendole più rigide per i c.d. *hosting provider*.

Si impongono, infatti, obblighi di comunicazione ed informazione più chiari e trasparenti; obblighi di moderazione dei contenuti e di azioni disincentivanti alla pubblicazione di contenuti illeciti; si introduce la possibilità di impugnare le decisioni; si istituisce un sistema interno di gestione dei reclami ed inoltre la proposta delinea degli speciali obblighi per le piattaforme di grandi dimensioni, soprattutto per quanto

²⁷³ Con riguardo ai tempi, alle circostanze e al contenuto da bloccare o rimuovere.

²⁷⁴ In forma prettamente automatizzata, emblematica sul punto è la sentenza C 324/09, *L'Oreal v. eBay*.

concerne i rischi sistemici. Rimane fermo il divieto di obbligo di controllo o di accertamento attivo, ma tale divieto deve essere rispettato seguendo i principi esaminati e, purché non si pongano a carico degli ISP oneri sproporzionati, si lascerebbe impregiudicata la possibilità, da parte delle autorità nazionali, di ordinare che vengano contrastati determinati contenuti illegali specifici o di fornire informazioni specifiche. Dunque, il legislatore europeo continua ad essere garante della libertà della rete e della libertà di opinione, operando però un bilanciamento con la possibilità di un intervento postumo, sottraendo le opinioni altrui ad un vaglio preventivo, con obblighi più rigidi di trasparenza e informazione.

Per quanto concerne le singole *policies* adottate, si osserva che *social network* come Facebook, Instagram, Twitter stabiliscono linee guida per i propri utenti. Il discorso è legato anche al fenomeno dell'*hate speech*: le piattaforme *social*, nel condannare comportamenti come la lesione dell'onore e della reputazione, il *cyberbullismo*, ecc., stabiliscono un sistema di segnalazione interno che valuta il contenuto ed eventualmente lo rimuove.

I contenuti, inoltre, quando violino le norme della *community*, possono essere moderati, retrocessi (deindicizzati), oppure può essere disabilitato l'accesso agli stessi. Nei casi più gravi, le piattaforme possono anche inibire l'utilizzo del *social* per un periodo di tempo, oscurando il profilo oppure configurandolo come "*sola lettura*" (l'utente può effettivamente accedere al *social* ma non può in alcun modo interagire con gli altri utenti o pubblicare ulteriori contenuti).

Twitter, in particolare, oltre ad attuare quanto appena detto, prevede la possibilità di etichettare il contenuto e renderlo visibile solo a chi lo desidera, avvertendo che dietro l'avviso si cela un contenuto che potrebbe includere informazioni errate o fuorvianti; ciò nei soli casi di covid-19, integrità civica e contenuti artificiosi e manipolati. Potrebbe accadere lo stesso anche nel caso di *tweet* in cui la piattaforma riscontri un interesse pubblico: si possono adottare accortezze che limitano la visibilità sul *social*. Ancora, in caso di messaggi offensivi via conversazione diretta, lo stesso *social* può porre fine alla conversazione a seguito di segnalazione da parte dell'offeso.

Facebook è la piattaforma più visitata *online*: vanta al 2020 il 77,5% del traffico totale rispetto alle altre piattaforme *online* in Europa, e oltre ad un sistema automatizzato di analisi dei contenuti segnalati, ha istituito dal 2020 un *Oversight Board* chiamato a giudicare la sorte dei contenuti contrari alle linee guida della *community*.

Il comitato è stato soprannominato una Corte Suprema della libertà di parola digitale, è composto da venti membri scelti e chiamati a pronunciarsi su alcuni casi controversi, casi che sono stati considerati confliggenti con gli standard del *social* e a cui l'autore si è opposto. Il *Board* deve effettuare una sintesi tra i diritti fondamentali e le regole private del *social*, operando una valutazione anche di contesto che sfugge ai sistemi automatizzati. Lo stesso *social network* sarà poi vincolato a tali decisioni.

La decisione di affidare ad un comitato le scelte in merito ai contenuti più controversi, secondo alcuni è da condividere e apprezzare, perché intesa come garanzia aggiuntiva di moderazione nelle scelte di oscuramento o rimozione dei contenuti.

Secondo altri, invece, il comitato – composto da venti tra uomini e donne bianchi e occidentali – non potrebbe divenire fonte di uguaglianza, perché dimostrerebbe, nelle decisioni prese, il contesto culturale di provenienza.

A ciò si aggiunga che gli standard sono univocamente decisi da Facebook, che “spaccia” per assoluti i parametri della piattaforma in un mondo culturalmente e socialmente variegato. È pur vero che, sottoscrivendo i termini e le condizioni d’uso del *social*, si accettano dichiaratamente le regole ivi decise. In conclusione, sicuramente si può dubitare che possano esistere delle linee guida che soddisfino tutti, in qualsiasi parte del mondo, ma si potrebbe pure dubitare che per favorire la libertà nella rete e garantire la libertà d’espressione, il parametro sia quello individuato dagli operatori del sistema.

Capitolo XVII

L'interoperabilità: il dialogo necessario tra il digitale e il diritto

Il termine “*interoperabilità*” esprime il concetto moderno, oggi sempre più applicato a molteplici settori, di permettere, mediante procedure tecniche unificanti e standardizzate, l'interscambio di dati e l'interazione dei sistemi nei campi dell'informatica, delle comunicazioni, della sanità, dell'istruzione, dei trasporti ferroviari ed aerei e dei sistemi di sicurezza di un Paese.

Più precisamente, il Codice dell'amministrazione digitale (D.Lgs. n. 82/2015, in prosieguo “CAD”) definisce l'interoperabilità come la “*caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi*”²⁷⁵. Questa definizione deve essere associata a quella di cooperazione applicativa, definita nel CAD come “*la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informativi dei soggetti partecipanti, per garantire l'integrazione dei metadati, delle informazioni, dei processi e procedimenti amministrativi*”²⁷⁶.

In breve, la combinazione e l'applicazione dei due principi consente lo scambio dati tra PPAA e i soggetti interessati in modo standard, al fine di consentire lo svolgimento di procedimenti amministrativi complessi, ovvero che coinvolgono più amministrazioni, ovvero, ancora, più banche dati anche esterne alla Pubblica Amministrazione.

Sempre il CAD, in più punti, ribadisce il principio in forza del quale le pubbliche amministrazioni sono tenute a gestire i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione (c.d. ICT). Lo specifico procedimento, dunque, deve fornire opportuni servizi di interoperabilità o integrazione/cooperazione a carico dell'amministrazione²⁷⁷. Tali servizi devono risultare conformi alle Linee Guida elaborate dall'AgID²⁷⁸ (Autorità per l'Italia Digitale).

²⁷⁵ Art. 1, comma 1, lett. dd) D. Lgs. n. 82/2015.

²⁷⁶ Art. 1, comma 1, lett. ee) D. Lgs. n. 82/2015.

²⁷⁷ G. MANCA, “*Interoperabilità nella pubblica amministrazione: presente e futuro digitale*”, in www.agendadigitale.eu, 6 settembre 2018.

²⁷⁸ L'art. 71 del CAD dispone che “*1. L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice. Le Linee guida divengono efficaci dopo la loro pubblicazione nell'apposita area del sito Internet istituzionale dell'AgID e di essa ne è data notizia nella Gazzetta Ufficiale della Repubblica italiana. Le Linee guida sono aggiornate o modificate con la procedura di cui al primo periodo.*

1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal

L'art. 71 del Codice dell'Amministrazione Digitale, norma primaria, richiede che le Linee Guida dell'Agid debbano essere adottate su parere positivo rilasciato dal Garante per la Privacy. I punti che rilevano sono:

- 1) nello scambio di dati tra PA chi deve considerarsi titolare del trattamento?;
- 2) che tempo di durata deve avere la conservazione dei dati nell'attività di *caching*?;
- 3) chi è il responsabile del trattamento dei dati a cui il privato può rivolgersi per eventuali osservazioni o richieste di chiarimento?;
- 4) vi è una modulazione dei sistemi di sicurezza in relazione al grado di riservatezza dei dati, ad esempio quelli giudiziari?;
- 5) il principio di *privacy by design and by default* riguarda solo la fase di conservazione o anche la fase di gestione dei dati?

Per cogliere gli aspetti problematici del rapporto tra interoperabilità e tutela dei dati personali, occorre chiarire il concetto di interoperabilità, strettamente connesso a quello di cooperazione applicativa. Le pubbliche amministrazioni, infatti, possono dialogare in via digitale non solo con i tradizionali mezzi di trasmissione telematica, ossia la posta elettronica e la posta elettronica certificata, ma anche tramite la cooperazione applicativa.

La cooperazione applicativa, ai sensi del CAD, è quella parte del sistema pubblico di connettività (di seguito anche "SPC") finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni al fine di garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea".

Mentre, l'art. 72 del CAD – abrogato dal D.Lgs. 179/2016 – forniva le definizioni di "d) *"interoperabilità evoluta": i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;* e) *"cooperazione applicativa": la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi"*.

L'art. 72, abrogato, recitava espressamente: "1. Ai fini del presente decreto si intende per:

- a) *"trasporto di dati": i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;*
- b) *"interoperabilità di base": i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;*
- c) *"connettività": l'insieme dei servizi di trasporto di dati e di interoperabilità di base;*
- d) *"interoperabilità evoluta": i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;*
- e) *"cooperazione applicativa": la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi."*

Il sistema pubblico di connettività²⁷⁹ costituisce l'infrastruttura telematica abilitante della pubblica amministrazione, definita anche la c.d. «*autostrada del sole digitale*»²⁸⁰; è l'insieme di infrastrutture tecnologiche e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati dell'amministrazione pubblica, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici²⁸¹ e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna amministrazione²⁸². È il concetto della c.d. «*infrastruttura immateriale*» alla base dell'economia della conoscenza dei dati.

L'art. 73 del Codice dell'Amministrazione Digitale, riguardo al Sistema Pubblico di Connettività, afferma che «*1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione, e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente Capo definisce e disciplina il Sistema pubblico di connettività e cooperazione (SPC), quale insieme di infrastrutture tecnologiche e di regole tecniche che assicura l'interoperabilità tra i sistemi informativi delle pubbliche amministrazioni, permette il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea ed è aperto all'adesione da parte dei gestori di servizi pubblici e dei soggetti privati.*

2. Il SPC garantisce la sicurezza e la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascun soggetto aderente.

3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:

a) sviluppo architeturale e organizzativo atto a garantire la federabilità dei sistemi; b) economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa; b-bis) aggiornamento continuo del sistema e aderenza alle migliori pratiche internazionali; c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.

²⁷⁹ Il Sistema Pubblico di Connettività e Cooperazione, istituito con D.Lgs. 28 febbraio 2005, n. 42 quale evoluzione della RUPA (Rete Unitaria della Pubblica Amministrazione), è confluito grazie al D.Lgs. 159/2006 (che ha abrogato il D.Lgs. 42/2005) negli artt. 72 ss. del D.Lgs. 82/2005, modificato dal D.lgs. 179/2016, poi dal correttivo D.lgs. 217/17. Operativo dal 2007, un quadro consolidato si è avuto con il d.p.c.m. 1° aprile 2008, recante regole tecniche e di sicurezza per il suo funzionamento.

²⁸⁰ L. AMADEI, «*Il codice dell'amministrazione digitale*», in L. DE PIETRO (a cura di), «*Dieci lezioni per capire e attuare l'e-government*», definisce l'SPC una sorta di «*framework*» nazionale di interoperabilità. Per M. IASELLI, «*La raccomandata on line: disciplina normativa ed aspetti operativi*», in *Diritto dell'Internet*, n. 6, 2006, l'SPC costituisce «*l'asse portante per l'applicazione del codice dell'amministrazione digitale*».

²⁸¹ L'art. 72 del D.Lgs. 82/2005 abrogato forniva una serie di definizioni relative al sistema pubblico di connettività. In particolare, oltre alla cooperazione applicativa (lett. e), l'interoperabilità evoluta (lett. d).

²⁸² Art. 73, co. 2, D.Lgs. 82/2005.

3-bis. [Le regole tecniche del Sistema pubblico di connettività sono dettate ai sensi dell'articolo 71.]²⁸³

3-ter. Il SPC è costituito da un insieme di elementi che comprendono:

a) infrastrutture, architetture e interfacce tecnologiche; b) linee guida e regole per la cooperazione e l'interoperabilità; c) catalogo di servizi e applicazioni.

3-quater. Ai sensi dell'articolo 71 sono dettate le regole tecniche del Sistema pubblico di connettività e cooperazione, al fine di assicurarne: l'aggiornamento rispetto alla evoluzione della tecnologia; l'aderenza alle linee guida europee in materia di interoperabilità; l'adequatezza rispetto alle esigenze delle pubbliche amministrazioni e dei suoi utenti; la più efficace e semplice adozione da parte di tutti i soggetti, pubblici e privati, il rispetto di necessari livelli di sicurezza.”.

Il SPC ha, quindi, il compito di assicurare la sicurezza e il buon esito della trasmissione dei dati, esito garantito dai fornitori del servizio, che possono svolgere questa attività solo laddove in possesso di determinati requisiti di qualità e sicurezza. Non si tratta, quindi, solo ed esclusivamente di una rete tecnologica, ma della condizione abilitante per il corretto funzionamento dell'*e-government*, dal momento che influenza fortemente le scelte organizzative ed è volta a promuovere la collaborazione tra amministrazioni, finalità quest'ultima estremamente rilevante in un sistema pubblico articolato su molte istruzioni e livelli diversi²⁸⁴.

È proprio la cooperazione applicativa ad entrare in gioco nella trasmissione e nello scambio di dati e informazioni tra amministrazioni: le comunicazioni telematiche, in tal caso, si atteggiavano in modo molto diverso rispetto alla posta elettronica e alla posta elettronica certificata che, si può dire, riproducono a livello informatico rispettivamente il meccanismo della posta ordinaria e della raccomandata. Nella cooperazione applicativa la comunicazione avviene, invece, attraverso l'interfacciamento fra le porte di dominio²⁸⁵ delle amministrazioni pubbliche, in quanto si basa sulle capacità di esportare i propri servizi applicativi e di accedere ai servizi erogati da altre amministrazioni attraverso le porte di dominio, punto di contatto telematico fra

²⁸³ Il comma 3-bis è stato abrogato dal D.Lgs. 179/2016, il quale ha modificato gran parte dell'articolo, riportando nell'art. 57, “*Modifiche all'articolo 73 del decreto legislativo n. 82 del 2005*”.

²⁸⁴ Appare la traduzione della nozione, elaborata da Sabino Cassese, di “*rete come figura organizzativa della collaborazione*”. Così, C. D'ORTA, “*Il sistema pubblico di connettività*”, in *Giornale di diritto amministrativo*, 2005, n. 7, riferendosi a S. CASSESE, “*le reti come figura organizzativa della collaborazione*”, in ID., “*Lo spazio giuridico globale*”, Roma-Bari, 2003.

²⁸⁵ La porta di dominio rappresenta un elemento concettuale che ha la funzione di *proxy* per l'accesso alle risorse applicative del dominio. Fa parte del modello organizzativo di SPCoop e, come tale, trova naturalmente posto nella progettazione concettuale piuttosto che in quella logica o fisica. La PD può essere ricoprire due ruoli: *Porta Applicativa* – Ruolo assunto da una porta di dominio di SPCoop nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la porta di dominio che, a seguito della ricezione di un messaggio di richiesta proveniente da un'altra porta di dominio (porta delegata) invia al mittente un messaggio di risposta; *Porta Delegata* – Ruolo assunto da una porta di dominio di SPCoop nell'ambito di un episodio di collaborazione applicativa. Assume tale ruolo la porta di dominio che origina un messaggio di richiesta (di servizio) destinato ad un'altra porta di dominio (porta applicativa).

amministrazioni che gestiscono i messaggi in entrata e in uscita. Le porte di dominio devono rispondere a determinati standard e regole di comunicazione definite; ciò le distingue dai domini che sono invece l'insieme di risorse software, hardware e di comunicazione di una pubblica amministrazione, da intendersi come lo spazio di competenza di ciascuna amministrazione in relazione al proprio sistema informativo e informatico, che per questo possono conservare strutture autonome, dato che la funzione di adattamento è compiuta dalle porte di dominio²⁸⁶.

Di conseguenza, la cooperazione applicativa non si limita all'aspetto tecnologico, ma implica una vera e propria riorganizzazione e reingegnerizzazione dei processi all'interno delle pubbliche amministrazioni. Segna il passaggio concreto dall'informatizzazione alla vera e propria "digitalizzazione" in senso non solo formale, ma anche sostanziale nel rispetto del principio "*once only*".

Sebbene l'importanza del meccanismo di cooperazione si colga primariamente sotto il profilo dello scambio di informazioni e delle comunicazioni che intercorrono tra soggetti pubblici, più in generale la cooperazione costituisce l'asse portante delle relazioni tra amministrazioni e, in quanto tale, dovrebbe essere favorita ed implementata al fine di garantire semplificazione, efficacia e sicurezza nell'ottica di una profonda evoluzione e modernizzazione dell'intero sistema pubblico²⁸⁷.

Il comma 2 dell'art. 73 del CAD pone in rilievo la necessità che l'SPC garantisca "sicurezza" e "riservatezza" delle informazioni: la seconda è da intendere come direttamente – sebbene non unicamente – condizionata dalla prima: è del tutto evidente, difatti, che un sistema non sicuro è potenzialmente idoneo a pregiudicare anche la riservatezza delle informazioni trasmissibili ed acquisibili per il suo tramite. Più precisamente, un sistema non sicuro potrebbe esporre al rischio di *data breach*, al verificarsi dei quali il Regolamento UE GDPR (n. 676/16) fa discendere l'obbligo di relativa comunicazione all'Autorità Garante Privacy e al ricorrere di determinati presupposti, anche agli interessati cui i dati si riferiscono, in entrambi i casi entro tempi assai ristretti. Senza trascurare l'evenienza di possibili richieste risarcitorie. Gli standard di sicurezza prescritti per l'SPC sono stati stabiliti, secondo quanto disposto dal comma 3-quater, dall'AgID, attraverso lo strumento delle Linee Guida di cui all'art. 71 del CAD²⁸⁸.

²⁸⁶ In tal senso F. MARTINI, "Il sistema informativo pubblico", in "Quaderni del Dipartimento Pubblico", Università di Pisa, Torino, 2006.

²⁸⁷ Come rileva F. MARTINI, op. cit., la cooperazione applicativa prospetta di dissolvere i confini di competenza fra amministrazione permettendo ad un'amministrazione di accedere con pieno valore giuridico ai servizi di un'altra. I concetti di interoperabilità e cooperazione applicativa sono considerati fattori chiave e ricevono impulso dalla normativa e dalle politiche dell'Unione europea, anche dall'attuale Agenda Digitale europea. Su interoperabilità e cooperazione applicativa cfr. B. DA RONCH – L. DE PIETRO, "Interoperabilità e cooperazione applicativa", in L. DE PIETRO (a cura di), "Dieci lezioni per capire e attuare l'e-government", cit. Sulla cooperazione applicativa e i suoi modelli, cfr. A. MAGGIPINTO.

²⁸⁸ Proprio il 1° gennaio 2022 sono entrate in vigore le Linee guida dell'AgID sulla formazione, gestione e conservazione dei documenti informatici – come disposto dalla proroga inserita nella

Tale aspetto viene ribadito anche dal Consiglio di Stato²⁸⁹ che, con riferimento all'art. 73, precisa che il SPC (Sistema Pubblico di Connettività) deve garantire la sicurezza e la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascun soggetto aderente secondo le regole tecniche di cui all'art.71 del CAD.

Con essa ed i relativi allegati, l'AgID ha definito la Linea di indirizzo sull'interoperabilità tecnica che tutte le Pubbliche Amministrazioni devono adottare al fine di garantire l'interoperabilità dei propri sistemi con quelli di altri soggetti e favorire l'implementazione complessiva del Sistema informativo della PA. In

determinazione n. 371/2021 del 17 maggio 2021 – che segneranno il salto quantico evolutivo dalla informatizzazione alla vera e propria digitalizzazione e porteranno l'azione amministrativa ad un altro livello digitale. Finalmente si attua, dunque, il processo di trasformazione digitale delineato nel CAD e nel TUDA (DPR 445/2000) che si attendeva da tempo. Erano state, infatti, già pubblicate con la determinazione n. 407/2020 del 9 settembre 2020, ma è stato dopo la correzione avvenuta con la determinazione del 17 maggio 2021 che sono iniziati i lavori finali per portare a compimento il documento: il gruppo di lavoro coordinato da AgID e costituito da Agenzia delle Entrate, Consiglio Nazionale dei dottori commercialisti, Assosoftware, ANORC e Assoconservatori – con il supporto del Politecnico di Milano e di Sogei – ha concluso i lavori a dicembre 2021. Inoltre, con la determinazione n. 629/2021 l'AgID ha modificato il Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici relativo alla fornitura del servizio in favore delle PA, adottato con la determinazione n. 455/2021. La nuova disciplina abroga, con delle eccezioni espresse, le regole tecniche precedentemente in vigore. Le Linee guida sono fondamentali per garantire il passaggio dall'informatizzazione, che costituisce la “mera” riproduzione sul supporto informatico, alla vera e propria digitalizzazione, che è la nascita del documento digitale, con tutte le regole tecniche necessarie per la forma scritta digitale, per la corretta fascicolazione informatica. Nonostante il lavoro sia stato portato a termine correttamente, Mariella Guercio, in un intervento del 29 dicembre 2021 nel Gruppo Facebook “*Italian Digital Minions*”, ha sostenuto che la parte relativa ai metadati contiene una «*somma di informazioni obbligatorie prive di contesto temporale e di finalità esplicite (non è chiaro chi, quando, come debba acquisire queste informazioni e gestirle sia all'interno del sistema documentale sia nelle successive – sottolineo successive – fasi di conservazione*». È stato osservato che l'ambito della metadattazione andrebbe riportata nell'alveo originario della gestione documentale e non della formazione del documento, «*infatti, se per una pubblica amministrazione l'utilizzo dei metadati resta assolutamente indispensabile per gestire le operazioni di registrazione e di segnature, quindi di classificazione (e di corretta formazione dell'archivio digitale), in ambito privato, al contrario, non vi è alcun obbligo di gestione documentale e l'utilizzo dei metadati, specie nell'attuale configurazione, rischia di rimanere solo un inutile e pericoloso esercizio di stile*», v. A. LISI, “*Come sarà il 2022 dei documenti informatici: nuove regole digitali e qualche polemica*”, su agendadigitale.eu. Le nuove Linee guida, comunque, garantiscono un buon collegamento con il sistema delineato dal GDPR, soprattutto per quanto riguarda il ruolo dei conservatori dei documenti informatici. Infine, la legge n. 108 del 2021, che modifica il CAD, all'art. 18-bis prevede in capo all'AgID poteri di vigilanza, verifica, controllo e monitoraggio simili a quelli dell'Anac, nell'esercizio dei quali l'Agenzia richiede e acquisisce presso tutti i soggetti pubblici, dati, documenti e altre informazioni strumentali e necessarie. Se non si ottempera alla richiesta di dati, documenti o informazioni, ovvero si trasmettono dati o informazioni parziali o non veritieri, si incorre in sanzioni amministrative pecuniarie nel minimo di euro 10.000 e nel massimo di euro 100.000.

²⁸⁹ Vedasi *parere n. 785 del 23 marzo 2016*. Più di recente, si segnala il parere del CdS del 26 novembre 2020, n. 1940 sull'*e-procurement*.

particolare, circolare ed allegati si occupano di individuare le tecnologie e gli standard che le PPAA devono tenere in considerazione nella realizzazione dei propri sistemi informatici, al fine di permettere il coordinamento informatico dei dati tra le amministrazioni nonché tra i gestori di servizi pubblici e i soggetti privati e l'Unione Europea.

L'Agenzia per l'Italia Digitale è, del resto, l'autorità responsabile delle attività di *governance* con l'obiettivo di definire, condividere e assicurare l'aggiornamento continuo dei seguenti aspetti:

- l'insieme delle tecnologie che abilitano l'interoperabilità tra PA, cittadini e imprese;
- i *pattern* di interoperabilità (interazione e sicurezza);
- i profili di interoperabilità.

Tutte le amministrazioni devono, dunque, aderire agli standard tecnologici ed utilizzare *pattern* e profili del nuovo Modello di interoperabilità, che consentirà di definire ed esporre *Application Programming Interface* (c.d. API) conformi agli standard consolidati anche in ambito EU. Le API realizzate in conformità con il nuovo Modello di Interoperabilità garantiscono in particolare:

- tracciabilità delle diverse versioni delle API, allo scopo di consentire evoluzioni non distruttive (*versioning*);
- documentazione coordinata con la versione delle API (*documentation*);
- limitazioni di utilizzo collegate alle caratteristiche delle API stesse e della classe di utilizzatori (*throttling*);
- tracciabilità delle richieste ricevute e del loro esito (*logging* e *accounting*);
- un adeguato livello di servizio in base alla tipologia del servizio fornito (SLA);
- configurazione scalabile delle risorse.

Il nuovo Modello di interoperabilità rappresenta un asse portante del Piano triennale per l'informatica nella PA 2020-2022. Come stabilito nel Piano, l'Agenzia per l'Italia Digitale:

- fornisce un catalogo delle API e dei servizi disponibili con una interfaccia di accesso unica;
- rende disponibili appositi strumenti di cooperazione per agevolare la risoluzione di problematiche relative alle API;
- stabilisce e pubblica le metriche di utilizzo delle API.

La Circolare n. 1 del 9 settembre 2020 aggiorna, altresì, il Sistema pubblico di cooperazione (SPCoop) proseguendo nel processo di aggiornamento avviato con la determinazione AgID 219/2017.

La messa in opera delle regole di interoperabilità, di integrazione e cooperazione per lo scambio di informazioni e l'erogazione di servizi nella PA è un percorso che parte da lontano, ma presenta ancora molte criticità.

Il tema dell'interoperabilità per lo scambio di informazioni e l'erogazione di servizi nella Pubblica Amministrazione rappresenta, infatti, un tema tra i più importanti per lo sviluppo del digitale nella PA insieme alla gestione dell'identità digitale anche in chiave anagrafica e di sicurezza dei dati e dei sistemi.

Non è un caso che nell'ultima versione del “*Recovery Plan*” si citi, tra gli obiettivi di “*digitalizzazione, innovazione, competitività e cultura*”, l'implementazione dell'interoperabilità nella Pubblica Amministrazione, con uno sguardo costante ai dati personali²⁹⁰.

Non solo. Nel decreto cd. Semplificazioni²⁹¹, gli artt. 24 e 25 prevedono una valorizzazione dei sistemi di identificazione digitale Spid e Cie per l'accesso ai servizi *on line*, rafforzando il concetto di identità digitale anche attraverso il “*punto di accesso telematico previsto dall'art. 64-bis*”, ossia l'applicazione per *smartphone* IO, la piattaforma unica per tutte le Pubbliche amministrazioni integrata con le piattaforme abilitanti come pagoPA, Spid e Cie. Allo stesso modo, l'art. 26 prevede una piattaforma unica per la notificazione digitale degli atti della Pubblica Amministrazione, e il comma 15 dell'art. 26 prevede un'articolata procedura da adottarsi con uno o più DPCM, sentito il Ministero dell'Economia e il Garante per la Privacy, nel termine ordinatorio di 120 giorni dalla data di entrata in vigore del decreto con cui vengano stabilite le regole tecniche, l'infrastruttura tecnologia e le modalità di inserimento degli atti, nonché il piano test per la verifica del corretto funzionamento. Ultimato il test, con atto del Capo della competente struttura presso la Presidenza del Consiglio dei Ministri “*è fissato il termine a decorrere dal quale le amministrazioni possono aderire alla piattaforma*”. Anche per l'elenco dei domicili digitali il comma 3-bis dell'art. 3-bis prevede che sia un DPCM, sentito Agid, il Garante per la Privacy e la Conferenza unificata, a fissare la data in cui le comunicazioni tra i soggetti non digitale e la PA avvenga “*esclusivamente in forma elettronica*”, mettendosi a disposizione di tali

²⁹⁰ Per uno studio più approfondito, si consiglia di consultare il Piano Nazionale di Ripresa e Resilienza (PNRR) 2021, da pag. 119 a 129, che, in tema di dati e interoperabilità, si esprime nei seguenti termini: “*Il gap digitale della PA italiana si traduce oggi in ridotta produttività e spesso in un peso non sopportabile per cittadini, residenti e imprese, che debbono accedere alle diverse amministrazioni come silos verticali, non interconnessi tra loro. La trasformazione digitale della PA si prefigge quindi di cambiare l'architettura e le modalità di interconnessione tra le basi dati delle amministrazioni affinché l'accesso ai servizi sia trasversalmente e universalmente basato sul principio “once only”, facendo sì che le informazioni sui cittadini siano a disposizione “una volta per tutte” per le amministrazioni in modo immediato, semplice ed efficace, alleggerendo tempi e costi legati alle richieste di informazioni oggi frammentate tra molteplici enti. Investire sulla piena interoperabilità dei dataset della PA significa introdurre un esteso utilizzo del domicilio digitale (scelto liberamente dai cittadini) e garantire un'esposizione automatica dei dati/attributi di cittadini/residenti e imprese da parte dei database sorgente (dati/attributi costantemente aggiornati nel tempo) a beneficio di ogni processo/servizio “richiedente”. Si verrà a creare una “Piattaforma Nazionale Dati” che offrirà alle amministrazioni un catalogo centrale di “connettori automatici” (le cosiddette “API” – Application Programming Interface) consultabili e accessibili tramite un servizio dedicato, in un contesto integralmente conforme alle leggi europee sulla privacy, evitando così al cittadino di dover fornire più volte la stessa informazione a diverse amministrazioni. La realizzazione della Piattaforma Nazionale Dati sarà accompagnata da un progetto finalizzato a garantire la piena partecipazione dell'Italia all'iniziativa Europea del Single Digital Gateway, che consentirà l'armonizzazione tra tutti gli Stati Membri e la completa digitalizzazione di un insieme di procedure/servizi di particolare rilevanza (ad es. richiesta del certificato di nascita, ecc.)”.*

²⁹¹ D.L. n. 76 del 16 luglio 2020, convertito in legge n. 120/20.

soggetti un domicilio digitale o altre modalità per superare il *Digital divide*. Occorre precisare che più recentemente il Ministro per l'Innovazione tecnologica e la transizione digitale Colao ha annunciato il progetto di realizzazione di una Rete Unica Digitale entro il 2026 con la necessità di un'unificazione dello Spid con la carta di identità elettronica. La tutela dei dati personali verrà a realizzarsi, anche in questo caso, con il rispetto delle procedure standardizzate contenute nelle Linee Guida Agid da aggiornarsi con l'evoluzione continua dei protocolli informatici grazie anche all'apporto tecnico di un apposito Dipartimento, il Dipartimento per la trasformazione digitale, struttura di supporto al Ministro per l'innovazione e la transizione digitale per la promozione il coordinamento delle azioni Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale e di modernizzazione del Paese.

Un campo in cui la tutela dei dati personali viene messa maggiormente in discussione è quello della tecnologia *Blockchain*²⁹² che si sta applicando in vari settori dell'agire pubblico, sanitario, appalti, transazioni. Tale tecnologia si scontra con i due principi Cardini del GDPR²⁹³: i dati inseriti nelle *blockchain* sono pubblici ed accessibili da chiunque partecipi alla catena e i dati presenti nelle *blockchain* sono conservati illimitatamente.

Le parole chiave del GDPR, ossia centralizzazione, limitazione e rimovibilità, si pongono in contrasto con la tecnologia *blockchain* basata su decentralizzazione, distribuzione e immutabilità. La tutela del dato personale risiede sempre in un *hash* crittografato²⁹⁴ e nella anomizzazione dei soggetti coinvolti.

I servizi di gestione dei dati e l'architettura dei dati, progettati per conservare, utilizzare, riutilizzare e organizzare i dati, sono componenti decisivi della catena del valore dell'economia digitale europea²⁹⁵. Per questo motivo, si pone l'attenzione sui costi e sulle competenze inerenti all'accesso e alla conservazione dei dati, che determinano la velocità, la profondità e la portata dell'adozione di infrastrutture e prodotti digitali, in particolare per le PMI e le *start-up*²⁹⁶.

²⁹² La *blockchain* è una particolare tecnologia di registro distribuito (DLT), in grado di registrare scambi e informazioni in modo sicuro e permanente, mediante la condivisione di un database che rimuove essenzialmente la necessità degli intermediari i quali, in precedenza, erano tenuti ad agire come terze parti di fiducia per verificare, registrare e coordinare i dati.

²⁹³ Regolamento CE del Parlamento europeo n. 679/2016 (*General Data Protection Regulation*).

²⁹⁴ Una *funzione hash crittografica* fa parte di un gruppo di funzioni *hash* adatte per applicazioni crittografiche come SSL/TLS. Come altre funzioni *hash*, le funzioni *hash* crittografiche sono algoritmi matematici unidirezionali utilizzati per mappare i dati di qualsiasi dimensione su una stringa di bit di una dimensione fissa. Le funzioni *hash* crittografiche sono ampiamente utilizzate nelle pratiche di sicurezza delle informazioni, quali firme digitali, codici di autenticazione dei messaggi e altre forme di autenticazione.

²⁹⁵ G. D'ACQUISTO, "Blockchain e GDPR: verso un approccio basato sul rischio", in *www.federalismi.it*, 18 gennaio 2021.

²⁹⁶ C. MORELLI, "Dallo spazio economico europeo allo spazio comune dei data UE", in *www.altalex.com*, 22 marzo 2021.

Negli ultimi anni, infatti, si sono sviluppati tanto gli ecosistemi tecnologici²⁹⁷ basati e sviluppati sul web, quanto, di conseguenza, i relativi problemi in ambito di sicurezza e trattamento dei dati, non solo delle aziende o dei professionisti, ma di tutti gli utenti in generale.

È chiaro che qualsiasi strumento, se usato in modo improprio, può causare danni, più o meno gravi. Spesso, quindi, non è tanto lo strumento in sé ad essere la causa del danno, bensì le modalità attraverso cui viene utilizzato, il che vale anche per gli strumenti più semplici. Tali problematiche investono naturalmente anche l'utilizzo della *Blockchain*.

Molto spesso si è inclini a collocare la *blockchain* nell'ambito dei *Bitcoin*, delle criptovalute o delle transazioni finanziarie; ma la *blockchain* può dare risposte assolutamente innovative anche sul piano della creazione di un sistema di relazioni interamente basato su un nuovo concetto di fiducia. In questo caso, occorre trovare uno strumento di disintermediazione, che permetta di dare un indirizzo di vita quotidiana per creare ecosostenibilità e benessere attraverso il digitale. Il che tradotto significa che la *blockchain* nella PA può e deve apportare dei benefici al cittadino e non la sola funzionalità²⁹⁸.

La *blockchain* di per sé è lo strumento che, se usato in modo inappropriato, può portare ad incorrere in situazioni contrarie alle normative nazionali e/o sovranazionali approvate a tutela del diritto alla riservatezza del cittadino. Il caso lampante è quello del trattamento dei dati personali²⁹⁹.

In merito all'adeguamento della *blockchain* al Regolamento UE 2016/679, lo scoglio apparentemente insormontabile è garantire i diritti dell'interessato, disciplinati al capo III, negli artt. 12-23 del Regolamento in oggetto.

In particolar modo, la peculiarità intrinseca della *blockchain* della non modificabilità e cancellazione risulta essere in forte contrasto con il più noto (per il clamore datogli post GDPR) "diritto all'oblio" sancito nell'art. 17 del GDPR.

Secondo lo studio condotto dalla "Queen Mary University" di Londra, sarebbe ipotizzabile una *blockchain compliance* al GDPR mediante la crittografia dei dati personali e la successiva eliminazione delle corrispettive chiavi decrittografiche, lasciando su *blockchain* solo i dati indecifrabili o mediante l'uso dei cosiddetti modelli di memoria "fuori catena"³⁰⁰.

Come sostiene N. Boldrini³⁰¹, infatti, le tecnologie *Blockchain* stanno rompendo molti schemi, soprattutto quelle di natura pubblica su cui si basa la circolazione delle *criptovalute bitcoin* ed *ethereum*, ed introducono nuovi paradigmi compresi quelli di natura legale. In quest'ottica, diventa interessante capire il binomio *Blockchain* e

²⁹⁷ R. D. CARDENAS ESPINOSA e altri, "Ecosistemi tecnologici per la ricerca formativa nel contesto", Ed. Sapienza, 2020.

²⁹⁸ W. NONNIS, "Blockchain, il suo contributo durante la pandemia", cit.

²⁹⁹ A. BELLO, "Blockchain e privacy: soluzioni per la compliance alle norme", cit.; M. IASELLI, "Blockchain e privacy, bisogna lavorare ancora molto", cit.

³⁰⁰ A. BELLO, "Blockchain e privacy: soluzioni per la compliance alle norme", cit.

³⁰¹ N. BOLDRINI, "Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati", cit.

GDPR, ossia come la *Blockchain* potrà supportare e rispettare le regole sulla protezione dei dati personali introdotte dal GDPR.

La tecnologia *Blockchain* consente transazioni tra le parti senza dover rivelare la propria identità direttamente. Tuttavia, ogni transazione che viene eseguita viene pubblicata e collegata a una chiave pubblica che rappresenta perciò uno pseudonimo di un determinato utente. Sebbene la chiave pubblica non contenga informazioni direttamente riconducibili all'utente, l'utilizzo della medesima chiave per diverse transazioni e l'incrocio con altre informazioni potrebbero consentire di individuare gli autori di una determinata transazione.

Ne consegue che la chiave pubblica, se associata a una persona, potrà eventualmente essere qualificata come dato personale ai fini della legislazione europea sulla protezione dei dati. Infatti, quando la chiave pubblica è ricondotta a un soggetto identificato, è possibile ottenere informazioni su tutte le transazioni che il soggetto ha compiuto sulla *blockchain*. Di conseguenza, le norme sulla protezione dei dati potrebbero essere applicabili ad almeno alcuni dei dati coinvolti nelle soluzioni *Blockchain*³⁰².

Qualora si intenda utilizzare la *blockchain* come *storage*³⁰³ di tutti i dati degli utenti, anziché, per esempio, creare una linea privata dove immagazzinare (c.d. *storare*) i dati sensibili accoppiandola ad una *blockchain* da usare in formato “notarile” è importante sapere che:

- i dati archiviati in una *blockchain* sono a prova di manomissione: questo si traduce in un'impossibilità pura (derivante da codifica della *blockchain*) di cancellazione dei dati, una volta che essi verranno immessi nella catena distribuita;
- le *Blockchain* sono distribuite, quindi nemmeno il controllo sui dati può essere centralizzato ed è demandato a tutti i partecipanti alla *blockchain*³⁰⁴;
- gli *Smart Contract* (contratti intelligenti)³⁰⁵ sono creati per essere automatizzati sotto il profilo decisionale: questo può aprire quindi criticità comprensibilmente non banali sul fronte, per esempio, di casi di impugnazioni e contestazioni.

In linea generale, ciò che si pone in contrasto con il GDPR, in questo caso, sono due dei principi che fino ad oggi hanno costituito il cardine su cui si sono affermati il valore ed il potere della *Blockchain*³⁰⁶, ossia:

- i dati inseriti nelle *blockchain* sono pubblici ed accessibili da chiunque partecipi alla catena;
- i dati presenti nelle *blockchain* sono conservati illimitatamente³⁰⁷.

³⁰² V. PORTALE, “Quanto è legale la Blockchain? La compatibilità tra Blockchain e normativa GDPR”, cit.

³⁰³ Supporto di memorizzazione dei dati.

³⁰⁴ Al più ai *miners*, che comunque non possono essere considerati dei *Data Protection Officer* come richiesto da GDPR.

³⁰⁵ Vedi *parere Consiglio di Stato del 26 novembre 2020, n. 1940* sullo Schema di regolamento recante le modalità di digitalizzazione delle procedure dei contratti pubblici (c.d. *e-procurement*).

³⁰⁶ A. GAMBINO, C. BOMPRESZI, “Blockchain e titolare del trattamento dei dati personali: il nodo rimane irrisolto”, cit.

³⁰⁷ A garanzia e tutela dell'intero registro distribuito.

Viceversa, se volessimo riassumere in breve ciò che caratterizza il GDPR potremmo utilizzare tre parole chiave: centralizzazione, limitazione e rimovibilità (cancellazione), termini che ovviamente, anche solo ad una prima lettura, si pongono in netto contrasto con i fondamenti che, al contrario, costituiscono la base della *blockchain*, ossia decentralizzazione, distribuzione ed immutabilità.

Come noto, il GDPR conferisce ai residenti nel territorio europeo una serie di diritti esecutivi in relazione al trattamento dei propri dati personali, i quali risultano sono comprensibili nel contesto di un database centralizzato controllato da un singolo controller di dati con un insieme finito di processor³⁰⁸.

Se partiamo dall'assunto che, in generale, le *Blockchain* si concentrano principalmente sulla protezione dell'identità più che sui dati ad essa associati, il parallelismo con la "Carta dei diritti digitali" delle persone appare evidente, dato che il GDPR nasce come volontà di restituire alle persone³⁰⁹ il "potere" sui propri dati personali.

In linea di principio, attraverso la *Blockchain* un utente è sempre in grado di controllare i propri dati personali, anzi, è l'unico a sapere a che informazioni corrisponde la propria chiave pubblica.

Nonostante le sfide legate principalmente a immutabilità e replicazione siano indubbiamente delicate e sarà necessario attendere le interpretazioni del legislatore europeo per avere un quadro di diritto completo, ad oggi ci sono delle possibili "vie" di prevenzione³¹⁰, ossia di applicabilità della *blockchain* in conformità a quanto stabilito dal GDPR.

Va, tuttavia, fatta un'ulteriore precisazione sulla sicurezza crittografica: «*la crittografia non libera persone ed aziende dalle proprie responsabilità sul controllo dei dati perché – per dirla senza mezzi termini – tutta la crittografia può essere violata*», avverte Rutjes³¹¹. «*Questo vale anche per gli hash crittografici che, nell'interpretazione del gruppo di lavoro di esperti tecnici dell'Unione Europea, è da considerarsi come dato personale. A mio avviso che un hash sia una stringa di codice ben progettata è sufficientemente sicura e anonima dal mettere al riparo i dati personali di chi possiede le chiavi crittografiche; tuttavia, sarà la Corte di Giustizia Europea a doversi pronunciare in merito*».

Per quanto riguarda i conflitti attorno alle caratteristiche uniche della *blockchain*, la soluzione è semplice, scrive Rutjes nel suo post: «*memorizzare i dati personali al di fuori della blockchain, ad esempio in un database privato. In generale, è buona norma limitare la quantità di informazioni condivise nel libro mastro; ancora di più con informazioni personali o comunque sensibili*».

³⁰⁸ D. MARCIANO, G. CAPACCIOLI, "La blockchain ed il problema del trattamento dei dati personali", cit.

³⁰⁹ In una *Blockchain* diremmo quindi l'identità.

³¹⁰ Come, ad esempio, la crittografia o i codici Qr, protocolli informatici che prevedano *http cache control*.

³¹¹ A. RUTJES, "Blockchain and GDPR: better safe than sorry", 2018.

L'opportunità potenziale è l'abilitazione di un futuro in cui la fornitura di servizi pubblici sia più vicina alla persona e alle imprese, creando delle condizioni di maggior sviluppo e integrazione economica e sociale.

I cosiddetti *smart contract*³¹² si candidano quali strumenti adatti a portare miglioramenti sostanziali in termini di conformità, uniformità, standardizzazione ed implementazione della catena di responsabilità.

Trattandosi di tecnologie ancora in fase di completamento del proprio ciclo di sviluppo, è fondamentale maturare degli elementi di valutazione delle diverse opzioni disponibili in quanto a paradigma di adozione, considerando gli specifici obiettivi dei relativi ambiti di applicazione.

Temi quali privacy, sicurezza, solidità e scalabilità diventano ancor più centrali e strategici quando la loro contestualizzazione avviene in ambiti di investimento pubblico; è pertanto necessario comprendere come la tecnologia sia lo strumento di implementazione di un modello che porta un effetto di trasformazione con implicazioni etiche e sociali.

In questa prospettiva va collocata l'iniziativa di creazione della *European Blockchain Service Infrastructure* (EBSI)³¹³, azione congiunta della Commissione europea e del partenariato europeo *Blockchain* (EBP) per fornire servizi pubblici transnazionali sicuri a livello dell'UE utilizzando le tecnologie *blockchain*.

Periodi di difficoltà e di incertezza, come quelli che stiamo attraversando in questi mesi, possono essere trasformati in occasioni per introdurre degli elementi di discontinuità che si candidano quali fattori decisivi per una visione programmatica di ripresa e sviluppo (naturale appare un richiamo al PNRR).

È necessario, quindi, affrontare resistenze culturali (e a volte ideologiche) che spesso ostacolano i processi di sviluppo per creare opportunità concrete di trasformazione attraverso delle progettualità di sistema volte a generare nuove prospettive di valore per cittadini e imprenditori³¹⁴.

Di recente, il Ministro per la transizione digitale ha annunciato che entro fine gennaio verrà emanato il bando di gara per il Piano Strategico Nazionale relativo alla realizzazione della rete unica digitale.

³¹² Protocolli informatici che facilitano, verificano o fanno rispettare la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale. Gli *smart contract*, di solito, hanno anche una interfaccia utente e spesso simulano la logica delle clausole contrattuali.

³¹³ Alla base dell'avvio del progetto EBSI c'è l'*European Blockchain Partnership* (promossa nel 2018), ossia un'iniziativa voluta dall'Unione europea che punta a favorire la collaborazione tra gli Stati membri per lo scambio di esperienze e di *expertise*, sia sul piano tecnico sia su quello della regolamentazione. L'Italia è entrata a far parte del partenariato il 27 settembre 2018. Secondo gli obiettivi del partenariato, lo sviluppo dell'infrastruttura permetterà di condividere in maniera sicura informazioni come, ad esempio, dati doganali e fiscali dell'Ue, documenti di audit di progetti finanziati, certificazioni transfrontaliere di diplomi e sulle qualifiche professionali e le identità digitali (eIDAS).

³¹⁴ P. GHEZZI, "Blockchain, quali prospettive per le politiche pubbliche", in www.blockchain4innovation.it, 14 aprile 2021.

La centrale di committenza per l'espletamento delle gare sarà Difesa Servizi, società *in house* del Ministero della Difesa, specializzata in acquisti ad altro contenuto tecnologico.

Ciò è emerso durante un'audizione alla Camera nell'ambito di un'indagine conoscitiva sulla digitalizzazione e interoperabilità delle banche dati fiscali, durante la quale il Ministro competente ha aggiunto che «entro la fine del 2022 prevediamo il collaudo della infrastruttura, mentre tra la fine del 2022 e il 2025, prevediamo di completare la migrazione dei dati della p.a.»³¹⁵.

Per garantire continuità in questo periodo, il Ministro ha chiarito che *Sogei*, società *in house* controllata al 100% dal MEF, potrà continuare ad erogare i servizi *cloud* che già eroga a diverse amministrazioni sulla base delle convenzioni in essere. Anche l'Agenzia Nazionale per la Cybersicurezza potrà avvalersi di *Sogei* per realizzare e gestire i propri sistemi informativi nelle more di realizzazione del piano.

È opportuno che la gestione di tali processi di digitalizzazione resti nella “mano pubblica” e che vengano individuati i centri di imputazione delle responsabilità nell'attività di trattamento dei dati.

È importante, altresì, che al centro di tale evoluzione digitale resti “il valore dell'uomo”, inteso sempre come fine, e mai come mezzo.

A tal riguardo, è opportuno ricordare che il termine “robot” deriva etimologicamente dalla lingua serba e significa “lavoro forzato”.

Viene in mente la “*Fenomenologia dello Spirito*” di Hegel, nella dinamica servo-padrone: l'algoritmo è il nuovo padrone delle nostre vite.

Se è vero che le “parole sono azioni”, come affermava Ludwig Wittgenstein, nel suo “*Tractatus logico-philosophicus*” del 1921, il linguaggio diventa strumento dinamico – e non statico – di descrizione dell'evoluzione culturale di una società. I termini che si utilizzano costituiscono l'espressione concreta di un'astrazione concettuale che si traduce nell'implicita accettazione di un comune sentire sociale e culturale.

Non è un caso che John Langslaw Austin, altro grande filosofo del Novecento, indicasse con il termine “*speech act*” il dinamismo descrittivo delle parole che innesta processi sociali e culturali in continuo divenire.

In questo senso, utilizzare nel linguaggio comune, sempre più frequentemente, termini come “decisioni robotizzate”, nel campo del diritto, della medicina e delle altre applicazioni, in ogni aspetto della nostra vita quotidiana, accende un *alert*, il campanello di allarme di elevata intensità sul graduale assoggettamento dell'uomo alla macchina.

³¹⁵ La memoria del Ministro Vittorio Colao del 24 novembre 2021 è reperibile al seguente link https://www.camera.it/application/xmanager/projects/leg18/attachments/upload_file_doc_acquisiti/pdfs/000/006/683/Memoria_Ministro_Colao_prot.pdf; Per gli atti dell'indagine conoscitiva si rinvia al sito della Camera https://www.camera.it/leg18/1101?idLegislatura=18&idCommissione=&tipoElenco=indaginiConoscitiveCronologico&annoMese=&breve=c31_banche_dati&calendario=false&soloSten=false&foglia=true&shadow_organo_parlamentare=3074.

Come spiega l'autrice Kate Crawford nel suo ultimo libro³¹⁶, la tecnologia sta diventando sempre più promiscua: l'intelligenza artificiale non è solo un'invenzione di supporto di cui usufruire, ma è una vera e propria *«idea, un'infrastruttura, un'industria, una forma di esercizio del potere e un modo di vedere le cose ... un attore nella formazione della conoscenza, nella comunicazione e nel potere»*. I computer, le macchine, i robot, gli algoritmi non sono solo concetti astratti, bensì vere e proprie *«infrastrutture fisiche che stanno rimodellando la Terra, modificando contemporaneamente il modo in cui vediamo e comprendiamo il mondo»*.

Si tratta di una rivoluzione nel modo di concepire il mondo intorno a noi, e il nostro compito allora diventa quello di “rimanere con i piedi per terra” per osservare, studiare e comprendere le riconfigurazioni che si stanno verificando *«a livello di epistemologia, principi di giustizia, organizzazione sociale, espressione politica, cultura, concezione del corpo umano, soggettività e identità: cosa siamo e cosa possiamo essere»*.

Bisogna comprendere che l'intelligenza artificiale è politica condotta con altri mezzi; è arrivato il momento di confrontarci con l'IA come forza politica, economica, culturale e scientifica.

Come osservato da Alondra Nelson, Thuy Linh Tu e Alicia Headlam Hines, *«le controversie in campo tecnologico sono sempre collegate a lotte più ampie per la mobilità economica, a questioni politiche e alla costruzione di comunità»*³¹⁷ e come scrive Ursula Franklin, *«la fattibilità della tecnologia, come la democrazia, dipende alla fin fine dalla pratica della giustizia e dall'imposizione di limiti al potere»*³¹⁸.

La tutela della democrazia è basata sulla conoscenza, intesa come *episteme* e non come *doxa*, come opinione volatile, volendo usare termini dell'antica Grecia: la conoscenza si nutre di concetti, dal latino “*cumcapio*”, prendere insieme elementi della realtà per giungere al *conceptus*, al pensiero critico concepito e ragionato.

Il giurista deve allora concepire il pensiero critico, osservando la realtà digitale con intelligenza (dal latino “*intuslegis*” leggere dentro le cose), saper cogliere la complessità, le straordinarie opportunità, ma anche i pericoli dell'intelligenza artificiale che sta invadendo le nostre vite, indicando le linee evolutive di un'equilibrata e lungimirante regolamentazione che sia capace di coniugare il progresso tecnologico con il concetto di “*humanitas*”.

È questa la grande sfida che dovrà affrontare nel prossimo futuro.

³¹⁶ K. CRAWFORD, “*Né intelligente né artificiale. Il lato oscuro dell'IA*”, il Mulino, 2021. L'autrice ci spinge a riflettere, bisogna porsi le seguenti domande: “*cos'è l'IA?*”, “*quali forme di politica propaga?*” “*quali interessi promuove e chi rischia il maggiore danno?*” e “*dove dovremmo limitare l'uso dell'IA?*”.

³¹⁷ A. NELSON, T. L. NGUYEN TU e A. HEADLAM HINES, “*Technicolor. Race, Technology, and Everyday Life*”, 2001.

³¹⁸ U. M. FRANKLIN, “*The Real World of Technology*”, 1999.

Bibliografia

- M. ADINOLFI, *“L’intelligenza artificiale che Platone non si aspettava. Vinceranno gli algoritmi?”*, su *IlFoglio.it*, 2021.
- I. M. ALAGNA, *“Abuso dati personali di utenti: respinto in appello il ricorso di Facebook contro l’Antitrust”*, *Diritto & Giustizia*, fasc. 74, 2021.
- I. ALAGNA, *“Diffamazione a mezzo stampa: il reato sussiste anche in assenza di esplicita indicazione del nome”*, su *Ridare.it*, 18 dicembre 2017.
- I. M. ALAGNA, *“L’interesse pubblico alla diffusione di una notizia non legittima la pubblicazione di immagini ritraenti un minore su testate giornalistiche”*, su *Diritto & Giustizia*, fasc. 38, 2021.
- F. ALBEGGIANI, *“Profili problematici del consenso dell’avente diritto”*, Milano, 1995.
- L. ALESIANI, *“I reati di opinione. Una rilettura in chiave costituzionale”*, Milano, 2006.
- L. ALEXANDRE, *“La guerra delle intelligenze, intelligenza artificiale contro intelligenza umana”*, ed. Torino, 2017.
- L. ALGERI, *“Neuroscienze e testimonianza della persona offesa”*, 2012.
- A. ALÌ, *“Diffamazione via Facebook: condividere post offensivi non è reato”*, su *altalex.com*, 2016.
- G. ALPA, *“Alle origini dei diritti della personalità”*, in *Riv. Trim. di Dir. Proc. Civ.*, 3, 2021.
- G. ALPA, *“La responsabilità civile. Principi”*, Milano, 2018.
- L. AMADEI, *“Il codice dell’amministrazione digitale”*, in L. DE PIETRO (a cura di), *“Dieci lezioni per capire e attuare l’e-government”*.
- V. AMENDOLAGINE, *“Il diritto all’oblio tra rievocazione storiografica online e cronaca giudiziaria”*, su *GiustiziaCivile.com*, 18 agosto 2020.
- P. ASARO, *“A body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics”*, in P. LIN, K. ABNEY, G. A. BEKEY (a cura di), *“Robot Ethics”*, MIT Press, 2012.
- I. ASIMOV, *“Circolo vizioso”*, 1942.

A. ASTONE, *“L’accesso dei minori d’età ai servizi della c.d. “società dell’informazione”: l’art. 8 del Reg (UE) 2016/679 e i suoi riflessi”*, in *Contratto e Impresa*, 2019, 2.

V. BACHELET, *“L’attività tecnica della pubblica amministrazione”*, 1967.

E. BADIALI, *“Il caso Barilla e la tutela del marchio rinomato: commento alla sent. n. 830/2018 del Tribunale di Milano”*, su *iusinitinere.it*, luglio 2018.

C. BAGNOLI, *“Teoria della responsabilità”*, 2019.

J. M. BALKIN, *“Information Fiduciaries and the First Amendment”*, 49 U.C Davis L.REV.1183 (2015).

S. BARCO, *“Il contratto di Influencer marketing: profili civilistici del rapporto tra brand ed influencer”*, su *iusinitinere.it*, 28 maggio 2020.

S. BAROCAS, *“Accountable Algorithms”*, 165 U.PA.L.REV. 633 (2017).

A. BASILE, *“Blockchain: La Nuova Rivoluzione Industriale”*, 2019.

R. BATTAGLINI, M. GIORDANO (a cura di), *“Blockchain e smart contract. Funzionamento, profili giuridici e internazionali, applicazioni pratiche”*, 2019.

M. BELLINI, *“La blockchain per le imprese. Come prepararsi alla nuova «internet del valore»”*, 2019.

A. BELLO, *“Blockchain e privacy: soluzioni per la compliance alle norme”*, 15 maggio 2019, in *agendadigitale.eu*.

V. BELLOMIA, *“Il contratto intelligente: questioni di diritto civile”*, su *judicium.it*, 10 dicembre 2020.

M. BENASOYAG, *“Cinque lezioni di complessità”*, 2020.

M. BENASOYAG, *“Il cervello aumentato, l’uomo diminuito”*, 2016.

M. BENASOYAG *“La responsabilità della rivolta”*, 2021.

M. BENASOYAG, *“La tirannia dell’Algoritmo”*, 2020.

M. BENASOYAG & G. SCHIMT *“L’epoca delle passioni tristi”*, 2004.

L. BENNET MOSES, J. CHAN, *“Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability”*, in *Policing and Society*, 2016.

A. BENVENÙ, *“Alexa, unica testimone di un omicidio. E (legittime) domande sulla nostra privacy”*, su *Nera-Mente*, 2020.

F. BERGER, *“Intelligenza artificiale, rileggere la storia per evitare un nuovo inverno”*, su *formiche.net*.

L. BERTO, *“E’ possibile registrare un hashtag come marchio?”*, su *iusinitinere.it*, 13 novembre 2017.

M. BIANCA, *“Diritto civile”*, Milano, 2011.

G. BIANCHEDI, *“Il consenso dei minori per i servizi della società dell’informazione sotto il profilo giuridico e informatico”*, in *Cyberspazio e diritto*, vol. 20, n. 63 (3-2019).

D. BIANCHI, *“Danno e oblio. Nesso di causalità, principio di proporzionalità e misure di sicurezza Data Protection”*, su *Ridare.it*, 19 ottobre 2016.

E. BLACKBURN, *“La scienza che allunga la vita. La rivoluzione dei telomeri”*, 2017.

N. BOLDRINI, *“Blockchain e GDPR: le sfide (e le opportunità) per la protezione dei dati”*, in *blockchain4innovation.it*, 2018.

M. BORGOBELLO, *“Acquisizione di tabulati telefonici: che cambia col nuovo decreto-legge”*, su *agendadigitale.ue*, 4 ottobre 2021.

F. BRAVO, *“Il consenso e le altre condizioni di liceità del trattamento dei dati personali”*, in G. FINOCCHIARO (diretto da), *“Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali”*, Torino, Zanichelli, 2017.

F. BRIZZI, *“Diffusione illecita di immagini o video sessualmente espliciti: tra tutela della privacy e revenge porn”*, su *Ilpenalista.it*, 30 Marzo 2021.

E. BUCCI, *“Anche all’intelligenza artificiale può essere attribuito un brevetto”*, 2021, su *IlFoglio.it*.

C. BURCHARD, *“L’Intelligenza Artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società”*, in *Rivista italiana di diritto e procedura penale*, 2019, Vol. 62.

G. BUSIA, L. FEROLA, *“Il Garante per la protezione dei dati personali: le funzioni, i rapporti con le altre Istituzioni ed Autorità in Italia e in Europa”*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *“Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive”*, Aracne, 2016.

- M. CAIELLI, *“Punire l’omofobia: (non) ce lo chiede l’Europa. Riflessioni sulle incertezze giurisprudenziali e normative in tema di hate speech”*, in *GenIus*, 2015.
- G. M. CALETTI, *“Revenge porn e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane”*, in *DirPenCont*, 2018.
- C. CALVERT – J. BROWN, *“Video Voyeurism, Privacy and the Internet: exposing Peeping Toms in Cyberspace”*, in *Cardozo Arts Entertainment Law Journal*, 2000.
- C. CAMARDI, *“L’eredità digitale. Tra reale e virtuale”*, in *“Il diritto dell’informazione e dell’informatica”*, 2018.
- E. CAPACCIOLI, *“Manuale di diritto amministrativo”*, Padova, 1983.
- P. F. CARBALLO-CALERO, *“Pubblicità occulta e product placement”*, Cedam, 2004.
- P. CARBONE, *“Adolescenza e disagio”*, 2001.
- R. D. CARDENAS ESPINOSA e altri, *“Ecosistemi tecnologici per la ricerca formativa nel contesto”*, Ed. Sapienza, 2020.
- P. CARETTI e A. CARDONE, *“Diritto dell’informazione e della comunicazione nell’era della convergenza”*, Bologna, Mulino, 2019.
- F. CASASOLE, *“Neuroscienze, genetica comportamentale e processo penale”*, 2012.
- A. CASSATELLA, *“La responsabilità funzionale nell’amministrare. Termini e questioni”*, in *Dir. Amm.*, 2018.
- S. CASSESE, *“Le reti come figura organizzativa della collaborazione”*, in ID., *“Lo spazio giuridico globale”*, Roma-Bari, 2003.
- J. L. CASTI, W. DE PAULI, *“Gödel. L’eccentrica vita di un genio”*, Raffaello-Cortina Edizioni, Milano, 2001.
- M. CASTIGLI, *“Come il metaverso ci cambia il rapporto col corpo: nuovi rischi psicologici”*, su *agendadigitale.eu*.
- C. CASTRONOVO, *“La «civilizzazione» della pubblica amministrazione”*, in *Europa e dir. priv.*, 2013.
- C. CASTRONOVO, *“Responsabilità civile”*, Milano, 2018.

C. CATH, S. WACHTER, B. MITTELSTADT, M. TADDEO, L. FLORIDI, “*Artificial Intelligence and the “Good Society”: the US, EU, and UK approach*”, in *Science and Eng. Ethics*, 2018.

N. CHAKRABORTI, J. GARLAND, “*Hate Crime. Impact, Causes, and Responses*”, Los Angeles-Londra, 2015.

V. CERULLI IRELLI, “*Giurisdizione amministrativa e pluralità delle azioni (dalla Costituzione al Codice del processo amministrativo)*”, in *Dir. Proc. Amm.*, 2012.

G. O. CESARO, “*Genitore pubblica sui social network foto e notizie del figlio minore: interviene d’ufficio il Giudice*”, su *Ilfamiliarista.it*, marzo 2018.

J. CIANI, M. TAVELLA, “*La riconoscibilità della natura pubblicitaria della comunicazione alla prova del digital: native advertising tra obbligo di disclosure e difficoltà di controllo*”, in “*Social media e diritto. Diritti e social media*” della *Rivista Informatica e Diritto*, 2017.

S. CIARDO, “*Privacy e tutela dei dati personali memorizzati nell’account della persona deceduta*”, su *Ridare.it*, 20 aprile 2021.

G. CITARELLA, “*Aggiornamento degli archivi online, tra diritto all’oblio e rettifica «atipica»*”, su *Responsabilità Civile e Previdenza*, fasc. 4, 2012.

D. CITRON – K. FRANKS, “*Criminalizing Revenge Porn*”, in *Wake Forest Law Review*, 2014.

M. CLARICH, “*La responsabilità della pubblica amministrazione nel diritto italiano*”, in *Riv. Trim. Dir. Pubbl.*, 1989.

J. CLOUGH, “*Principles of Cybercrime*”, Cambridge, 2010.

M. COCUCCIO, “*Deindicizzare per non censurare: il «ragionevole compromesso» tra diritto all’oblio e diritto di cronaca*”, su *Responsabilità Civile e Previdenza*, fasc. 1, 2021.

COMMISSIONE EUROPEA, “*Libro Bianco sull’intelligenza artificiale – Un approccio europeo all’eccellenza e alla fiducia*”, Bruxelles, 19.2.2020 COM (2020) 65 final.

T. M. COOLEY, “*A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*”, Chicago, 1888.

M. CORRADINO, “*Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*”, su *www.giustizia-amministrativa.it*, 10 settembre 2021.

K. CRAWFORD & J. SCHULTZ, *“Big Data and Due Process: toward a Framework to Redress Predictive Privacy Harms”*, 55 B.C.L. REV.93 (2014).

K. CRAWFORD, *“Né intelligente né artificiale. Il lato oscuro dell’IA”*, il Mulino, 2021.

A. CREA, *“L’Intelligenza Artificiale sta rivelando una biologia sconosciuta”*, su tomshw.it.

E. J. CRIDDLE, P. B. MILLER & R. H. SITKOFF, *“Oxford Handbook of Fiduciary Law”*, Oxford, 2018.

L. CUSANO, *“Tabulati telefonici: ulteriori ricadute della sentenza della CGUE del 2 marzo 2021 sul piano della utilizzabilità degli esiti di prova”*, su ilpenalista.it, 25 maggio 2021.

G. D’ACQUISTO, *“Blockchain e GDPR: verso un approccio basato sul rischio”*, in www.federalismi.it, 18 gennaio 2021.

M. DAL CO E A. LONGO, *“Metaverso, nuovo business della rete? Ecco gli scenari”*, su agendadigitale.eu.

A. DAMASIO, *“Alla ricerca di Spinoza. Emozioni, sentimenti e cervello”*, Adelphi, Milano, 2003.

A. DAMASIO, *“L’errore di Cartesio. Emozioni, ragione e cervello umano”*, Adelphi, Milano, 1995.

M. D’ANGELOSANTE, *“La consistenza del modello dell’amministrazione invisibile nell’età della tecnificazione della formazione delle decisioni alla responsabilità per le decisioni”*, in S. CIVITARESE MATTEUCCI – L. TORCHIA (a cura di), *“La tecnificazione”*.

V. D’ANTONIO e D. TARANTINO, *“Il product placement nell’ordinamento italiano: breve fenomenologia di uno strumento pubblicitario”*, in *Comparazione e Diritto Civile*, 2011.

J. W. DAWSON JR., *“Dilemmi logici. La vita e l’opera di Kurt Gödel”*, Bollati Boringhieri, Torino, 2001.

G. DE CRISTOFARO, *“Influencer Marketing: caso ‘Crema Pan di Stelle’. Come nel caso Alitalia-Ferretti nessuna sanzione. L’Antitrust accetta gli impegni di Barilla e dei Micro-Influencer. tanto rumore per nulla? Non si direbbe: altri spunti utili per inserzionisti e influencer”*, su youmark.it, 17 marzo 2020.

J. DELLA TORRE, *“L’acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del Gip di Roma”*, su sistemapenale.it.

A. DE LUCIA, *“Offese su Facebook: la Cassazione conferma la legittimità del licenziamento”*, su altalex.com.

E. DHAWAN, *“Digital body language. How to build trust & connection no matter the distance”*, 2021.

A. DI MAJO, *“Profili della responsabilità civile”*, Torino, 2010

L. DIOTALLEVI, *“La Corte di cassazione sancisce l’“equiparazione” tra giornali cartacei e telematici ai fini dell’applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di “scivolamento” dalla “nomofilachia” alla “nomopoiesi”?”*, su *Giurisprudenza Costituzionale*, fasc. 3, 2015.

C. D’ORTA, *“Il sistema pubblico di connettività”*, in *Giornale di diritto amministrativo*, 2005.

N. ELIAS, *“La civiltà delle buone maniere”*, 2009.

A. FALZEA, *“Teoria dell’efficacia giuridica”*, in *“Ricerche di teoria generale del diritto e di dogmatica giuridica”*, vol. I, Milano, 1999.

B. J. FEIJOS SANCHEZ, *“Derecho Penal y Neurociencias, Una relación tormentosa?”*, 2011.

P. FERRAGINA – F. LUCCIO, *“Il pensiero computazionale. Dagli algoritmi al coding”*, Bologna, 2017.

W. FERRI, *“2,4 milioni per 500mq di cyber spazio: il Metaverso e la corsa all’oro digitale”*, su lindipendenteonline.it.

F. FERRONETTI, *“Blockchain e smart contract, servono regole chiare: lo scenario”*, su agendadigitale.eu, 14 ottobre 2021.

L. FILIPPI, *“La nuova disciplina dei tabulati: il commento “a caldo” del Prof. Filippi”*, su penaledp.it, 1° ottobre 2021.

L. FLORIDI, *“Intelligenza Artificiale. L’uso delle nuove macchine”*, Bompiani, 2021.

E. FOLLIERI, *“La tipologia delle azioni proponibili”*, in F. G. SCOCA (a cura di), *“Giustizia amministrativa”*, Torino, 2017.

G. FORNASARI, *“I principi del diritto penale tedesco”*, Padova, 1993.

U. M. FRANKLIN, *“The Real World of Technology”*, 1999.

S. GABORIAU, *“Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà a questi valori?”*, in *Questione Giustizia*, fasc. 4, 2018.

A. GAMBINO, C. BOMPRESZI, *“Blockchain e titolare del trattamento dei dati personali: il nodo rimane irrisolto”*, in www.iaic.it, 20 gennaio 2020.

C. GARBARINO, *“Applicazione del FATCA a livello europeo e protezione dei dati”*, 2018, su privatebank.jpmorgan.com.

P. GHEZZI, *“Blockchain, quali prospettive per le politiche pubbliche”*, in www.blockchain4innovation.it, 14 aprile 2021.

S. GIANCONE, *“Influencer e social network: quando l’uso di un marchio altrui è un atto illecito”*, su iusinitinere.it, 8 ottobre 2020.

M. S. GIANNINI, *“Il potere discrezionale della pubblica amministrazione. Concetto e problemi”*, Milano, 1939.

S. GLEß, E. SILVERMAN, T. WEIGEND, *“If robots cause harm, who is to blame? Self-driving cars and criminal liability”*, in *New Criminal Law Review*, 2016.

K. GÖDEL, *“Sulle proposizioni formalmente indecidibili dei Principia Mathematica e di sistemi affini”*, in S. G. SHANKER (a cura di), *“Il teorema di Gödel”*, trad. it. di P. PAGLI, Franco Muzzio Editore, Padova, 1991.

L. GOISIS, *“Hate Crimes: perché punire l’odio. Una prospettiva internazionale, comparatistica e politico-criminale”*, in *RIDPP*, 2018.

L. GOISIS, *“Libertà di espressione e odio omofobico. La Corte europea dei diritti dell’uomo equipara la discriminazione in base all’orientamento sessuale alla discriminazione razziale”*, in *RIDPP*, 2013.

L. GOISIS, *“Omosessualità, hate crimes e diritto penale”*, in *GenIus*, 2015.

R. GOLDSTEIN, *“Incompletezza. La dimostrazione e il paradosso di Kurt Gödel”*, Codice Edizioni, Torino, 2006.

C. GRANDI, *“Neuroscienze e responsabilità penale: nuove soluzioni per problemi antichi”*, 2016.

G. GRECO, *“Dal dilemma diritto soggettivo-interesse legittimo, alla differenziazione interesse strumentale-interesse finale”*, in *Dir. amm.*, 2014.

A. GRECO, *“Il metaverso come il Monopoli: scatta la corsa al mattone virtuale”*, su *Repubblica.it*

G. GRIZIOTTI, *“Neurocapitalismo: mediazioni tecnologiche e linee di fuga”*, 2016.

G. HALLEVY, *“The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control”*, in *Akron Intellectual Property Journal*, 2010

A. HODGES, *“Storia di un enigma. Vita di Alan Turing 1912-1954”*, Bollati Boringhieri, Torino, 2004.

M. IASELLI, *“Blockchain e privacy, bisogna lavorare ancora molto”*, in *federprivacy.org*, luglio 2020.

M. IASELLI, *“Consiglio di Stato: quando si può parlare di intelligenza artificiale? Palazzo Spada affronta una delicata questione tecnica sulla nozione di algoritmo, che assume notevole importanza anche per le necessarie conseguenze di carattere giuridico”*, su *altalex.it*.

M. IASELLI, *“La raccomandata on line: disciplina normativa ed aspetti operativi”*, in *Diritto dell’Internet*, n. 6, 2006.

A. IEVOLELLA, *“Offeso con una e-mail inviata a lui e ad alcuni colleghi: è diffamazione”*, su *Diritto & Giustizia*, fasc. 73, 2021.

L. IMARISIO, *“Il reato che non osa pronunciare il proprio nome. Reticenze e limiti nel c.d. disegno di legge Scalfarotto”*, in *GenIus*, 2015.

G. IOZZIA, *“Influencer marketing e quadro normativo”*, su *altalex.com*, 17 luglio 2019.

N. IRTI, *“Il diritto nell’età della tecnica”*, Editoriale Scientifica, 2007.

N. IRTI, *“Norme e fatti. Saggi di teoria generale del diritto”*, Milano, 1984.

R. JACCHIA, M. STILLO, *“Codice Ue delle comunicazioni elettroniche: la nuova normativa per un mercato più accessibile e sicuro”*, su *agendadigitale.eu*, 30 aprile 2021.

P. JEAMMET, *“Psicopatologia dell’adolescenza”*, 2019.

D. KAHNEMAN, *“Pensieri lenti e veloci”*, 2012.

M. KAMAL – W. NEWMAN, “*Revenge Pornography: Mental Health Implications and Related Legislation*”, in *The Journal of American Academy of Psychiatry and the Law*, 2016.

E. R. KANDEL “*Principi di neuroscienze*”, 2015.

I. KANT, “*Principi metafisici della dottrina del diritto*”, 1797.

D. KEATS CITRON, “*Technological Due Process*”, 85, Wash. Un.L.Rev.1249.

D. KEATS CITRON & F. PASQUALE, “*The Scored Society: Due Process for Automated Predictions*”, 89 WASH.L.REV. 1 (2014).

T. KING, N. AGGARWAL, M. TADDEO, L. FLORIDI, “*Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*”, in *Science and Engineering Ethics*, 2019.

H. A. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER, “*The Age of AI: And Our Human Future*”, 2021.

J. KROLL, “*Accountable Algorithms*”, 165 Univ.Penn.L.Rev. 2017.

M. LANCINI, “*Abbiamo bisogno di genitori autorevoli. Aiutare gli adolescenti a diventare adulti*”, Mondadori, 2017.

M. LANCINI, “*Adolescenti navigati, Come sostenere la crescita dei nativi digitali*”, Erickson, 2015.

M. LANCINI, “*Cosa serve ai nostri ragazzi. I nuovi adolescenti spiegati ai genitori, agli insegnanti, agli adulti*”, Utet, 2020.

M. LANCINI, “*Il ritiro sociale negli adolescenti. La solitudine di una generazione iperconnessa*”, Raffaello Cortina, 2019.

E. LATIFAH, A. H. BAJREKTAREVIC, M. N. IMANULLAH, “*Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution*”, in *Brawijaya Law Journal – Journal of Legal Studies*, vol. 6, aprile 2019.

A. LAVAZZA, L. SAMMICHELI, “*Il delitto del cervello. La mente tra scienza e diritto*”, 2012.

F. M. LAWRENCE, “*Punishing Hate. Bias Crimes under American Law*”, Cambridge, 1999.

- D. LEAVITT, *“L’uomo che sapeva troppo. Alan Turing e l’invenzione del computer”*, La Biblioteca delle Scienze, Milano, 2009.
- F. LEDDA, *“Potere, tecnica e sindacato giudiziario”*, in *“Studi in memoria di V. Bachelet”*, Milano, 1987.
- G. LEGANZA, *“Luciano Floridi ci spiega cosa c’è di antico nell’intelligenza artificiale”*, su *IlFoglio.it*.
- L. LESSIG, *“Code.Version 2.0”*, New York, 2006.
- I. LICATA, *“Complessità. Un’introduzione semplice”*, Di Renzo Editore, 2018.
- I. LICATA, *“I teoremi di Gödel e l’intelligenza artificiale”*, su *Indiscreto.org*.
- I. LICATA, *“La logica aperta della mente”*, Codice Edizioni, Torino, 2008.
- I. LICATA, *“Piccole variazioni sulla scienza”*, Dedalo, Bari, 2016.
- D. LIMA, *“Could AI Agents Be Held Criminally Liable? Artificial Intelligence and the Challanges for Criminal Law”*, in *South Carolina Law Review*, 2018.
- A. LISI, *“Come sarà il 2022 dei documenti informatici: nuove regole digitali e qualche polemica”*, su *agendadigitale.eu*.
- A. R. LODDER, J. ZELEZNIKOW, *“Artificial Intelligence and Online Dispute Resolution”*, in A. R. LODDER, J. ZELEZNIKOW, *“Enhaced Dispute Resolution through the Use of Information Technology”*, Cambridge University Press, 2010.
- I. M. LO PRESTI, *“CasaPound, Forza Nuova e Facebook. Considerazioni a margine delle recenti ordinanze cautelari e questioni aperte circa la relazione tra partiti politici e social network”*, in *Forum di Quaderni Costituzionali*, 2, 2020.
- J. R. LUCAS, *“Mind, Machines and Gödel”*, in *Philosophy*, 36, 1961.
- G. LUIGI, *“La Corte di cassazione ritorna sull’acquisizione dei tabulati telefonici dopo le indicazioni della CGUE”*, su *Ilpenalista.it*, 5 ottobre 2021.
- L. LUPARIA, *“Data retention e processo penale. Un’occasione mancata per prendere i diritti davvero sul serio”*, in *Diritto di Internet*, 2019, 4.
- A. MALACARNE, *“La decretazione d’urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132”*, su *Sistema Penale*, 8 ottobre 2021.

B. MANCA, *“L’Antitrust apre istruttoria su Alitalia e Aege di Alberta Ferretti: nel mirino anche le foto di influencer: “pubblicità non riconoscibile”*, su *ilfattoquotidiano.it*, 15 dicembre 2018.

G. MANCA, *“Interoperabilità nella pubblica amministrazione: presente e futuro digitale”*, in *www.agendadigitale.eu*, 6 settembre 2018.

A. MAGNANI, *“L’eredità digitale”*, in *Notariato*, 2014.

D. MARCIANO, G. CAPACCIOLI, *“La blockchain ed il problema del trattamento dei dati personali”*, in *www.affidaty.io*, 4 giugno 2019.

R. MARDON, *“The relationship between ownership and possession: observations from the context of digital virtual goods”*, 2016.

F. MARENGHI, *“Diritto alla presunzione di innocenza e nuovi strumenti di tutela”*, su *altalex.com*, febbraio 2022.

F. MARENGHI, *“Riforma giustizia penale: il provvedimento di «deindicizzazione»”*, su *altalex.com*.

G. MARINO, *“La successione digitale”*, in *Oss. dir. civ. e comm.*, 2018.

F. MARTINI, *“Il sistema informativo pubblico”*, in *“Quaderni del Dipartimento Pubblico”*, Università di Pisa, Torino, 2006.

M. MARTORANA, *“L’offesa su Facebook non è reato se l’insultato è online”*, su *altalex.com*, febbraio 2022.

M. MARTORANA, *“Minori sui social: educiamoli per difenderli”*, su *agendadigitale.eu*.

M. MASSIMI, *Art. 132*, in R. SCIAUDONE (a cura di) *“Il Codice della Privacy”*, Pacini, Ospedaletto, 2019.

G. MASTROBUONI, *“Crime is Terribly Revealing: Information Technology and Police Productivity”*, 2017.

R. MAZZUCCONI, *“L’influencer marketing e il rapporto di endorsement tra aziende e influencers: profili giuridici e derive illecite”*, su *cyberlaws.it*, 21 maggio 2020.

V. MAYER-SCHOENBERGER, K. CUKIER, *“Big Data. Una rivoluzione che trasformerà il nostro modo di vivere”*, Garzanti, Milano, 2016.

C. MELZI D'ERIL, *“La Cassazione esclude l'estensione ai siti internet delle garanzie costituzionali previste per il sequestro di stampati”*, in *Dir. Pen. Uomo*, 2014.

L. MISCHITELLI, *“Intelligenza artificiale etica: ecco l'approccio “globale” Unesco (approvato anche dalla Cina)”*, su *agendadigitale.eu*.

S. MOLFINO, *“Vietato pubblicare le foto dei figli sui social network senza il consenso dell'altro genitore”*, su *Ilfamiliarista.it*, gennaio 2018.

P. G. MONATERI, *“La responsabilità civile”*, Torino, 2006.

L. MORASSUTTO, *“Omofobia e medioevo italiano”*, in *GenIus*, 2015.

C. MORELLI, *“Dallo spazio economico europeo allo spazio comune dei data UE”*, in *www.altalex.com*, 22 marzo 2021.

A. MORETTI, *“Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento UE 2016/679”*, in *“Diritto dell'informazione e dell'Informatica”*, 2018

L. MUMFORD, *“Technics and Civilization”*, 1961.

G. NATALE, *“La Grande Sezione della Corte di Giustizia si è pronunciata sui poteri delle Autorità Nazionali nell'ambito del RGDP a fronte della gestione dei dati da parte dei colossi del web (C. giust. UE, Grande Sezione, sentenza 15 giugno 2021, C-645/19)”*, su *Rassegna Avvocatura dello Stato*, Gennaio-Marzo 2021.

A. NATALINI, *“Diritto all'immagine e pubblicazione di foto non autorizzata: per essere risarcita è la parte lesa che deve provare il pregiudizio economico”*, su *Diritto & Giustizia*, fasc. 0, 2010.

A. NELSON, T. L. NGUYEN TU e A. HEADLAM HINES, *“Technicolor. Race, Technology, and Everyday Life”*, 2001.

W. NONNIS, *“Blockchain, il suo contributo durante la pandemia”*, in *www.blockchain4innovation.it*, 19 aprile 2021.

E. NUNZIANTE, *“Influencer e pubblicità, quale trasparenza: che fare”*, su *agendadigitale.eu*, 30 ottobre 2019.

D. ORMEROD, *“Voyeurism: Elements of Offence-Privacy-Reasonable Expectation of Privacy”*, in *CrimLawReview*, 2008.

P. OTRANTO, *“Decisione amministrativa e digitalizzazione della p.a.”*, in *federalismi.it*.

U. PAGALLO, S. QUATTROCOLO, *“The impact of AI on criminal law, and its two fold procedures”*, in W. BARFIELD, U. PAGALLO (a cura di), *“Research Handbook on the Law of Artificial Intelligence”*, Edward Elgar Pub, 2018.

E. PALAZZOLO, *“Libertà di espressione, Facebook e movimenti di estrema destra: provvedimenti a confronto”*, 2020.

C. PAPPALARDO, *“Influencer e Autodisciplina pubblicitaria – prime applicazioni della Digital Chart”*, su *DeJure*.

L. PARDO, *“Il metaverso spalanca nuove frontiere dell’economia. E delle regole”*, su *wired.it*.

C. PARODI, *“Sottratto al P.M. il potere di richiedere autonomamente i tabulati”*, su *ilpenalista.it*, 1° ottobre 2021.

C. PARODI, *“Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge”*, su *ilpenalista.it*, 3 maggio 2021.

C. PARODI, *“Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE”*, su *ilpenalista.it*, 5 agosto 2021.

L. PASCULLI, *“Genetics, Robotics and Crime Prevention”*.

F. PASQUALE, *“The Black Box Society. The secret Algorithms that Control Money and Information”*, Cambridge – Ma 2015.

N. PATRIGNANI, *“Metaverso, rischio di un nuovo Medioevo digitale”*, su *agendadigitale.eu*.

F. PATRONI GRIFFI, *“La decisione robotica e il giudice amministrativo”*, in *giustizia-amministrativa.it*.

M. PELISSERO, *“La parola pericolosa. Il confine incerto del controllo penale del dissenso”*, in *QuestG*, 2015.

M. PELISSERO, *“Omofobia e plausibilità dell’intervento penale”*, in *GenIus*, 2015.

R. PELLICCIA, *“Polizia predittiva”*, *Human Rights Data Analysis Group (Hrdag)*.

R. PENROSE, *“La Mente Nuova dell’Imperatore”*, nel 1992.

S. PERON, *“Il risarcimento dei danni da diffamazione: analisi e riflessione sui criteri orientativi proposti dell’Osservatorio sulla Giustizia civile di Milano”* (edizione 2018), in *filodiritto.it*, 2018.

- S. PERON, *“Internet, regime applicabile per i casi di diffamazione e responsabilità del direttore”*, su *Responsabilità Civile e Previdenza*, fasc. 1, 2011.
- B. PERRY, *“In the Name of Hate: Understanding Hate Crimes”*, Londra, 2001.
- E. PERUSIA, *“Giurisdizione italiana anche per le offese on line su un sito straniero”*, su *Cassazione Penale*, fasc. 6, 2001.
- G. PESTELLI, *“D.L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici”*, su *quotidianogiuridico.it*, 4 ottobre 2021.
- D. PETRINI, *“Il direttore della testata telematica, tra horror vacui e prospettive di riforma; sperando che nulla cambi”*, su *Riv. It. Dir. e Proc. Pen.*, fasc. 4, 2012.
- E. PICOZZA, *“Problems about enforcement”*, in E. PICOZZA, *“Neurolaw. An Introduction”*, Ed. Springer, 2016.
- I. PIETROLETTI, *“Nessun risarcimento per l’avvocato se non prova i pregiudizi concreti ricollegabili all’attività”*, su *Diritto & Giustizia*, fasc. 128, 2018.
- G. PIETROPOLLI CHARMET, *“I nuovi adolescenti”*, 2000.
- F. PIZZETTI, *“Intelligenza artificiale, protezione dei dati personali e regolazione”*, Torino, 2018.
- F. PIZZETTI, *“Privacy e il diritto europeo alla protezione dei dati personali. dalla direttiva 95/46 al nuovo Regolamento europeo”*, 2016.
- F. PIZZETTI, *“Protezione dei dati personali in Italia tra GDPR e codice novellato”*, 2021.
- A. POLICE, *“Il principio di responsabilità”*, in M. RENNA, F. SAITTA, (a cura di) *“Studi sui principii del diritto amministrativo”*, Milano, 2012.
- O. POLLICINO, *“Codice della comunicazione digitale”*, 2015.
- O. POLLICINO, *“Diritto dell’informazione e dei media”*, 2019.
- O. POLLICINO, *“Parole e potere. Libertà di espressione, hate speech e fake news”*, 2017.
- V. PORTALE, *“Quanto è legale la Blockchain? La compatibilità tra Blockchain e normativa GDPR”*, in *www.blog.osservatori.net*, 31 luglio 2020.
- R. A. POSNER, *“The Right of Privacy”*, 12 *Georgia Law Review* 393, 1977.

A. PROTO PISANI, “*Appunti sulla c.d. tutela costitutiva e sulle tecniche di produzione degli effetti sostanziali*”, in *Riv. dir. proc.*, 1991.

A. PUGIOTTO, “*Aporie, paradossi ed eterogenesi dei fini nel disegno di legge in materia di contrasto all’omofobia e alla transfobia*”, in *GenIus*, 2015.

S. PUGLIATTI, “*La proprietà nel nuovo diritto*”, 1964.

M. RACO, “*La Digital Chart: una prima regolamentazione dell’influencer marketing*”, su *iusinitinere.it*, 5 maggio 2020.

M. RACO, “*Product placement ai limiti della pubblicità occulta: Baby K e Chiara Ferragni per Pantene*”, su *iusinitinere.it*, 3 gennaio 2021.

G. U. RESCIGNO, “*L’esercizio dell’azione pubblica ed il pubblico ministero*”, relazione dell’8 novembre 2004 al Convegno dell’Associazione Italiana dei Costituzionalisti su “*Separazione dei poteri e funzione giurisdizionale*”.

F. RESTA, “*Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*”, su *Giustizia Insieme*.

G. RESTA, V. ZENO-ZENCOVICH (a cura di), “*Il diritto all’oblio su internet dopo la sentenza Google Spain*”, Roma Tre Press, Roma, 2015.

F. RESTA, “*La nuova disciplina dell’acquisizione dei tabulati*”, su *Giustizia Insieme*, 2 ottobre 2021.

N. REZENDE, “*Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*”, in *www.sistemapenale.it*.

V. RICCIUTO, C. SOLINAS, “*Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto*”, *GiustiziaCivile.com*, 18 maggio 2021.

L. RINALDI, “*Sul cibo, sul corpo e sul divenire della forma*”, 2021.

L. RINALDI, “*Sul nascere madri e padri. L’abisso, le sue insidie e le sue possibilità*”, 2019.

E. RINALDINI, “*Data retention e procedimento penale. Gli effetti della sentenza della Corte di Giustizia nel caso H.K. sul regime dell’acquisizione dei tabulati telefonici e telematici: urge l’intervento del legislatore*”, in *Giurisprudenza Penale Web*, 2021, 5.

S. RIONDATO, “*Robotica e diritto penale (robot, ibridi, chimere, “animali tecnologici”)*”, in D. PROVOLO, S. RIONDATO, F. YENISEY (a cura di), “*Genetics, Robotics, Law, Punishment*”.

S. RODOTÀ, “*Il mondo nella rete. Quali diritti, quali vincoli*”, Editori Laterza e la Repubblica, Roma-Bari, 2014.

M. ROSSETTI, “*Post nubila phoebus, ovvero gli effetti concreti della sentenza delle sezioni unite n. 26972 del 2008 in tema di danno non patrimoniale*”, su *Giustizia Civile*, fasc. 4-5, 2009.

E. ROTOLO, “*Sarà metaverso in mille settori: ecco tutte le possibilità di business*”, su *agendadigitale.eu*.

C. ROXIN, “*Sul consenso nel diritto penale*”, in “*Antigiuridicità e cause di giustificazione. Problemi di teoria dell’illecito penale*”, a cura di S. MOCCIA, Napoli, 1996.

C. ROXIN, “*Über die mutmassliche Einwilligung*”, in “*Festschrift für Hans Welzel*”, Berlino-New York 1974.

U. RUFFOLO, E. AL MUREDEN, “*Autonomous vehicles e responsabilità nel nostro sistema ed in quello statunitense*”, in *Giurisprudenza Italiana*, 2019.

U. RUFFOLO, A. AMIDEI, “*Intelligenza artificiale e diritti della persona: le frontiere del transumanesimo*”.

U. RUFFOLO, “*Intelligenza Artificiale, machine learning e responsabilità da algoritmo*”, in *Giurisprudenza Italiana* n. 7/2019, Utet Giuridica, Torino.

N. RUGGIERO, “*Quanto (e come) ci spia lo smartphone? Tutte le trappole che ignoriamo*”, su *agendadigitale.eu*

A. RUTJES, “*Blockchain and GDPR: better safe than sorry*”, 2018.

F. SAITTA, “*Le patologie dell’atto amministrativo elettronico e il sindacato del giudice amministrativo*”, in *Riv.dir.amm.elettronico*, disponibile on line, 2003.

B. SANDYWELL, “*On the globalisation of crime: The internet and the new criminality*”, in “*Handbook of Internet Crime*”, a cura di Y. JEWKES – M. YAR, Milton, 2010.

S. SARDELLA, “*Influencer marketing e Fashion Law*”, su *iusinitinere.it*, 19 aprile 2020.

G. SATELL, “*3 Reasons to Kill Influencer Marketing*”, su *Harvard Business Review*, 2014.

C. SCHMITT, *“Il nomos della terra nel diritto internazionale dello «Jus publicum europaeum»”*, Adelphi, 2011.

F. G. COCA, *“L’interesse legittimo. Storia e teoria”*, Torino, 2017.

A. SERENA, *“Eredità digitale”*, in AA.VV, *“Identità ed eredità digitali, stato dell’arte e possibili soluzioni”*, Aracne, 2016.

R. SETTIMIO, *“Deindicizzazione e diritto all’oblio al vaglio della Suprema Corte”*, su *GiustiziaCivile.com*, 27 settembre 2021.

G. SIAS, *“La Nuova Sardegna”*, 2 febbraio 2018.

A. SIMEONE, *“La nuova compagna del padre non può pubblicare le foto dei minori senza il consenso della madre”*, su *Ilfamiliarista.it*, luglio 2019.

E. SIMIONATO, *“AGCM e pubblicità occulta: aperto il procedimento istruttorio nei confronti di BAT e Stefano De Martino, Cecilia Rodriguez e Stefano Sala”*, su *iusinitinere.it*, 1° giugno 2021.

E. SIMIONATO e M. E. ORLANDINI, *“Fedez, Mille e Coca Cola: è davvero pubblicità occulta?”*, su *iusinitinere.it*, 8 luglio 2021.

G. SIMMEL, *“La socievolezza”*, 2011.

A. SIMONCINI, *“L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà”*, 2019.

G. SPANGHER, *“I tabulati: un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali”*, in *Giustizia Insieme*, 3 maggio 2021.

A. SPENA, *“Libertà di espressione e reati di opinione”*, in *RIDPP*, 2007.

L. STEINBERG, *“Adolescence”*, 2010.

L. STEINBERG, *“Age of opportunity: Lessons from the New Science of Adolescence”*, 2015.

L. STEINBERG, *“The 10 Basic principles of Good parenting”*, 2005.

L. STEINBERG, *“You and your adolescent”*, 2011.

S. STERRETT, *“Bringing up Turing’s “Child Machine”*, in *“How the world computes”* Turing Centenary Conference, Springer, 2012.

F. TARSITANO, *“Il diritto del lavoro alla prova degli algoritmi: la “tappa” della Procura di Milano nella corsa alla tutela dei riders”*, su *quotidianogiuridico.it*, Marzo 2021.

S. TORDINI CAGLI, *“Principio di autodeterminazione e consenso dell’avente diritto”*, Bologna, 2008.

A. TRAVERSI, *“Intelligenza artificiale applicata alla giustizia”*, 2005.

P. TRIMARCHI, *“La responsabilità civile: atti illeciti, rischio, danno, responsabilità civile”*, 2021.

A. TURING, *“Le basi chimiche della morfogenesi”*, Mimesis Edizioni, Sesto San Giovanni, 2021.

F. VALERINI, *“La familiarità della minore con i social network non salva Yahoo.it dal risarcimento del danno per la pubblicazione della foto”*, su *Diritto & Giustizia*, fasc. 92, 2018.

G. VELLAR, F. BASILE, *“Diritto penale e neuroscienze”*, 2016.

G. E. VIGEVANI, O. POLLICINO, C. MELZI D’ERIL, M. CUNIBERTI, M. BASSINI, *“Diritto dell’informazione e dei media”*, G. Giappichelli Editore, Torino, 2019.

A. VILLA, *“Il diritto di critica ancorché contenga giudizi soggettivi deve fondarsi su fatti che debbono corrispondere a verità perlomeno putativa”*, su *Diritto & Giustizia*, fasc. 171, 2017.

P. VILLASCHI, *“Facebook come la RAI?: note a margine dell’ordinanza del Tribunale di Roma del 12.12.2019 sul caso CasaPound c. Facebook”*, su *osservatorioaic.it*.

F. VOLPE, *“Discrezionalità tecnica e presupposti dell’atto amministrativo”*, in *Dir. Amm.*, 2008.

S. D. WARREN e L. D. BRANDEIS, *“The Right to privacy”*, *Harvard Law Review*, 1890.

D. M. WEGNER, *“The illusion of conscious will”*, 2002.

L. WINNER, *“Autonomous technology”*, Cambridge, Mass., 1977.

M. ZALNIERIUTE, L. BENNETT MOSES, G. WILLIAMS, *“The Rule of law and Automation of Government Decision-Making”*, in *“The modern law review”*, 2019.

F. ZAMBONIN, *“Alexa testimone in un caso di omicidio”*, su *Il tuo legale*, 2019.

G. ZARA, “*Tra il probabile e il certo. La valutazione del rischio di violenza e di recidiva criminale*”, in *Diritto penale contemporaneo*, 20 maggio 2016.

Z. ZENCOVICH, “*The Datasphere, Data flows beyond control and the challenges for law and governance*”, in *European Journal of Comparative Law and Governance*, V, 2019/162.

S. ZUBOFF, “*Big other: surveillance capitalism and the prospects of an information civilization*”, “*Journal of Information Technology*” (2015) 30.

S. ZUBOFF, “*The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*”, London, 2019.

S. ZUBOFF, “*You Are the Object of a Secret Extraction Operation*”, *The New York Times*, 2021.