

## LA VULNERABILITÀ NELL'AMBIENTE DIGITALE E LA PROTEZIONE DELLA LIBERTÀ DEL VOLERE

Di Antonio Gorgoni

| 915

**SOMMARIO:** *1. Manipolazione dell'utente online e vulnerabilità digitale. – 2. I riferimenti normativi della manipolazione e della vulnerabilità. – 3. Gli strumenti tecnologici in grado di sfruttare le vulnerabilità dell'utente online: pubblicità mirata e rilevamento delle emozioni. – 4. Dipendenza digitale e induzione a compiere atti: contro la distorsione della volontà. – 5. La vulnerabilità digitale quale categoria giuridica non riconducibile a figure specifiche di debolezza. – 6. I rimedi rispetto al contratto concluso dall'utente online vulnerabile e manipolato.*

**ABSTRACT.** *Il funzionamento delle tecnologie nell'ambiente digitale al fine di manipolare l'utente online, alterandone la volontà, è una delle ragioni che hanno indotto l'Unione europea a intervenire con una normativa senz'altro utile ma non ancora compiuta. Il potere manipolante capace di far deflagrare le fragilità umane, di tutte le persone e non soltanto dei minorenni o dei disabili, ha imposto di porre al centro della relativa normativa la categoria della vulnerabilità. Vi sono diverse disposizioni del diritto europeo che vi fanno riferimento. Il che esige una riflessione sul suo significato, in parallelo con la diversa linea di policy del codice civile, anche al fine di stabilire i rimedi applicabili qualora il contratto online sia stato concluso sfruttando proprio una condizione di debolezza umana socialmente rilevante.*

*The functioning of technologies in the digital environment in order to manipulate the online user, altering his will, is one of the reasons that have led the European Union to intervene with a regulation that is certainly useful but not yet complete. The manipulative power capable of making human fragility explode, of all people and not only of minors or disabled people, has required placing the category of vulnerability at the center of the relevant legislation. There are several provisions of European law that refer to it. This requires a reflection on its meaning, in parallel with the different policy line of the civil code, also in order to establish the remedies applicable when the online contract has been concluded by exploiting a socially relevant condition of human weakness.*





## 1. Manipolazione dell'utente online e vulnerabilità digitale.

Uno dei rischi maggiori, anzi il più grande, che corre ogni utente nell'«ambiente digitale»<sup>1</sup> è quello di essere manipolato e di acquisire dipendenze comportamentali derivanti dal funzionamento fuorviante e oscuro delle piattaforme online e dalle pratiche di intelligenza artificiale (IA) distorsive del volere<sup>2</sup>.

Questo rischio di alterazione della volontà e finanche, come vedremo, di impossessamento della persona (dipendere da qualcosa, come un algoritmo, significa perdere il controllo di sé), determina conseguenze negative rilevanti di ampia e differente portata: sulla salute e sul patrimonio. La diffusione su vasta scala della manipolazione non solo mina alla radice il principio personalistico euro-unitario, ma anche, e di conseguenza, compromette il funzionamento della Repubblica e la tenuta dello Stato di diritto. Ne è consapevole l'Unione europea, la quale, attraverso la legislazione, ha legato il tema decisivo della salvaguardia della libertà del volere al corretto svolgimento delle democrazie<sup>3</sup> e del mercato

<sup>1</sup> Sintagma, questo, contenuto nell'art. 2 n. 9 direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20.5.2019 «relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali», il quale si riferisce all'«hardware, al software e alle connessioni di rete di cui il consumatore si serve per accedere al contenuto digitale o al servizio digitale o per usarlo». L'ambiente digitale è un nuovo e sconfinato spazio di vita in cui gli individui trascorrono la loro esistenza e compiono atti giuridici, sollecitati dalla tecnologia che si avvale di svariati sistemi per attrarre e determinare la volontà umana.

<sup>2</sup> G. VETTORI, *Persona e pluralismo*, in *Persona e mercato*, 2024, 2, 331; S. ORLANDO, *Consenso al trattamento e liceità*, in *Persona e mercato*, 2024, 2, 347 ss.; N. CRISTIANINI, *La scorciatoia, Come le macchine sono diventate intelligenti senza pensare in modo umano*, Bologna, 2023, 99 ss.; F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori*, in *Contr. e impr.*, 2022, 3, 919 ss.; D. IMBRUGLIA, *La presunzione delle macchine e il consenso dell'interessato*, in *Riv. trim. dir. proc. civ.*, 2023, p. 921 ss.; B.-C HAN, *Infocrazia, Le nostre vite manipolate dalla rete*, Torino, 2021, 30 ss.; S. ZUBOFF, *Il capitalismo della sorveglianza, Il futuro dell'umanità nell'era dei nuovi poteri*, trad. di P. Bassotti, Bologna, 2019, 211 ss.; M. LEISER, *Psychological patterns and article 5 of the AI Act*, in *AIRe*, 2024, 1, 1 ss.; KAWON (KATHY) KIM, WOO GON KIM, MINWOO LEE, *Impact of dark patterns on consumers' perceived fairness and attitude: moderating effects of types of dark patterns, social proof, and moral identity*, in *Tourist management*, ([www.elsevier.com/locate/tourman](http://www.elsevier.com/locate/tourman)), 2023, 1 ss.

<sup>3</sup> Al considerando 69 del regolamento (UE) 2022/2065 «relativo a un mercato interno dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)» - in seguito DSA - si afferma che quando la manipolazione e lo sfruttamento delle vulnerabilità riguarda interi gruppi si amplificano «i danni per la società». Il considerando 104, a proposito della redazione di codici di condotta volontari, sottolinea che «un altro ambito da prendere in considerazione riguarda gli eventuali effetti negativi dei rischi sistemici sulla società e sulla democrazia, quali la disinformazione o le attività di manipolazione e abuso o eventuali effetti avversi sui minori. Ciò comprende operazioni coordinate volte ad amplificare informazioni, compresa la disinformazione, come l'utilizzo di bot o account falsi per la creazione di informazioni intenzionalmente inesatte o fuorvianti, talvolta a scopo di lucro, che sono particolarmente dannose per i destinatari del servizio vulnerabili, quali i minori. In relazione a tali ambiti l'adesione a un determinato codice di condotta e il suo rispetto da parte di una piattaforma online di dimensioni molto

interno<sup>4</sup>.

Le tecnologie operanti nella rete internet, adoperate soprattutto per incrementare i profitti delle imprese e delle multinazionali come Microsoft, Google, Amazon, Meta, Tencent, Netflix, sono predisposte e immesse sul mercato per indurre gli utenti all'acquisto di beni e servizi; un'induzione che fa leva sulla preventiva conoscenza dei loro interessi, gusti e propensioni acquisita tramite il trattamento dei dati personali.

Va sottolineato però che non è illegittimo indurre l'utente-consumatore all'acquisto, aiutarlo nella selezione dei prodotti, facendo comparire sull'interfaccia ciò che maggiormente gli interessa. La pubblicità mirata, ossia quella indirizzata a un determinato utente online, non è vietata [salvo che origini dalla profilazione di dati sensibili di cui all'art. 9 regolamento (UE) 2016/679 sul trattamento e la circolazione dei dati personali, GDPR], ma è assoggettata a determinate regole per evitare lo sfruttamento degli utenti (art. 26 DSA), i quali, nella logica manipolativa, vengono trasformati in mezzi nelle mani altrui.

È vietata la manipolazione della volontà, la quale, per definizione, comporta la perdita dell'autonomia personale, ossia della libertà di scelta.

La tecnologia digitale usufruisce di molti strumenti per depotenziare l'intelletto umano e premere sulla volontà, la quale, più semplicemente dell'intelletto, che è la sede del ragionamento e della valutazione delle circostanze, opera con l'immediatezza del secco «acconsento», «non acconsento»<sup>5</sup>.

---

grandi o di un motore di ricerca online di dimensioni molto grandi possono essere ritenuti una misura di attenuazione dei rischi adeguata» (cfr. anche cons. 106 DSA). Al cons. 1 del regolamento (UE) 2024/1689 «che stabilisce regole armonizzate sull'intelligenza artificiale», pubblicato in Gazzetta ufficiale dell'Unione europea il 12.7.2024 – in seguito AI-Act – si stabilisce che lo scopo di tale di regolamento è di promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione». Cfr. anche i considerando: 2, 8 (in cui si afferma che si garantisce una elevata protezione degli interessi pubblici «quali la salute e la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente»), 27, 28, 61, 62, 176 AI-Act. A questi si legano gli artt. 1 e 74 par. 8 AI-Act.

<sup>4</sup>Assicurare la contendibilità dei mercati contenendo lo strapotere del *gatekeeper* (cioè dell'impresa che diventa punto di accesso per gli utenti commerciali delle piattaforme i quali vorrebbero raggiungere gli utenti finali) è fondamentale per ridurre i rischi oltre che di pratiche scorrette e di aumento dei prezzi anche di manipolazione digitale. Da questo punto di vista fondamentale è il regolamento (UE) 2022/1925 del 14 settembre 2022 «relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)», c.d. DMA. Sulla modifica dell'art. 9 d. lgs. 231/2002 cfr. M. Libertini, *La presunzione di dipendenza economica nei mercati digitali. Un commento all'art. 33 della legge 5 agosto 2022, n. 118*, in *Orizz. dir. comm.*, 2023, 1 (accesso online all'editore).

<sup>5</sup> A. SCHOPENHAUER, *Il primato della volontà*, Milano, 2022, a cura e con un saggio di G. Gurisatti, *passim*, si sofferma sulla distinzione tra volontà (agile nel suo operare, sottratta alla catena causale, espressione del carattere e influenzata dalle emozioni) e intelletto, le cui funzioni «sono tanto molteplici quanto complesse» (p. 53). Afferma il filosofo che «quando l'intelletto mostra alla volontà un semplice dato intuitivo, essa, a seconda che questo le

La manipolazione digitale di cui parliamo è ben diversa dal raggio costitutivo il dolo quale vizio del consenso, perché l'algoritmo, la pratica di intelligenza artificiale (IA) o il funzionamento dell'interfaccia online, se deviati da un funzionamento etico<sup>6</sup>, predispongono non già false realtà, ma determinate realtà che inducono l'utente ad agire in un certo modo: ossia come previsto dal potere tecnologico. Ma più esattamente: chi è l'utente manipolato?

La manipolazione ha due bersagli: potenzialmente tutti gli utenti online (tramite, ad esempio, i *dark patterns*)<sup>7</sup> o, più nello specifico, gli utenti vulnerabili, i quali sono vittime delle loro fragilità, sfruttate dalla tecnologia digitale. E allora occorre chiarire quale sia il concetto giuridico di vulnerabilità nelle fonti del diritto europeo.

La persona vulnerabile può anche sapere che una certa cosa è negativa e per sé pregiudizievole e tuttavia volerla ugualmente. Difficilmente il codice civile protegge questa situazione, almeno sul piano dell'invalidità dell'atto, perché le maglie dell'incapacità naturale (art. 428 c.c.) e dei vizi del consenso (artt. 1427 ss. c.c.) sono piuttosto strette. Ciò è dovuto all'esigenza di contemperare la protezione della libertà del volere con la tutela dell'affidamento e, quindi, della sicurezza della circolazione<sup>8</sup>.

---

vada più o meno a genio, esprime il suo “mi è gradito, non mi è gradito”; e quando il primo, con fatica, ha almanacato e ponderato per riuscire a estrarre, alla fine, da innumerevoli dati e in mezzo a difficili combinazioni, il risultato conforme all'interesse della volontà, essa, che è il sovrano, e che durante questo almanaccare ha riposato oziosa e come assente, non appena il risultato è raggiunto si avvicina, come il sultano nel Divano, ed esprime soltanto il suo monotono “gradito” o “non gradito”. Stante il funzionamento dell'ambiente digitale è la volontà ad essere fortemente sollecitata.

<sup>6</sup> Al cons. 7 del regolamento (UE) 2024/1689 [che «stabilisce regole armonizzate sull'intelligenza artificiale»], c.d. AI-Act] si prevede che le regole comuni sull'IA richiedono di tener conto «degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG)». Al cons. 8 l'Unione europea si propone l'obiettivo di diventare «leader mondiale nello sviluppo di una IA sicura affidabile ed etica. Ugualmente il cons. 165 promuove lo sviluppo di sistemi di IA non ad alto rischio in conformità al regolamento con conseguente adozione nell'Unione «di un'IA etica e affidabile». Cfr. anche: il cons. 27 che indica i sette principi etici non vincolanti per l'IA e la Risoluzione del Parlamento europeo del 20 ottobre 2020 «recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate».

<sup>7</sup> Un «*dark pattern*» è un design o una pratica di interfaccia che frutta soprattutto la psicologia o perpetra un inganno per indurre gli utenti a compiere azioni che, in un contesto digitale corretto, informato e obiettivo, non avrebbero altrimenti posto in essere. Questi schemi sono utilizzati in ambiti commerciali attivi nei siti web o nelle app, per massimizzare i profitti, attirare abbonamenti indesiderati o raccogliere dati personali per diverse finalità, tra cui quella di profilare e targettizzare. I «*dark patterns*» si manifestano in diverse forme come, a titolo esemplificativo e non esaustivo: nascondere e confondere informazioni o opzioni significative o presentarle in modo poco chiaro; presentare una falsa urgenza affermando che un'offerta è di prossima scadenza per indurre gli utenti ad assumere decisioni frettolose; adottare una impostazione predefinita ingannevole, ossia *opt-in* automatici per servizi o comunicazioni che gli utenti non desiderano; approntare difficoltà di cancellazione, rendendo cioè complicato o frustrante il processo di eliminazione di un servizio o di una sottoscrizione.

<sup>8</sup> V. PIETROBON, *Errore, volontà e affidamento*, Padova, 1990, 69 ss., si sofferma ampiamente sul principio dell'affidamento come temperamento al principio volontaristico.

Nell'ambiente online, però, opera un potere più incisivo sulla psicologia della persona<sup>9</sup>; tutto è più veloce e si svolge nella solitudine del rapporto con la macchina, senza l'incidenza di quelle spinte e contropinte, pesi e contrappesi che connotano il rapporto tra due persone in dialogo tra loro faccia a faccia. Nel contesto online è più agevole indurre a compiere un atto; ma se questo agire dipende dalla distorsione della volontà di un utente *compos sui* o affetto da una qualche fragilità, con conseguente danno alla persona, l'atto compiuto deve essere qualificato negativamente.

Insomma la manipolazione digitale si dirige in una duplice direzione: vuole etero-dirigere nella manifestazione di volontà *tutti* i possibili utenti online<sup>10</sup>; si concentra sull'individuazione e sul conseguente sfruttamento di quelle particolari fragilità emerse durante la navigazione nella rete internet. Vedremo, infatti, che le fonti del diritto europeo distinguono la manipolazione in generale dallo sfruttamento delle vulnerabilità, dedotte e categorizzate dall' algoritmo, degli utenti online.

## 2. I riferimenti normativi della manipolazione e della vulnerabilità.

L'ambiente digitale, in ragione del suo funzionamento e della solitudine dell'individuo, costituisce un terreno fertile per la distorsione della volontà. Le diverse tecniche idonee a catturare l'attenzione dell'utente, spingendolo a rimanere online il più a lungo possibile, e le fragilità connaturate a ogni essere umano hanno reso indispensabile l'emanazione di una normativa volta a salvaguardare la libertà decisionale della persona che opera nel contesto digitale.

Si possono richiamare alcuni articoli incentrati sulla manipolazione in generale e su quella indirizzata nei confronti degli utenti vulnerabili:

- art. 25 regolamento (UE) 2022/2065 [«relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)» c.d. DSA], sulla «progettazione e organizzazione delle interfacce online». Esso stabilisce che «i fornitori di piattaforme online non progettano, organizzano o gestiscono le loro interfacce online in modo tale da *ingannare* o *manipolare* i destinatari dei loro servizi o da *materialmente falsare* o *compromettere altrimenti* la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate»<sup>11</sup>;

- art. 5, par. 1 lett. a), AI-Act (sulle «pratiche di IA vietate»): è vietata l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza *tecniche subliminali* che agiscono senza che una persona ne sia

---

Non va certo negato rilievo alla volontà, ma solo sottolineato che quest'ultima non ha valore assoluto.

<sup>9</sup> O. POLLICINO, *Potere digitale* (voce), in *Enc. dir. (I Tematici)*, diretto da M. Cartabia e M. Ruotolo, Milano, 2023, V, 410 ss.; ivi G. RESTA, *Poteri privati e regolazione*, 1008 ss.

<sup>10</sup> P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo europeo delle fonti*, Napoli, 2020, 40 ss., in cui si ragiona di tutela più che del consumatore del contraente debole secondo le diverse declinazioni dell'ordinamento. In argomento G. VETTORI, *Il contratto senza numeri e aggettivi. Oltre il consumatore e l'impresa debole*, in *Persona e mercato*, 2013, 1, 10 ss.

<sup>11</sup> Si aggiungano i riferimenti alla vulnerabilità nei considerando 62, 69, 94, 95, 104 DSA.

consapevole o tecniche *volutamente manipolative o ingannevoli* aventi lo scopo o l'effetto di *distorcere materialmente il comportamento* di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a *prendere una decisione che non avrebbero altrimenti preso*, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo»;

- art. 5, par. 1 lett. b), AI-Act: è altresì vietata l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che *sfrutta le vulnerabilità* di una persona fisica o di uno specifico gruppo di persone, dovute all'*età*, alla *disabilità* o a una *specifica situazione sociale o economica*, con l'obiettivo o l'effetto di *distorcere materialmente il comportamento* di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo»;

- art. 7, par. 2 lett. h), AI-Act in cui, con riguardo al potere della Commissione europea di modificare l'allegato III (sui «sistemi di IA ad alto rischio di cui all'art. 6, paragrafo 2)), si stabilisce che, nel valutare la condizione di cui al paragrafo 1 lett. b) (ossia la presenza di un rischio di danno per la salute e la sicurezza o di un impatto negativo sui diritti fondamentali), la Commissione tiene conto « [del]la misura in cui esiste uno squilibrio di potere o [del]le persone che potrebbero subire il danno o l'impatto negativo [e che] si trovano in una *posizione vulnerabile* rispetto al deployer di un sistema di IA, in particolare a causa della *condizione*, dell'*autorità*, della *conoscenza*, della *situazione economica o sociale* o dell'*età*»;

- art. 9, par. 9, AI-Act, in cui, rispetto all'obbligo di istituire, attuare e documentare un sistema di gestione dei rischi (previsto anche dal DSA), si afferma che «nell'attuare il sistema di gestione dei rischi di cui ai paragrafi da 1 a 7, i fornitori prestano attenzione, nell'ottica della sua finalità prevista, all'eventualità che il sistema di IA ad alto rischio possa avere un impatto negativo sulle persone di età inferiore a 18 anni o, a seconda dei casi, su altri *gruppi vulnerabili*»<sup>12</sup>.

A queste disposizioni specifiche occorre aggiungerne altre, di contenuto più ampio, la cui finalità è di salvaguardare la libertà del volere dell'utente online, soprattutto di quello vulnerabile.

<sup>12</sup> Tra gli altri riferimenti normativi alla vulnerabilità cfr. anche i cons.: 29 (dove tra le condizioni di vulnerabilità vengono indicate, tra l'altro, la «specifica situazione sociale ed economica», la «povertà estrema» e l'essere minoranza etnica o religiosa), 48, 58 (in cui, rispetto all'utilizzo di sistemi di IA, si riconduce alla vulnerabilità il bisogno di servizi essenziali di assistenza pubblica legato alla maternità, alla malattia, agli infortuni sul lavoro, alla dipendenza, alla vecchiaia, alla perdita del lavoro e alla necessità di un alloggio), 60 (sull'utilizzo dei sistemi di IA rispetto al settore della migrazione, dell'asilo e della gestione del controllo delle frontiere), 67, 93, 110 (in cui si parla di modelli di IA per finalità generali e rischi sistemici tra cui quello di scoprire e sfruttare le vulnerabilità degli utenti), 132, 141, 165, e gli artt. 60, par. 4 lett. g), 79 par. 2 (in cui si fa riferimento ai sistemi di IA «che presentano un rischio per i gruppi di persone vulnerabili di cui all'art. 5») e 95, par. 2 lett. e) AI-Act.

L'art. 34 DSA, nell'imporre ai fornitori di piattaforme online (e di motori di ricerca) molto grandi di valutare gli «eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio o dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi», indica tra siffatti rischi quelli che interessano «l'esercizio dei diritti fondamentali», tra cui vanno ricompresi la capacità autodeterminarsi (artt. 1, 6 e 7 CDFUE), la «salute pubblica e dei minori» e il «benessere fisico e mentale della persona».

Alla protezione online dei minorenni, l'art. 28 DSA dedica disposizioni specifiche. Una più generale, al paragrafo 1, in cui si stabilisce che i fornitori di piattaforme online accessibili ai minori devono adottare «misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio»; un'altra più specifica, al paragrafo 2, in cui si pone il divieto di presentare sulla interfaccia pubblicità basata sulla profilazione se si ha la «ragionevole [non già l'assoluta] certezza» che il destinatario del servizio è minore. Si aggiungano i considerando 38, 58, 65, 71 e gli artt. 6 par. 1 lett. f), 8 e 40 par. 2 lett. g) del GDPR.

Oltre all'AI-Act e al DSA occorre richiamare la Convenzione quadro del Consiglio d'Europa «sull'intelligenza artificiale e sui diritti umani, la democrazia e lo Stato di diritto». È la prima Convenzione di diritto internazionale<sup>13</sup>, il cui scopo è vincolare gli Stati Parte ad adottare misure legislative, amministrative o di altro tipo funzionali ad assicurare la coerenza dell'intero ciclo di vita dei sistemi di IA con i diritti umani, la democrazia e lo Stato di diritto (art. 1)<sup>14</sup>. È significativo che in un mondo in cui la vita umana e l'economia si svolgono sempre più online, anche gli Stati siano obbligati ad adottare misure idonee a governare il cambiamento, assicurando opportunità a tutti e salvaguardando l'autonomia e la libertà individuale.

Non è un risultato scontato, infatti già nel Preambolo si esplicita la preoccupazione che alcune attività dei sistemi di IA «possano minare l'autonomia individuale» e aggravare il rischio di discriminazioni e disuguaglianze soprattutto rispetto agli «individui in situazioni di vulnerabilità». Coerentemente: l'art. 7, contenuto nel capo III sui principi, obbliga gli Stati parte ad adottare o mantenere misure «per il rispetto della dignità umana e dell'*autonomia individuale* in relazione alle attività del

<sup>13</sup> La firma della Convenzione è avvenuta a Vilnius (Lituania) durante la conferenza dei ministri della Giustizia del Consiglio d'Europa. Tra i primi firmatari ci sono l'Unione europea, gli Stati Uniti d'America, il Canada, il Regno Unito e alcuni paesi membri del Consiglio d'Europa. Ai sensi dell'art. 30, la Convenzione è aperta alla firma degli Stati membri del Consiglio d'Europa che ancora non l'hanno sottoscritta (tra cui l'Italia) e all'adesione di qualsiasi Stato non membro del Consiglio d'Europa ai sensi dell'art. 31.

<sup>14</sup> L'art. 3 della Convenzione, da un lato, assoggetta ciascuna Parte ad applicare le disposizioni della Convenzione «alle attività svolte nell'ambito del ciclo di vita dei sistemi di intelligenza artificiale dalle autorità pubbliche o da soggetti privati che agiscano per conto loro»; dall'altro, impone a ciascuna Parte di «affronta[re] i rischi e gli impatti derivanti dalle attività svolte nell'ambito del ciclo di vita dei sistemi di intelligenza artificiale da parte di soggetti privati (...)». Il modo di attuazione di tale obbligo dovrà essere specificato in un'apposita dichiarazione presentata al Segretario generale del Consiglio d'Europa al momento della firma o del deposito dello strumento di ratifica.



ciclo di vita dei sistemi di intelligenza artificiale<sup>15</sup>; l'art. 18, all'interno del capo VI sull'attuazione della Convenzione, obbliga gli Stati parte a tenere conto di «esigenze e vulnerabilità specifiche in relazione al rispetto dei diritti delle persone con disabilità e dei bambini».

Tutte queste disposizioni suscitano almeno due considerazioni. La prima attiene alla fattispecie, che si delinea con una certa nettezza, del divieto di manipolazione dell'utente online. Su essa non ci si può qui soffermare organicamente, stante l'ampiezza della trattazione; basti rilevare come le espressioni e i termini «tecniche subliminali che agiscono senza che una persona ne sia consapevole», «manipolazione» e «materialmente falsare o compromettere altrimenti» la libertà del volere oltrepassano le fattispecie dei vizi del consenso (errore, violenza e dolo) e le pratiche commerciali scorrette<sup>16</sup>.

La seconda considerazione riguarda la categoria della vulnerabilità, accolta dalle fonti europee in luogo della specificità e tipizzazione delle condizioni soggettive di debolezza umana giuridicamente rilevanti. Su essa ci si soffermerà ed emergerà un'impostazione ordinamentale molto diversa da quella del codice civile, la quale è stata più attenta a circoscrivere con puntualità le condizioni soggettive di debolezza rilevanti, laddove il diritto europeo, stante l'evoluzione sociale e tecnologica, ha aperto maggiormente al rilievo delle plurime e non predeterminabili fragilità umane.

È utile però, prima di sviluppare questo tema, svolgere due passaggi intermedi, attinenti: 1) all'individuazione degli strumenti attraverso cui può essere effettuato lo sfruttamento delle vulnerabilità; 2) a una più precisa delimitazione del problema della manipolazione, da cui scaturisce l'esigenza normativa di accogliere il concetto di vulnerabilità digitale.

### 3. Gli strumenti tecnologici in grado di sfruttare le vulnerabilità dell'utente online: pubblicità mirata e rilevamento delle emozioni.

Da sempre alle imprese interessa conoscere i gusti dei consumatori e acquisire la loro fiducia; è noto, infatti, che il marketing risale al tempo anteriore all'avvento di internet. Esso si basava su strategie attuate prima della produzione dei beni, ma soprattutto su svariate tecniche volte ad indurre i consumatori ad acquistare i prodotti già immessi sul mercato<sup>17</sup>.

<sup>15</sup> Le misure a tutela dei diritti umani, della democrazia e dello Stato di diritto devono essere individuate dagli Stati parte (artt. 7-12 Conv.) e, ove accorra, aggiornate. In forza dell'art. 16 co. 1, in linea con quanto previsto dal DSA e dall'AI-Act, ciascuna Parte deve «adottare o mantenere in vigore misure per l'identificazione, la valutazione, la prevenzione e l'attenuazione dei rischi posti dai sistemi di intelligenza artificiale (...)».

<sup>16</sup> Su questo tema mi permetto di rinviare a un altro scritto in corso di ultimazione.

<sup>17</sup> Sulla storia del marketing cfr: P. KOTLER-K.L. KELLER, *Marketing management*, a cura di W G. Scott, trad. it. di F. Sarpi, Milano, 12 ed., 2007. Questo volume, ebbene sia un manuale di marketing, è un testo fondamentale che include una sezione sulla storia e l'evoluzione del marketing; Più di recente P. KOTLER-K.L. KELLER-F. ANCARANI-M. COSTABILE, *Marketing management*, Pearson Italia, 2012; R.S. WINER-S.A. NESLIN, *The history of marketing science*, Word Scientific, 2014, *passim*. In estrema sintesi si possono

Quando si afferma e dilaga la dimensione online dell'esistenza umana, nella quale si è attratti dal palesare sé stessi agli altri, oltre alla diffusione dell'economia dei dati personali e al crescente perfezionamento delle tecnologie digitali, il marketing assume un tratto spiccatamente prognostico. Le imprese, attraverso l'impossessamento dei dati della navigazione online e la valorizzazione di ciò che da essi è desumibile con riguardo agli interessi e alle propensioni degli utenti, sempre più indirizzano pubblicità mirate, offrendo quel prodotto che piace o di cui – lo si sa già – ha bisogno l'utente-consumatore.

Naturalmente – è bene sottolinearlo – non vi è alcuna antiggiuridicità nell'offrire ciò che soddisfa la domanda di beni, sebbene tale domanda sia conosciuta dalle imprese prima che essa venga formulata. La qualificazione negativa dell'atto di consumo si appunta sulla mancanza di libertà del volere e non già nel volere conforme all'esercizio della propria autonomia negoziale fosse anche stimolata. Certo, talvolta il confine è sottile, perché il fenomeno della dipendenza comportamentale, come si dirà meglio nel paragrafo successivo, è subdolo nella sua scaturigine e difficile da scorgere soprattutto da parte di chi ne è vittima<sup>18</sup>.

Se la pubblicità mirata non è vietata dal diritto europeo, bensì assoggettata a una disciplina volta a salvaguardare la libertà del volere (art. 26 DSA)<sup>19</sup>, è utile indicare, sebbene siano noti, gli strumenti attraverso cui l'utente online può essere indotto a compiere un atto giuridico.

---

ricordare alcuni aspetti funzionali al nostro discorso sulla vulnerabilità e manipolazione. Prima dell'avvento della tecnologia digitale, le indagini di marketing erano basate su approcci più tradizionali e meno personalizzati. Le imprese conducevano soprattutto ricerche di mercato attraverso sondaggi, interviste e *focus group* per raccogliere opinioni e preferenze. Queste ricerche erano, tuttavia, meno frequenti perché costose. Piuttosto le aziende si concentravano su altre strategie: 1) implementavano promozioni e sconti, campioni gratuiti e offerte speciali per incentivare le vendite; 2) *branding*, ossia si puntava sullo sviluppo del marchio e sull'immagine dell'azienda. Lo scopo era di creare un'identità forte e riconoscibile attraverso loghi, slogan e campagne pubblicitarie coerenti; 3) *networking* e relazioni, ossia le aziende investivano nella costruzione di relazioni personali con i clienti importanti e i partner commerciali, spesso attraverso eventi dal vivo, fiere e conferenze; 4) distribuzione e posizionamento consistente nella scelta dei punti vendita nei luoghi giusti per massimizzare la visibilità e le vendite.

Queste e altre tecniche, ancora oggi utilizzate, erano decisamente meno mirate e personalizzate rispetto a quelle attuali, essendo volte a conquistare la fiducia del cliente senza conoscerne preventivamente i gusti. Nel passato del marketing occorreva creatività e intuizione per cercare di capire e anticipare i bisogni e i desideri dei consumatori. Oggi i bisogni e i desideri sono palesati nell'ambiente digitale, dove la tecnologia che vi opera riesce anche a far nascere interessi e desideri, spingendo all'acquisto. Rispetto a questo potere delle imprese e di chi adopera certe tecnologie digitali, diventa sottile il confine tra soddisfacimento della domanda, induzione al consumo e manipolazione dell'utente-consumatore.

<sup>18</sup> Anche da questo punto di vista si constata come sia più semplice accorgersi di essere stati vittima di un raggio piuttosto che di aver sviluppato una dipendenza comportamentale nell'ambiente digitale in cui operano spinte costanti e silenziose.

<sup>19</sup> L'art. 26 («pubblicità sulle piattaforme online») – parte della sezione 3 («disposizioni applicabili ai fornitori di piattaforme online») del capo III («Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro») il quale detta obblighi generali, variamente distribuiti tra i prestatori di servizi intermediari (sezioni 1) e i fornitori di piattaforme online o applicabili a entrambi (2) – obbliga i fornitori di piattaforme online

Il trittico su cui far leva per approfittare della vulnerabilità dell'utente è il seguente: consenso al trattamento dei dati personali, profilazione e *targeting*<sup>20</sup>. Il primo è un elemento delicatissimo, perché attraverso il consenso si consente l'intromissione nella propria vita privata, esponendosi, di conseguenza, anche a pregiudizi arrecati a sé stessi da chi intenda sfruttare la conoscenza di elementi personali significativi. Ecco perché il GDPR, diversamente dal codice civile (art. 1322 e artt. 1426-1440 c.c.), insiste maggiormente e in diverse direzioni sul consenso negoziale.

Ai sensi dell'art. 4, n. 11 GDPR, il consenso dell'interessato è definito come «qualsiasi manifestazione di volontà *libera, specifica, informata, inequivocabile* (...), con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile», a che i dati personali che lo riguardano siano oggetto di trattamento». Questa disposizione si inverte in diversi articoli, la cui finalità è di garantire la consapevolezza e spontaneità del consenso [art. 6 par. 1 lett. a), art. 7, in part. il par. 4 e art. 13 GDPR sui doveri di informazione in capo al titolare del trattamento una volta ottenuti i dati]<sup>21</sup>.

che presentano pubblicità sulle loro interfacce *a rendere alcune informazioni* «per ogni singola pubblicità presentata a ogni singolo destinatario». Tra queste informazioni merita una particolare sottolineatura quella di cui alla lett. d) del paragrafo 1, attinente sia ai «parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità» e, se praticabile, sia «alle modalità di modifica di detti parametri». Qual è la finalità di queste disposizioni? Affinché l'utente non sia strumentalizzato/manipolato nella manifestazione del consenso, egli deve conoscere gli elementi considerati dalla macchina per raggiungerlo con una pubblicità. Questa conoscenza è essenziale per consentire all'utente di valutare le ragioni della proposta commerciale e, quindi, per decidere se acquistare o meno il prodotto oggetto della pubblicità mirata. Altrimenti, in assenza di tali disposizioni, la volontà dell'utente-consumatore rischierebbe di essere etero-diretta dall'algoritmo, non libera, tale per cui la persona degrada dall'essere un valore intrinseco a strumento per raggiungere un obiettivo economico a prescindere dalle sue reali esigenze e dal suo benessere psichico. Ecco perché l'utente, dopo aver valutato le ragioni della intromissione nella propria vita attraverso l'invio della pubblicità, deve, possibilmente, essere in grado di modificare quei parametri, così da determinare un adeguamento dell'offerta commerciale ai suoi effettivi interessi e bisogni. Analogamente si articola la disciplina sulla trasparenza dei sistemi di raccomandazione [(art. 27 DSA), cfr. R. MONTINARO, *Sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)*, in *Persona e mercato*, 2022, 3, p. 368 ss.].

<sup>20</sup> V. RICCIUTO, *Consenso al trattamento e contratto*, in corso di pubblic.; D. PAOLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, 2783 ss.; V. ZENO-ZENCOVICH, G. RESTA, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2018, p. 432 ss.; G. COMANDÈ, *Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems and Opportunities of Algorithms*, in T. Cerquitelli, D. Quercia, F. Pasquale (eds.), *Transparent Data Mining for Small and Big Data* (Basel: Springer, 2017), 169 ss.; S. TOMMASI, *Verso il Digital Services Act: la Proposta di Regolamento sul "mercato unico dei servizi digitali" del 15.12.2020*, in *Persona e mercato*, 2021, 1, 215 ss.

<sup>21</sup> Dal considerando 32 GDPR emergono due aspetti fondamentali del consenso: 1) la sua forma a garanzia della consapevolezza del proprio atto; 2) lo stretto legame con la finalità per la quale è espresso (per una limpida e convincente trattazione del consenso al trattamento dei dati personali e del suo rapporto con il bene servizio ottenuto cfr. V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, *passim*, cfr. anche: G. FINOCCHIARO, *Intelligenza artificiale quale regole?*, Bologna, 2024, p. 87 ss., sul superamento della logica proprietaria dei dati personali, e S. ORLANDO, *Consenso al*



La profilazione, invece, rende edotto il titolare del trattamento di plurimi aspetti, esteriori e interiori, riguardanti l'interessato. La definizione di questo termine, contenuta nell'art. 4, n. 4, GDPR, restituisce tutta l'ampiezza dell'ambito di intrusione nella vita privata della persona mediante l'impiego della tecnologia digitale. Per profilazione si intende «qualsia forma di trattamento automatizzato di dati personali consistenti nell'utilizzo di tali dati personali per *valutare determinati aspetti personali* relativi a una persona fisica, in particolare per *analizzare e prevedere* aspetti riguardanti il rendimento professionale, la situazione economica, la salute, *le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*». Si tratta, dunque, di una tecnica attraverso cui, sulla base di una valutazione automatica dei dati personali, si conoscono molte cose di una persona («aspetti personali»), al punto da poterne anche prevedere le «preferenze personali» e «il comportamento».

I dati personali, va precisato, possono essere forniti alla registrazione, osservati, attraverso diverse tecniche<sup>22</sup> o desunti. Lo scopo è di acquisire

---

*trattamento e liceità, in Persona e mercato, 2024, 2, 361 ss., espone l'idea secondo cui l'autonomia privata nel campo dei dati personali va intesa come «un potenziamento della tutela della persona».* Si riporta per comodità di lettura il testo: «il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione *libera, specifica, informata e inequivocabile* di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

<sup>22</sup> Tra queste tecniche o attività si indicano, in sintesi e senza pretesa di esaustività, le seguenti: a) il tracciamento delle attività che avviene mediante i cookies e altre tecnologie di tracciamento con cui il titolare del trattamento monitora il comportamento dell'utente sulla piattaforma. Ad esempio si verifica quali pagine vengono visitate, per quanto tempo e come si interagisce con i contenuti; b) l'analisi dei contenuti consiste nell'esame delle interazioni con i contenuti, appunto; interazioni quali sono i commenti e le risposte, i quali, nel loro insieme, possono fornire utili informazioni, a fini diversi (soprattutto economici dell'impresa), sui gusti, interessi e opinioni dell'utente; c) l'indicazione dei dati demografici, solitamente forniti dagli utenti durante la registrazione (come età, sesso, localizzazione), è utilizzabile per creare profili e segmentare gli utenti; d) l'utilizzo di reti sociali fa sì che il titolare del trattamento possa accedere a informazioni aggiuntive dal profilo dell'utente, come amici, interessi e attività; e) propinare sondaggi e questionari all'utente serve anch'esso a raccogliere informazioni su opinioni e preferenze; f) anche l'attività offline, riguardante ad esempio gli acquisti effettuati in negozio, combinata con quella online contribuisce a costruire un profilo più completo dell'utente; g) la *machine learning* e l'intelligenza artificiale, attraverso algoritmi di *machine learning*, analizzano per i titolari del trattamento grandi volumi di dati al fine di estrarre informazioni comportamentali e caratteriali. Sulle diverse distinzioni tra i dati cfr. S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, in *Nuovo dir. civ.*, 2022, 4, 27, il quale distingue tra

quante più informazioni possibili su quegli interessi e preferenze degli utenti, pregni di valore economico per le imprese.

Sulla base di questa conoscenza, ogni singolo utente può essere raggiunto con un'offerta personalizzata, rispondente ai propri gusti, attraverso il *targeting*. Con tale termine si intende «l'atto di indirizzare o rivolgere qualcosa a un particolare gruppo di persone» o come «l'atto di tentare di attrarre una persona o un gruppo o di influenzarli in qualche modo» sulla base di una conoscenza pregressa<sup>23</sup>.

Questa pratica reca con sé almeno due rischi: il primo attiene al mancato controllo dei propri dati personali. È stato rilevato che «le attività di profilazione collegate al *targeting* potrebbero comportare un'inferenza di interessi o altre caratteristiche, che la persona non aveva attivamente rivelato, minando così la capacità di quest'ultima di esercitare il controllo sui suoi dati personali»<sup>24</sup>. Il secondo, collegato al primo, che ci interessa di più, attiene alla possibilità di manipolare gli utenti-consumatori quanto alle loro decisioni di acquisto. Difatti alcuni approcci di *targeting* sono in grado di minare l'autonomia e la libertà del volere<sup>25</sup>, sfruttando la conoscenza acquisita di vulnerabilità dell'utente emerse durante la navigazione o già all'atto della registrazione effettuata per fruire di un servizio.

Il problema dello sfruttamento delle fragilità è particolarmente delicato, come si è accennato, per i minori di età; ne è consapevole l'Unione europea, la quale, tra le diverse regole a tutela dei minorenni, ne prevede una particolarmente significativa secondo cui «i fornitori di piattaforme online non presentano sulla loro interfaccia pubblicità basata sulla profilazione come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore» (art. 28, par. 2, DSA).

È vietato profilare i minori di età e inviare loro sull'interfaccia online pubblicità mirata, perché è noto che la loro volontà è altamente influenzabile, come si afferma nella Risoluzione del Parlamento europeo sulla protezione dei consumatori nei videogiochi online, in cui si invoca una

---

dati personali e informazioni quali forme rappresentative dei dati. Sono queste ultime ad interessare maggiormente i professionisti, costituendo la base delle strategie di marketing.

<sup>23</sup> È questa la definizione di *targeting* contenuta nelle Linee guida 8/2020 «sul *targeting* degli utenti di social media» adottate il 13 aprile 2021 dal Comitato europeo per la protezione dei dati (EDPB)», in [www.edpb.europa.eu](http://www.edpb.europa.eu). Il *targeting* degli utenti di social media coinvolge soggetti diversi: i fornitori di social media, i loro utenti, i *targeter* e altri soggetti (come gli intermediari dei dati). Il fornitore di social media può raccogliere una grande quantità di dati personali; si pensi anche soltanto ad un "mi piace" cliccato su un post sui social-media o alla visione di un video. Il *targeter* è la persona fisica o giuridica che utilizza i servizi di social-media per indirizzare messaggi specifici – commerciali, politici o di altro tipo - a un insieme di utenti di social-media sulla base di parametri o criteri specifici. Gli intermediari dei dati e i fornitori di gestione dei dati aggregano i dati raccolti da un'ampia varietà di fonti; dati che possono essere venduti ad altre parti interessate, coinvolte nel processo di *targeting*.

<sup>24</sup> Linee guida EDPB, 8/2020 «sul *targeting* degli utenti di social media», cit.

<sup>25</sup> G. FINOCCHIARO, *Intelligenza artificiale quale regole?*, cit., 47, sottolinea l'importanza del rispetto da parte dei sistemi di IA dei valori dell'UE tra cui la dignità umana e l'autonomia personale, il che giustifica «l'intervento e la sorveglianza umana».

particolare attenzione ai minorenni, i quali hanno diritto di giocare online, ma in sicurezza, in un tempo contenuto e nella consapevolezza dei rischi<sup>26</sup>.

Senza questo divieto di profilare i minorenni, si sarebbe consentito alle imprese di impadronirsi della volontà di un soggetto che è strutturalmente vulnerabile e incline alla decisione impulsiva. Vedremo, però, che la minore età è solo una delle vulnerabilità disciplinate dal diritto europeo. Se il minorenne va protetto perché non ha ancora raggiunto un livello sufficiente di maturazione e di autocontrollo, l'utente maggiorenne, più o meno giovane, si trova comunque anch'egli in una condizione di vulnerabilità, di particolare esposizione al pregiudizio, se la tecnologia digitale lo manipola, finanche traendo indicazioni dalle sue emozioni.

Il rilevamento delle emozioni non è vietato in assoluto<sup>27</sup>. Stabilisce, infatti, l'art. 5, par. 1 lett. f), AI-Act che è vietata l'immissione sul mercato o l'uso «di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del *luogo di lavoro* e degli *istituti di istruzione*, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza». Al di fuori di questi contesti (luogo di lavoro e istituti di istruzione), è legittimo rilevare le emozioni e anche le «intenzioni» (art. 3 n. 39 AI-Act) dell'utente durante la navigazione in internet<sup>28</sup>. Credo, però, che si debba convenire su un aspetto: se la conoscenza delle emozioni di una persona (gioia, rabbia, disgusto, ansia, felicità, confusione) e la comprensione scientifica del funzionamento del cervello possono servire come base dei profitti commerciali

<sup>26</sup> Nella Risoluzione del Parlamento europeo del 18.1.2023 sulla «protezione dei consumatori nei videogiochi online: un approccio a livello del mercato unico europeo», in [www.europarl.europa.eu](http://www.europarl.europa.eu), al punto 36 il Parlamento europeo «evidenzia che l'industria dei videogiochi, gli utenti e i genitori non dovrebbero sottovalutare i rischi e gli effetti dovuti al disturbo da gioco; ricorda che la ricerca scientifica ha dimostrato che la pubertà e l'adolescenza sono i periodi della vita in cui le persone sono più vulnerabili ai comportamenti di assuefazione; chiede una maggiore collaborazione tra i progettisti di videogiochi, gli editori, le piattaforme e la più vasta comunità di soggetti interessati, comprese le autorità nazionali e la Commissione, per contribuire a mitigare il rischio di disturbo da gioco; indica che sarebbe opportuno avviare un maggior numero di campagne di sensibilizzazione per garantire che i genitori e i giovani giocatori siano consapevoli dei rischi connessi al disturbo da gioco e invita gli sviluppatori a evitare la progettazione di giochi manipolativa, che può portare alla dipendenza dal gioco, all'isolamento e a molestie online». Cfr. anche la lettera M) e i nn. 15, 17, 19, 29 e 45.

<sup>27</sup> Per un approfondimento cfr. E.M. INCUTTI, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata*, in *Giust. civ.*, 2022, 2, 519 ss.

<sup>28</sup> Il considerando 18 AI-Act indica la nozione di sistema di riconoscimento delle emozioni, da definirsi come «un sistema di IA finalizzato a *identificare o inferire emozioni o intenzioni di persone fisiche*, sulla base dei loro dati biometrici. La nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. Non comprende stati fisici, quali dolore o affaticamento, compresi, ad esempio, i sistemi utilizzati per rilevare lo stato di affaticamento dei piloti o dei conducenti professionisti al fine di prevenire gli incidenti. Non comprende neppure la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni. Tali espressioni possono essere espressioni facciali di base quali un aggrottamento delle sopracciglia o un sorriso, gesti quali il movimento di mani, braccia o testa, o caratteristiche della voce di una persona, ad esempio una voce alta o un sussurro».

(neuromarketing)<sup>29</sup>, si determina una manipolazione della volontà della persona.

La libertà del volere esige che il comportamento del proprio interlocutore, uomo o macchina che sia, si formi spontaneamente durante la relazione alla pari con l'altro. Se, invece, si conoscono *a priori* circostanze fondamentali attinenti alla sfera altrui, poiché, in ragione di ciò, si è in grado di orientare il proprio comportamento all'insaputa dell'altro, si ha indiscutibilmente una manipolazione. Ecco perché l'art. 50, par. 3, AI-Act stabilisce che «i deployer di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica<sup>30</sup> informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema e trattano i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 a seconda dei casi». Gli utenti devono ricevere una notifica quando sono esposti a sistemi che, nel trattamento dei loro dati biometrici, possono identificare o inferire emozioni o intenzioni o assegnarli a specifiche categorie. Nell'attuare tale obbligo da parte di chi adopera il sistema di IA deve essere riservata una particolare attenzione ai minorenni e ai disabili, considerati soggetti vulnerabili (cons. 132 AI-Act).

Si aggiunga, in coerenza con tale quadro normativo, che i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni sono considerati, giustamente, ad alto rischio [allegato III, n. 1 lett. c), AI-Act]<sup>31</sup>.

<sup>29</sup> E. TUCCARI, *Neuromarketing: un'asistematica disciplina... oltre il consenso?*, in *Persona e mercato*, 2024, 2, 511 ss.; ivi B. PARENZO, *Neuromarketing: un inventario di (spuntati) divieti contro il pericolo di una scelta manipolata*, p. 539 ss.; R. ALFONSI, *Neuromarketing, vizi del consenso e libertà di scelta*, in corso di pubblic, in un volume a cura di S. Orlando ed ivi anche L. CASALINI-E.M. INCUTTI, *Volontà e vulnerabilità in ambiente digitale: profili giuridici del neuromarketing*, A. A. MOLLO, *Emozioni e autodeterminazione in ambiente digitale: prime riflessioni sull'affect recognition e il neuromarketing relativi alle persone con disabilità* e S. TOMMASI, *Neuromarketing discriminatorio e mercato digitale: il ruolo del Digital Services Act e dell'Artificial Intelligence Act*. Cfr. anche L. TAFARO, *Neuromarketing e tutela del consenso*, Napoli, 2018.

<sup>30</sup> L'identificazione biometrica consente di individuare le emozioni dell'utente online perché riconosce in modo automatico, secondo la definizione contenuta nel considerando 15 dell'AI-Act, le «caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia [*id est*: le caratteristiche intonative, ritmiche e melodiche del linguaggio parlato, il che può consentire di scorgere l'emozione dell'oratore], l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità della persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso» (cfr. anche art. 3 nn. 34-36 AI-Act). Ora, i dati biometrici, ottenuti da un trattamento specifico attinente alle caratteristiche fisiche, fisiologiche o comportamentali di una persona, possono essere sfruttati in vari modi, alcuni certamente di grande utilità (come l'autenticazione degli utenti nei sistemi online, tecnica più sicura rispetto alle password); tuttavia, le informazioni biometriche si prestano a costituire la base della creazione di profili dettagliati degli utenti, da sfruttare per la pubblicità mirata o altre forme di manipolazione commerciale.

<sup>31</sup> I sistemi di riconoscimento delle emozioni sono ad alto rischio anche perché, come rilevato dal considerando 44 AI-Act, è difficile trarre dalle emozioni elementi di generalità esatti. Non fosse altro perché «l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona». E allora questi sistemi

Si deve ammettere, dunque, che attraverso il riconoscimento delle emozioni o la profilazione dell'utente mediante i suoi dati biometrici è possibile perpetrare una manipolazione psicologica e approfittare delle vulnerabilità, influenzando le decisioni. Il che avviene attraverso suggerimenti di contenuti, raccomandazioni e offerte di prodotti, il tutto dipendente da una valutazione automatica degli stati d'animo o stati fisiologici dell'utente.

**4. Dipendenza digitale e induzione a compiere atti: contro la distorsione della volontà.**

Il secondo passaggio intermedio del discorso attiene, come si diceva sopra, a una più chiara enucleazione del fenomeno manipolativo che è alla base della nozione di vulnerabilità, intesa in senso ampio; più ampio rispetto alla linea politica accolta dai codici civili del Novecento<sup>32</sup>.

È un fatto acquisito, più dagli studiosi che dai consociati<sup>33</sup>, che le tecniche manipolative e di sfruttamento delle vulnerabilità umane, diffuse

---

«possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate».

<sup>32</sup> G.B. FERRI, *Il negozio giuridico*, Padova, 2024, 267 ss. sulle patologie contrattuali e circolazione della proprietà.

<sup>33</sup> Si riscontra un ritardo nell'alfabetizzazione digitale. Non a caso il d.l. 15.9.2023, n. 123 contenente «*misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori nell'ambito digitale*», convertito con modificazioni in legge n. 1591/2023, prevede significative disposizioni su questo punto. L'art. 14 pone un dovere a carico delle Istituzioni, anche non politiche, di proteggere i minorenni attraverso una più approfondita conoscenza del funzionamento dell'ambiente digitale; una protezione che necessita, inevitabilmente, di un'alfabetizzazione digitale anche delle famiglie. Si prevede in sintesi: 1) la promozione da parte della Presidenza del Consiglio dei ministri (Dipartimento per le politiche della famiglia) di studi e l'elaborazione di linee guida rivolte ai fruitori di disposizioni di comunicazione elettronica e del controllo parentale, «con particolare attenzione agli educatori, alle famiglie e ai minori»; 2) offerta di consulenza e servizi da parte dei Centri per la famiglia «in merito alla alfabetizzazione mediatica e digitale dei minori, con particolare attenzione alla loro tutela rispetto all'esposizione a contenuti pornografici e violenti»; 3) avviamento annuale da parte della Presidenza del Consiglio dei ministri (Dipartimento per le politiche della famiglia) di «campagne di informazione sull'uso consapevole della rete e sui rischi connessi, in particolar modo sui mezzi di prevenzione dall'accesso a contenuti potenzialmente nocivi per lo sviluppo armonioso dei minori». Al fine di rafforzare le prescrizioni contenute nella legge in esame, si prevedono due relazioni annuali: una redatta dall'Autorità per le garanzie nella comunicazioni, da inviare all'Autorità politica con delega alla famiglia, «sull'impatto dell'attuazione dell'art. 13 [sulle «applicazioni di controllo parentale nei dispositivi di comunicazione elettronica»], con particolare riferimento all'uso dell'applicazione del controllo parentale»; l'altra predisposta dall'Autorità politica con delega alle politiche per la famiglia, da presentare al Parlamento, sull'attuazione della presente legge.

Cfr. anche: il cons. 20 AI-Act secondo il quale l'alfabetizzazione in materia di IA deve riguardare tutti gli attori della catena del valore dell'IA (fornitori, *deployer*, persone interessate). Occorre promuovere quegli strumenti volti a raggiungere una conoscenza sufficiente dei benefici, rischi, garanzie, diritti e obblighi attinenti all'uso dei sistemi di IA; il cons. 56 collega la diffusione dei sistemi di IA nell'istruzione alla formazione digitale dei discenti e degli insegnanti in modo da acquisire la capacità di stare nell'ambiente digitale e





nell'ambiente digitale, sono decisamente più insidiose di quelle note che si praticano nell'ambiente offline. Si consideri che tra persone presenti fisicamente si instaura un livello maggiore di attenzione; la presenza dell'altro attiva una capacità superiore di riflessione, argomentazione e resistenza, di talché occorre uno sforzo più evidente, maggiori capacità, per costruire una realtà ingannevole o per sfruttare vulnerabilità altrui.

È così nel dolo, dove il raggio costa di una *mise en scène* in mala fede con cui si altera la realtà, mostrando alla controparte ciò che non è<sup>34</sup>. Il *deceptor* deve ingannare in un modo che risulti evidente nella valutazione *ex post* e causalmente incidente sulla volontà del *deceptus*, di modo che una tale condotta ingannevole possa essere accertata dal giudice. Non a caso la giurisprudenza è restia ad attribuire rilievo alla mera omissione quale causa di invalidità del contratto (c.d. dolo omissivo)<sup>35</sup>, al di là delle ipotesi

---

un «pensiero critico per partecipare attivamente all'economia, alla società e ai processi democratici». In tale considerando si indicano altresì i pericoli insiti nei sistemi di IA impiegati per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale e per valutare i risultati dell'apprendimento degli studenti e altro ancora. Tali sistemi devono essere classificati ad alto rischio; il cons. 91 sull'alfabetizzazione di chi è coinvolto nel funzionamento del sistema di IA; il cons. 165 contiene un altro riferimento alle «misure di alfabetizzazione in materia di IA»; e cfr. altresì gli artt. 3 n. 56, 4, 66 lett. f) e 95 par. 2 lett. c) AI-Act.

L'accento sull'alfabetizzazione è posto anche dall'art. 20 della Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e dall'art. 22, co. 2 lett. b), dello «schema di disegno di legge recante disposizioni e delega al Governo in materia di intelligenza artificiale».

<sup>34</sup> A. TRABUCCHI, *Il dolo nella teoria dei vizi del volere*, (1937), rist. anastatica, a cura di P. Perlingieri, Napoli, 2022, 167 ss.

<sup>35</sup> Cass., 11.10.1994, n. 8295, in *Banca dati-One legale* afferma che il dolo omissivo, causa di annullamento, non è integrato dal silenzio o dalla reticenza, richiedendosi ... che il comportamento passivo *si inserisca in una condotta configurabile, nel complesso, quale malizia o astuzia volta a realizzare l'inganno perseguito*. Il connotato essenziale del dolo invalidante è dato dalla volontaria realizzazione, ad opera di una parte, di una alterazione nella rappresentazione delle situazioni determinanti sulla formazione del consenso della controparte, al fine di coartarne la libera determinazione. Per contro *il semplice silenzio*, anche su situazioni di interesse della controparte, *e la reticenza non immutano la rappresentazione della realtà*, ma si limitano a non contrastare la percezione della realtà alla quale sia pervenuto l'altro contraente. Cfr. in senso analogo anche Cass., 31.5.2010, n. 13231, in *Banca dati-One legale*. Minoritaria è la posizione F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, Napoli, 2022, 171, secondo il quale «non costituisce dolo né la menzogna, perché la legge, se tutela la buona fede, non tutela la credulità, né la reticenza». Diversa è l'opinione di altri Autori che reputano il mendacio e il silenzio cause di annullabilità del contratto, tra cui si richiamano qui, per brevità, solo R. SACCO, *Il contratto*, in Sacco-De Nova, Torino, 2004, 559 ss., il quale argomento l'obbligo di informare dall'art. 1337 c.c.; G. VETTORI, *Anomalie e tutela nei rapporti di distribuzione tra imprese*, Milano, 2983, 98-148; G. VISINITINI, *La reticenza nella formazione dei contratti*, Padova, 1972, 76 ss., la quale trae argomento da disposizioni che hanno di mira un dovere di informazione e V. ROPPO, *Il contratto*, Milano, 2011, 763-764, muovendo dalla crescente valorizzazione del principio di buona fede e dall'incremento delle disposizioni sull'informazione, ammette il dolo omissivo nei limiti però di un equilibrio caso per caso tra l'esigenza di valorizzare il dovere di informazione e quella di chi ha pagato e lavorato molto e pagato per avere un'informazione.

espressamente previste dalla legge. E anche con riguardo al mendacio, la Cassazione ha cura di precisare i connotati della condotta menzognera<sup>36</sup>.

Nell'ambiente digitale il condizionamento della volontà e lo sfruttamento delle vulnerabilità avvengono incidendo non tanto sulla parte cosciente della persona, inducendola a commettere un errore, quanto piuttosto sul subconscio, cioè su quel livello della mente responsabile dei processi automatici che gestisce emozioni, paure, gioie e altri profili emotivi<sup>37</sup>. È sull'emotività e sull'inibizione del funzionamento dell'intelletto umano che fa perno l'influenza negativa del potere digitale. La volontà, vocata a dire sì o no, si stacca dall'intelletto, stimolata com'è dalle tecniche di persuasione.

La normativa ha colto questo aspetto, difatti, come si diceva, l'art. 5, par. 1 lett. a), AI-Act stigmatizza le «tecniche subliminali che agiscono senza che una persona ne sia consapevole», l'art. 25 DSA vieta non solo le interfacce che ingannano, ma anche quelle che «materialmente falsano» o «compromettono altrimenti» e l'art. 5, par. 1 lett. f), AI-Act limita i sistemi di IA di riconoscimento delle emozioni.

Si taglia allora un punto: nell'ambiente digitale la persona manipolata crede di essere libera, ma non lo è; ritiene che l'interesse e la curiosità palesati in un atto siano espressione spontanea del proprio essere, quando invece sono indotti dalla manipolazione, la quale, talvolta fa perno sulla categorizzazione delle persone fisiche, consistente nell'assegnazione di queste ultime a categorie specifiche sulla base dei loro dati biometrici; categorie riguardanti tra l'altro, «i tratti comportamentali o di personalità»<sup>38</sup>.

In questo *modus vivendi* apparentemente libero, è stato acutamente sottolineato, con accezione negativa, che «libertà e uguaglianza

<sup>36</sup> Cass., 13.6.2015, n. 12892, in *Banca dati-One legale*, afferma che «ricorre il “*dolus malus*” solo se, in relazione alle circostanze di fatto e personali del contraente, il mendacio sia accompagnato da malizie ed astuzie volte a realizzare l'inganno voluto ed idonee in concreto a sorprendere una persona di normale diligenza e sussista, quindi, in chi se ne proclami vittima, assenza di negligenza o di incolpevole ignoranza (Cass. n. 14628/2009)». I raggiri devono essere stati determinanti della volontà del *deceptus* ed aver ingenerato in quest'ultimo «una rappresentazione alterata della realtà, provocando nel suo meccanismo volitivo un errore da considerarsi essenziale ai sensi dell'art. 1429 c.c. Ne consegue che per aversi annullamento del contratto non è sufficiente una qualunque influenza psicologica sull'altro contraente, *ma sono necessari artifici o raggiri, o anche semplici menzogne* [n.d.r. più d'una quindi] che abbiano avuto comunque un'efficienza causale sulla determinazione volitiva della controparte e, quindi, sul consenso di quest'ultima (Cass. n. 20792/2004). Sull'incidenza causale della condotta cfr. A. TRABUCCHI, *Il dolo nella teoria dei vizi del volere*, cit. p. 84-90.

<sup>37</sup> G. VETTORI, *Persona e pluralismo*, in *Persona e mercato*, cit., p. 331, sottolinea come il controllo delle nostre vite attraverso i dati personali opera «sull'inconscio nascosto dietro lo spazio cosciente. Di più. Le nostre emozioni, carpite dall'espressione del volto, dalle parole, dal movimento degli occhi, sono raccolte e si forma un inconscio digitale, non ancora nostro. Anticipato e creato da macchine intelligenti e capace di condizionare i nostri desideri e i nostri comportamenti, ad un livello posto al di sotto della soglia della coscienza». L'inconscio «non ancora nostro» che la tecnologia può delimitare e isolare - fatto inquietante a cui attribuire molta considerazione - interessa al legislatore e all'interprete, perché dà adito a un pericolo di manipolazione della persona senza precedenti nella storia (ne è perfettamente consapevole B.-C. HAN, *Infocrazia*, cit., 4 ss.).

<sup>38</sup> Cfr. i cons. 14, 16, 30, 54 e gli artt. 3 n. 40, 5 par. 1 lett. g), 50 par. 3 e all. III punto 1 lett. b) AI-Act.

coincidono»<sup>39</sup>. Se la libertà del volere si sovrappone all'uguaglianza significa che si ha un appiattimento e una strumentalizzazione delle persone, le quali, manifestando tutte la stessa volontà (prevista), non sono più libere di decidere e il loro essere uguali agli altri si traduce in un esproprio dell'identità. L'uguaglianza è apparente perché essa non può esistere senza la libertà del volere.

Questo esito nefasto per la vita del singolo e per l'umanità è avversato dall'Unione europea, non solo attraverso la regolamentazione dei dati personali – secondo un sistema più aperto, equo e innovativo che rispetti i diritti degli utenti, da ultimo come da regolamento (UE 2023/2854) c.d. *european data act*<sup>40</sup> – ma anche e soprattutto attraverso il divieto di manipolazione di cui si è detto. Con una consapevolezza delle Istituzioni europee: occorre offrire una risposta legislativa più completa al problema della progettazione dei servizi online che creano dipendenza<sup>41</sup>. Il dipendere da un sito, da un servizio, dall'acquisto di uno stesso bene è determinato dalla macchina in ragione di una vulnerabilità dell'utente ben individuata; così dipendenza e manipolazione si stringono in un abbraccio perverso dove l'una alimenta ed espande l'altra.

Secondo la risoluzione del Parlamento europeo del 2023, la «progettazione manipolativa» o «progettazione che crea dipendenza» segue il seguente schema: l'interfaccia funziona in modo tale da assicurare la maggiore permanenza possibile dell'utente online (ad es. tramite le tecniche di «*gamification*»)<sup>42</sup>; così chi offre il servizio o fornisce la piattaforma avrà a disposizione più dati personali. Inoltre si potranno sfruttare le vulnerabilità dell'utente, facendogli spendere più denaro stante il tempo sempre maggiore trascorso nel web (c.d. economia dell'attenzione)<sup>43</sup>.

Non c'è, tuttavia, solo un problema di induzione a manifestare la volontà e di danno economico, ma anche e soprattutto di possibili pregiudizi non

<sup>39</sup> G. VETTORI, *Persona e pluralismo*, cit., 331.

<sup>40</sup> Al cons. 38 del reg. (UE)2023/2854 «riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 202/1828 (regolamento sui dati)» si afferma che i terzi e i titolari dei dati non devono pregiudicare l'autonomia, il processo decisionale o le scelte dell'utente attraverso i *dark patterns*.

<sup>41</sup> Risoluzione del Parlamento europeo, 12 dicembre 2023, «sulla progettazione di servizi online che crea dipendenza e sulla tutela dei consumatori nel mercato unico dell'UE», in *Persona e mercato*, 2024, 2, 694 ss., all'interno dell'Osservatorio OGID, con segnalazione di R. ALFONSI. Cfr anche: Studio della Commissione intitolato «*Behavioural study of unfair commercial practises in the digital environment: dark patterns and manipulative personalisation: final report*», 2022, in *op.europa.eu*, in part. p. 85 ss. sul *measuring the impact of unfair practices*; studio del servizio ricerca del Parlamento europeo del 2019 intitolato «*Harmful internet use. Part I: Internet addiction and problematic use*», in *www.europarl.europa.eu*, in part. p. 22 ss. sul *gaming* (cfr. *infra* nota 39).

<sup>42</sup> Le tecniche di «*gamification*», utilizzate in vari settori tra cui il marketing, perseguono lo scopo di accrescere la partecipazione attiva dell'utente, la motivazione e il tempo trascorso online. Esse rendono le interazioni più coinvolgenti e stimolanti attraverso badge e certificati premianti, il feedback immediato, lo storytelling e altro ancora.

<sup>43</sup> Risoluzione del Parlamento europeo, 12.12.2023, «sulla progettazione di servizi online che crea dipendenza (...)», cit., cons. A. Cfr. R. MONTINARO, *Sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (non solo)*, cit., p. 381, in part. sull'uso di RS per 'catturare' l'attenzione dei consumatori.

patrimoniali alla persona, rispetto ai quali i bambini e i giovani sono i più esposti. Allarmante è il quadro dei possibili riflessi negativi sulla persona, dipinto dalla Risoluzione appena richiamata<sup>44</sup>.

La progettazione e il funzionamento manipolante della tecnologia non investe soltanto le categorie tradizionali di soggetti vulnerabili, quali i minorenni, i disabili e, in certi casi, gli anziani, ma tutti gli utenti. L’asimmetria digitale impone di ammettere l’esistenza di uno stato generale di vulnerabilità digitale, da intendersi quale condizione umana. Nell’ambiente online si è fragili non solo a causa dell’età o perché affetti da una patologia psichica, ma soprattutto in quanto persona, *compos sui*, esposta al potere tecnologico attraverso plurime tecniche manipolative<sup>45</sup>.

Se muta il contesto in cui si vive – in media i giovani dai 16 ai 24 anni trascorrono più di 7 ore al giorno su Internet<sup>46</sup> – se sorgono nuovi pericoli

<sup>44</sup> Risoluzione del Parlamento europeo, 12.12.2023, «sulla progettazione di servizi online che crea dipendenza, cit., al cons. D) afferma che l’uso problematico dello smartphone o di Internet è stato collegato «a una minore soddisfazione esistenziale e a sintomi di disturbi mentali quali depressione, bassa autostima, disturbi dell’immagine corporea, disturbi alimentari, ansia, alti livelli di stress percepito, indifferenza nei confronti di familiari e amici, perdita dell’autocontrollo, mancanza di sonno e sintomi ossessivo-compulsivi, come l’acquisto compulsivo diffuso tra i giovani adulti; che gli utenti assidui di media digitali hanno il doppio delle probabilità di sviluppare problemi di salute mentale, compresi i fattori di rischio di suicidio e autolesionismo; che i bambini e i giovani sono più vulnerabili a tali sintomi; che le patologie di salute mentale che si sviluppano durante l’infanzia *possono condizionare il successivo corso della vita di un individuo*; che l’uso eccessivo di Internet è associato a problemi con gli obblighi quotidiani, al calo dei voti e allo scarso rendimento scolastico, accademico o lavorativo; che la prevalenza delle dipendenze digitali e la loro associazione con i sintomi di disturbi mentali comuni è un problema crescente di salute pubblica e, come tale, dovrebbe essere fonte di preoccupazione per i decisori politici; che è necessario condurre ulteriori ricerche al fine di ottenere maggiori informazioni per lo sviluppo dei criteri diagnostici più appropriati e per stabilire i fattori di rischio per le diverse dipendenze digitali; che alcuni servizi, prodotti o funzioni che potenzialmente non hanno alcun effetto sugli adulti possono invece essere estremamente rischiosi e dannosi per i minori e creare dipendenza in questi ultimi, anche a causa dell’impatto cumulativo di una combinazione di più funzioni o degli effetti prolungati nel tempo».

<sup>45</sup> La risoluzione del Parlamento europeo, 12.12.2023, «sulla progettazione di servizi online che crea dipendenza (...)», cit., cons. L, indica diverse pratiche frutto della progettazione che creano dipendenza, tra le quali: «lo scorrimento infinito, il caricamento delle pagine con la funzione “aggiornamento tramite trascinarsi verso il basso”, la riproduzione automatica dei video incessante, i consigli personalizzati, le notifiche di recupero, ossia le notifiche per riguadagnare l’attenzione degli utenti che hanno abbandonato un servizio o una app, la funzione “*playing by appointment*” (gioca su appuntamento) che spinge a giocare in determinati momenti della giornata, la progettazione che causa una percezione diluita del tempo trascorso sulla piattaforma o le false notifiche social che creano l’illusione di aggiornamenti nell’ambito della cerchia sociale online dell’utente». Queste e altre tecniche, attuate anche in modo personalizzato, inducono l’utente a restare online e a operare continuamente in diverse direzioni.

<sup>46</sup> *Average daily time spent using the internet by online users worldwide as of 4th quarter 2022, by age and gender* (Tempo medio giornaliero trascorso online dagli utenti di Internet in tutto il mondo nel quarto trimestre del 2022, per età e genere), Statista, 22 maggio 2023, in <https://www.statista.com/statistics/1378510/daily-time-spent-onlineworldwide-by-age-and-gender>.



per la persona rispetto a quelli già considerati dal diritto, non possono che mutare il concetto di vulnerabilità e le condizioni della sua rilevanza<sup>47</sup>.

L'impostazione del codice civile è stravolta dal diritto dell'ambiente digitale: rilevano non solo specifiche condizioni di debolezza, ma soprattutto uno stato di fragilità ontologica della persona rispetto a certi usi della tecnologia<sup>48</sup>. Questo perché la digitalizzazione dell'esistenza può influire sull'identità, sempre meno unitaria, sulle relazioni, che divengono più superficiali e sulla percezione di sé, in un mondo dove il pensare retrocede rispetto al nudo fare inducendo a scambiare la sorte per il proprio destino<sup>49</sup>.

Se il fenomeno della manipolazione, dipendenza e sfruttamento della vulnerabilità umana è connotato dall'intrappolare la volontà al di fuori del proprio Sé, sono insufficienti sia le norme sui vizi del consenso sia quelle sulle pratiche commerciali scorrette, rispetto alle quali pure emerge, come acutamente osservato, un ampliamento delle condizioni soggettive di debolezza rilevanti (arg. ex art. 26 cod. cons.)<sup>50</sup>.

In questo contesto in cui l'utente è un bersaglio, è giusta la considerazione del Parlamento europeo secondo cui occorre incrementare la normativa sulla manipolazione e sulle dipendenze digitali in un quadro di maggiore unità, introducendo altresì un diritto digitale a non essere disturbati, da irrobustire però con un'adeguata politica di alfabetizzazione digitale. La base di partenza però è ragguardevole e innovativa: c'è un divieto di manipolare l'utente online e di determinare dipendenze comportamentali, cui si aggiunge il divieto di sfruttare le vulnerabilità umane che si palesano in conseguenza di un utilizzo non etico della tecnologia in quanto limitativo della libertà del volere.

<sup>47</sup> B. PASTORE, *Semantica della vulnerabilità, soggetto, cultura giuridica*, Torino, 2021, 25, sottolinea che il diritto esprime in pieno la sua funzione quando vi sono pericoli nuovi per la persona, per cui viene in rilievo «l'esserci della persona», il saper guardare «alla concretezza delle sue esigenze e dei suoi bisogni esistenziali».

<sup>48</sup> B. PASTORE, *Semantica della vulnerabilità, soggetto, cultura giuridica*, cit., 7, muove dalla vulnerabilità quale condizione universale, la quale assume forme e gradi peculiari legati a concreti contesti esistenziali. Egli afferma che «la vulnerabilità, insieme alle altre verità elementari, è di importanza vitale per la comprensione delle istituzioni giuridiche. Essa si pone come condizione di praticabilità, e della stessa pensabilità, del diritto». La vulnerabilità è un concetto diverso da quello astratto di soggettività, ponendo in rilievo la persona concreta. Pastore coglie nel segno quando afferma che «è il concetto di vulnerabilità che, riportandoci alla condizione di esseri limitati, fragili, dipendenti, consente di riconfigurare l'idea della soggettività, in quanto concetto riassuntivo della condizione generale della persona, superandone l'astrattezza e riposizionandola su una dimensione concreta, situata, relazionale. La vulnerabilità diventa...un referente universale nella configurazione del soggetto che consente di includere le differenze, ponendo attenzione agli esseri umani reali, in carne ed ossa». Da questo punto di vista è senz'altro felice la scelta dell'Unione europea di utilizzare la categoria – perché di questo si tratta – della vulnerabilità quale risposta alla strapotere della tecnologia.

<sup>49</sup> Z. BAUMAN, *Modernità liquida*, Roma-Bari, 2011, 248-249, coglie benissimo, in profondità, questo esito negativo per l'individuo dato dallo scambiare la propria sorte per il proprio destino, quando la velocità del vivere e del decidere annichilisce il pensiero.

<sup>50</sup> S. ORLANDO, *Commento agli artt. 24, 25, 26 del codice del consumo*, in *Codice e del consumo. Pratiche commerciali scorrette e azioni collettive*, aggiornamento, a cura di G. Vettori, Padova, 2009, 94 ss.

## 5. La vulnerabilità digitale quale categoria giuridica non riconducibile a figure specifiche di debolezza.

| 934

Il legislatore del codice civile è stato piuttosto restio a individuare le fragilità umane, privilegiando un sistema contrattuale imperniato sull'affidamento della controparte del contratto e dei terzi e sulla certezza della circolazione. Non è necessario in questa sede ripercorrere l'evoluzione che vi è stata dall'interdizione giudiziale all'amministrazione di sostegno<sup>51</sup>, se non per rimarcare che, in tema di incapacità legale, sintagma questo di cui si propugna l'abrogazione<sup>52</sup>, vi è stata un'ampia apertura dell'ordinamento italiano al concetto internazionale di disabilità<sup>53</sup>, come enunciato nella convenzione dell'ONU sui diritti delle persone con disabilità del 13 dicembre 2006, ratificata con legge del 3 marzo 2009 n. 18. L'art. 404 c.c., com'è noto, ha affiancato all'infermità il concetto di «menomazione fisica o psichica», col risultato di comprendere, quali condizioni soggettive di debolezza, non solo le più diverse malattie e condizioni di salute, ma anche le riduzioni di funzionalità fisiche e mentali.

Ma è con riguardo alle condizioni di fragilità della persona non sottoposta a misure di protezione che il codice civile, diversamente da altri codici europei<sup>54</sup> e da alcune fonti c.d. persuasive<sup>55</sup>, è rimasto fermo

<sup>51</sup> Si rinvia al bel volume di G. LISELLA-F.PARENTE, *Persona fisica*, in *Tratt. di dir. civ. del CNP*, diretto da P. Perlingieri, Napoli, 2012, in part. 1-92, 243-370

<sup>52</sup> Cfr. la proposta di legge «abrogazione dell'interdizione e dell'inabilitazione e rafforzamento dell'amministrazione di sostegno, versione 2020», testo in [www.civilistiitaliani.eu](http://www.civilistiitaliani.eu). Nella relazione si sottolinea come il ribaltamento di prospettiva prodotto dall'introduzione dell'amministrazione di sostegno e l'abrogazione dell'interdizione e dell'inabilitazione non consente più l'utilizzo del sintagma incapace legale con riguardo alla persona maggiorenne sottoposta ad amministrazione di sostegno. La quale non diviene incapace ma è interessata da «(I) una mera e contingente sospensione di poteri, (II) giustificata da specifici pericoli sul terreno gestionale, e comunque (III) circoscritta, secondo la modulazione che verrà stabilita dal giudice tutelare, nel caso concreto, ad uno o a più (in limitatissimi casi, a tutti quanti gli) atti e operazioni da compiersi». Anche qualora vi sarà la necessità di togliere il potere di compiere tutti gli atti si avrà una «incapacitazione funzionale», relativa non già alla persona, ma a uno o a tutti gli atti. Si propone, dunque, di eliminare la categoria dell'incapacità legale per le persone disabili, in linea del resto con la Convenzione ONU sopra richiamata del 2009 e con la terminologia del titolo XII del libro primo del codice civile.

<sup>53</sup> Ai sensi dell'art. 2 co. 2 della Convenzione ONU sulla disabilità «le persone con disabilità includono quanti hanno minorazioni fisiche, mentali, intellettuali o sensoriali a lungo termine che in interazione con varie barriere possono impedire la loro piena ed effettiva partecipazione nella società su una base di eguaglianza con gli altri». È agevole notare che una tale accezione di disabilità è più estesa di quella accolta dal codice civile prima dell'introduzione nel 2004 dell'amministrazione di sostegno imperniata sull'infermità mentale. Erano le innumerevoli condizioni di disagio psichico e di fragilità umana, non riconducibili al concetto di infermità mentale a rimanere nell'ombra, schiacciate dalla rigidità disciplinare dell'interdizione e dell'inabilitazione.

<sup>54</sup> La riforma del codice civile francese, avvenuta con ord. n. 2016-131, ha ampliato l'ambito applicativo dei vizi del consenso, introducendo la nuova fattispecie dell'*état de dépendance* all'art. 1143 *code civil*. Lo stato di dipendenza è un'ulteriore ipotesi di violenza, introdotta per superare quella rigidità che connotava anche la disciplina d'oltralpe dei vizi del



all'incapacità di intendere e di volere (art. 428 c.c.), allo stato di pericolo (art. 1447 c.c.) e allo stato di bisogno (art. 1448 c.c.). A queste si aggiungono i concetti di deficienza psichica di cui all'art. 643 c.p. e di «condizioni di difficoltà economica o finanziaria» (c.d. usura reale)<sup>56</sup> di cui all'art. 644, co. 3, c.p. e la relativa problematica della sorte del contratto rispetto al reato<sup>57</sup>.

Tutte queste condizioni soggettive sono diverse dalla (e comunque non esaustive della) vulnerabilità che connota l'utente online. L'incapacità legale, l'incapacità naturale e la deficienza psichica sono accomunate dalla presenza di uno stato patologico, abituale o temporaneo, di debolezza della persona. La quale, prima di manifestare la volontà, è già minata nell'intelletto e la controparte ne approfitta per farle compiere un atto a sé svantaggioso che altrimenti non sarebbe stato compiuto. La patologia non è determinata da altri, ma esiste già e condiziona inevitabilmente il controllo razionale del proprio agire.

L'utente online di cui parliamo, invece, quando inizia la navigazione non è affetto da alcuna patologia; è il funzionamento della piattaforma, il tipo di servizio che egli utilizza o la pratica manipolante di IA che palesa una vulnerabilità dell'utente, che la stimola, la accresce e la fa sfociare in un atto o in un comportamento pregiudizievole. Ecco perché la normativa digitale si

---

consenso. In questa direzione potremmo richiamare anche l'art. 138 § 2 BGB che dà rilievo a diverse condizioni di debolezza - «lo stato di costrizione, l'inesperienza, la mancanza di discernimento o la rilevante debolezza» della controparte – che incidono sulla validità del contratto. Entrambe le normative francese e tedesca richiedono per invalidare il contratto anche l'evidente sproporzione delle prestazioni e l'abuso/sfruttamento della debolezza altrui. Sullo stato di dipendenza cfr.: E. TUCCARI, *Lezioni francesi sull'abuso di dipendenza (economica?)*, in *Jus civile*, 2022, 762 ss. e F. RENDE, *Abus dé dependance e controllo del regolamento contrattuale*, in *Persona e mercato*, 2021, 3, 526 ss.

<sup>55</sup> Cfr. l'art. 3.2.7 *Unidroit principles* (versione 2016) attribuisce rilevanza alle seguenti condizioni di debolezza: «*dependance, economic distress or urgent needs, or of its improvidence, ignorance, inexperience or lack of bargaining skill*». Analogamente dispongono l'art. II-7:207(*unfair exploitation*) *Draft common frame of reference* (DRAFT) e l'art. 4:109 (*excessive benefit or unfair advantage*) dei *principles of european contract law* (PECL). L'art. 30.3 dei principi di diritto europeo dei contratti (accademia dei giuristi europei-Pavia) considera anche l'*assujettissement économique ou moral de l'autre partie*. Non è sufficiente, però, l'elemento soggettivo per invalidare il contratto, occorrendo, tra l'altro, una manifesta sproporzione delle due prestazioni.

<sup>56</sup> A. GENTILI, *Contratti usurari: tipologie e rimedi*, in *Riv. dir. civ.*, 2001, I, 354-360, sottolinea come l'usurato non sia riconducibile a una categoria socio-economica debole come il lavoratore, il consumatore o il risparmiatore, soggetti, questi ultimi, deboli al di là del singolo acquisto di beni o servizi di investimento; l'usurato è percepibile solo nel suo specifico ruolo in una concreta vicenda contrattuale. Egli afferma che il legislatore non si è limitato a proteggere un parte debole, ma abbia inteso dirigere i flussi creditizi. L'utente online, invece, come si diceva, è ontologicamente debole rispetto alle forze manipolanti dell'ambiente digitale e la relativa normativa si concentra sulla sua protezione, sia pur in quadro più generale, come diremo nell'ultimo paragrafo, di rilevanza pubblica.

<sup>57</sup> Per un approfondimento del tema cfr. AA.VV., *Contratto e reato*, a cura di A. Flamini e L. Ruggeri, Napoli, 2014, in part. F. D. BUSNELLI, *Atto illecito e contratto illecito: quale connessione?*, p. 15 ss.; M. RABITTI, *Illiceità penale e illiceità civile*, p. 81 ss.; M. MANTOVANI, *Norme penali e nullità virtuale del contratto*, 93 ss.; A.A. DOLMETTA, *Sul contratto usurario*, p. 281 ss. In particolare sul contratto concluso all'esito della circonvenzione di incapace cfr. A. DI AMATO, *Contratto e reato. Profili civilistici*, in *Trattato di diritto civile del CNN*, a cura di P. Perlingieri, Napoli, 2003, 43 ss e 193 ss.

concentra non tanto e non solo sulle specifiche fattispecie di debolezza umana rilevanti, per circoscriverle in modo stringente, quanto piuttosto sul funzionamento, sulla sicurezza della tecnologia e sugli obblighi a carico di certi soggetti, affinché non si verificano violazioni di diritti fondamentali.

Si prevedono molti obblighi, tra cui spicca la valutazione preventiva, a carico dei fornitori di piattaforme (e di motori di ricerca) online molto grandi, dei rischi sistemici attinenti a possibili pregiudizi dei diritti fondamentali, alla «salute pubblica» e a «gravi conseguenze negative per il benessere fisico e mentale della persona» (art. 34 DSA); analogamente stabilisce l'art. 9 AI-Act.

Anche con le fattispecie dello stato di pericolo (art. 1447 c.c.) e dello stato di bisogno (1448 c.c.) in cui versa la persona, il codice civile mostra la sua linea di policy consistente nel circoscrivere con precisione le fattispecie di eliminazione del contratto. Inoltre – ed è ciò che più conta – nella rescissione gli elementi soggettivi dello stato di bisogno e di approfittamento «non penetrano nel consenso, come i vizi della volontà», atteggiandosi piuttosto a circostanze estrinseche alla struttura del contratto<sup>58</sup>. Diversamente la manipolazione digitale e lo sfruttamento delle vulnerabilità attengono proprio alla volontà e dunque alla struttura dell'atto, con quanto ne consegue, come vedremo, sul piano rimediale.

Non solo: c'è un altro elemento che differenzia la rescissione dalla manipolazione digitale. La persona che cede allo stato di pericolo o allo stato di bisogno in cui si trova è consapevole di ciò fa e comprende il disvalore della condotta altrui. Invece l'utente online manipolato, la cui vulnerabilità è carpita per divenire fonte di lucro, crede di aver esercitato una sua libertà; si sente libero e non compulsato. La tecnologia digitale, se manipolante, ha il potere di sollecitare le debolezze umane, qualunque esse siano. Perciò il legislatore europeo ha introdotto la categoria della vulnerabilità, pur non rinunciando a specificarla in certi casi, quale condizione connaturata alla persona che si manifesta sollecitata dalle forze dell'ambiente digitale.

Certo, lo stato di bisogno è un concetto elastico che apre a tutte le necessità purché «qualificat[e] da un dato oggettivo, socialmente apprezzabile<sup>59</sup>, ossia «il bisogno di qualcosa che serva a evitare un significativo pregiudizio»<sup>60</sup>, su cui fa leva illecitamente la controparte. Ma il bisogno attinente a una carenza o difficoltà riferibile, nel limite predetto, ad

<sup>58</sup> G. BENEDETTI, *La rescissione*, in *Tratt. di dir. priv.*, diretto da M. Bessone, Torino, 2007, tomo VIII, 44 ss., confuta egregiamente sia la tesi che riconduce la rescissione a un vizio della causa del contratto (F. SANTORO PASSARELLI, *Dottrine generali del diritto civile*, cit., 184; G. MARINI, *Rescissione (dir. vig.)*, in *Enc. dir.*, Milano, 1988, p. 981); sia la tesi che ne individua il fondamento unitario nei vizi del volere (M. ALLARA, *La teoria generale del contratto*, Torino, 1945, 177; G. SCALFI, *Il fondamento dell'azione di rescissione*, in *Temi*, 1949, 39). L'A. offre una ricostruzione originale ed eclettica della rescissione, quale rimedio «legato tanto al momento genetico dell'atto quanto a quello funzionale del rapporto».

<sup>59</sup> V. ROPPO, *Il contratto*, cit., 834-835.

<sup>60</sup> V. ROPPO, *Il contratto*, cit., 835, reca l'esempio dell'imprenditore in grave crisi di liquidità, il quale, per evitare il fallimento, vende sottocosto i propri beni per tacitare i creditori: «il suo bisogno è oggettivo e serio».





aspetti economici o sociali che richiederebbero un sostegno da parte delle istituzioni o di enti/istituti della società, non è certo l'unica condizione di vulnerabilità che funge da sostrato alla manipolazione. Non solo: l'agire dell'utente online non è necessariamente caratterizzato, come invece lo stato di bisogno di cui all'art. 1448 c.c., dalla «prospettiva di un pregiudizio conseguente alla mancata soddisfazione del bisogno»<sup>61</sup>, di cui la controparte approfitta.

L'art. 5, par. 1 lett. b), AI-Act pone l'accento, quale esito riprovato dall'ordinamento euro-unitario, sullo sfruttamento delle «vulnerabilità di una persona o di uno specifico gruppo di persone», lasciando intendere che ogni fragilità socialmente rilevante assurge alla giuridicità. L'elencazione successiva – vulnerabilità «dovute all'età, alla disabilità o a una specifica situazione sociale o economica» - è meramente esemplificativa poiché il legislatore non ha cura di chiudere l'elenco con l'avverbio «esclusivamente».

Se ne ha una conferma in altre disposizioni in cui si adopera solo il lemma vulnerabilità, senza limitarlo in alcun modo: l'art. 9, par. 9, AI-Act stabilisce che, nell'attuare il sistema della gestione dei rischi, i fornitori di sistemi di IA devono prestare attenzione «all'eventualità che il sistema di IA ad alto rischio non abbia un impatto negativo su minorenni o «su altri gruppi di *persone vulnerabili*»; il considerando 69, cui si lega l'art. 26, par. 3, DSA, sottolinea la pericolosità delle inserzioni pubblicitarie basate sul *targeting*, le quali possono attirare le vulnerabilità, indistinte, degli utenti<sup>62</sup> (anche i sistemi di raccomandazione rischiano di pregiudicare le «persone in situazioni vulnerabili», cons. 94 e art. 27 DSA).

È significativo anche il considerando 75 del GDPR, il quale, nell'elencare i rischi per i diritti e le libertà della persone fisiche derivanti dal trattamento di alcuni tipi di dati personali, menziona proprio quello in cui «sono trattati dati personali di persone vulnerabili, in particolare minori».

Insomma, rispetto all'impostazione del codice civile che individua condizioni di debolezza specifiche e rispetto alla centralità del consumatore nel diritto europeo, i rischi di sfruttamento degli utenti online hanno riportato al centro dell'ordinamento europeo la persona con le sue fragilità e l'idea, di derivazione kantiana<sup>63</sup>, connaturata al principio personalistico,

<sup>61</sup> V. ROPPO, *op.loc.ult.cit.*

<sup>62</sup> S. ORLANDO, *Per un sindacato di liceità del consenso privacy*, in *Persona e mercato*, 2022, 4, 527 ss., si sofferma sul caso Leon, un signore di cui è stata carpita, tramite la profilazione, l'inclinazione al gioco d'azzardo. Il caso è tratto dalle Linee guida dell'EDPB sul targeting degli utenti dei social media, adottate il 13 aprile 2021. È un esempio – il n. 8 delle linee guida – emblematico della rilevanza della vulnerabilità, in cui la volontà è alterata dalla propria condizione di debolezza caratteriale e psichica, non predeterminata dalla legge ma riconducibile alla categoria della vulnerabilità. In questo esempio la specifica condizione di fragilità dell'utente viene abilmente sfruttata dalla tecnologia digitale.

<sup>63</sup> I. KANT, *Fondazione della metafisica dei costumi*, trad. e introduzione di F. Gonnelli, Roma-Bari, 2022, 127 ss. riflette sulla libertà quale presupposto necessario della ragione (p. 155), che è il sostrato della volontà. La manipolazione digitale mira proprio a elidere la libertà, così da impadronirsi della persona.

dell'uomo da considerarsi come fine, giammai come mezzo per raggiungere i propri obiettivi.

## 6. I rimedi rispetto al contratto concluso dall'utente online vulnerabile e manipolato.

Il divieto di manipolazione e di sfruttamento delle vulnerabilità dell'utente online, desumibile da diverse disposizioni, non stabilisce le sorti del contratto compiuto dalla vittima dell'impiego anti-giuridico della tecnologia. E allora occorre ricostruire il giusto rimedio in coerenza con la natura delle disposizioni coinvolte e con gli interessi da queste protetti.

Si consideri, com'è emerso in precedenza, che tale divieto coinvolge l'essenza del contratto, poiché attiene al piano dell'autonomia privata (art. 1322 c.c.). È stato affermato da un illustre Autore<sup>64</sup> che, con riguardo al contratto, «l'idea fondamentale da cui la legge muove, e che vuole realizzata nell'ordinamento, è che il contratto funzioni come contratto, strumento essenzialmente misurato sul principio di parità e sulla libera determinazione del contenuto ad opera delle parti».

Se manca la libertà non solo nel determinare il contenuto del contratto, ma, ancor prima, nella scelta del se concludere il contratto (l'*an*), viene in rilievo un vizio genetico dello stesso, difettandone un elemento di struttura. Questo difetto di libertà determina, ad avviso di chi scrive, non già l'annullabilità bensì la nullità del contratto. Il che deve essere tenuto fermo, sebbene in queste pagine si sia sostenuto che la manipolazione digitale dell'utente vulnerabile incida sulla sua volontà. Va sottolineato, infatti, che il legislatore europeo ha attribuito alla manipolazione online un disvalore maggiore di quello sotteso ai vizi del consenso, come pure alle pratiche commerciali scorrette. Le quali, sebbene anch'esse vietate dall'art. 5 della direttiva 2005/29/CE e dall'art. 20 cod. cons., non incidono tutte allo stesso modo sulla volontà del consumatore, innescando una pluralità di rimedi<sup>65</sup>. Invece del contratto concluso all'esito della manipolazione online deve essere predicata la nullità.

Il diritto europeo vieta l'immissione sul mercato tanto di sistemi di IA manipolanti o idonei a sfruttare le vulnerabilità dell'utente [art. 5, par. 1 lett. a) e b), AI-Act], quanto di piattaforme parimenti in grado di compromettere la volontà del destinatario (artt. 25 e 26 par. 3 DSA). Questi divieti presidiano non solo l'interesse privato alla salvaguardia della libertà di

<sup>64</sup> G. BENEDETTI, *Tutela del consumatore e autonomia contrattuale*, in *Materiali e commenti sul nuovo diritto dei contratti*, a cura di G. Vettori, Padova, 1999, 809, osserva che quando la legge interviene sul contratto intende garantire e non limitare l'autonomia privata. Ciò emerge con chiarezza dalla legislazione sul consumo e sui contratti tra imprese, in particolare sulla subfornitura, ma anche, spostandoci nell'ambiente digitale, dal citato regolamento (UE) 2022/1925 «relativo ai mercati equi e contendibili nel settore digitale (...)».

<sup>65</sup> C. GRANELLI, *Pratiche commerciali scorrette: le tutele*, in *Enc. dir. (I Tematici), Contratto*, Milano 2021, 825 ss.; ID., *Pratiche commerciali scorrette; tutele individuali*, in *Nuova giur. civ. comm.*, 2019, 1074 ss.; G. DE CRISTOFARO, *Pratiche commerciali scorrette*, in *Enc. dir. Annali*, 2012, 1079 ss.



scelta e della capacità di autodeterminarsi, ma anche l'interesse generale alla salute pubblica, alla protezione dei diritti fondamentali e alla tenuta della democrazia e dello Stato di diritto (cons. 104 e 106 DSA, cons. 1, 7, 8, 27, 28, 61, 176 e artt. 1 AI-Act), oltre a costituire un mezzo per il raggiungimento dell'obiettivo di policy del diritto europeo di garantire un ambiente digitale sicuro, prevedibile e affidabile (artt. 1 e 34 ss. DSA).

La persona manipolata, colpita a causa di una sua fragilità, compie un atto non voluto perché eterodiretto, con conseguente privazione di quella libertà di scelta desumibile in positivo dall'art. 13, co. 1, Cost. e in negativo, dall'art. 41, co. 2 Cost. quale limite all'esercizio dell'iniziativa economica privata.

Se il divieto di manipolazione presidia un interesse privato e pubblico, gli artt. 25 DSA e 5, par. 1 lett. a) e b), AI-Act devono qualificarsi norme imperative<sup>66</sup>. Si aggiunga che la natura imperativa di una norma si desume anche dalla previsione di un sistema di controlli e sanzioni, operanti a prescindere dall'iniziativa dei legittimati ad agire, idoneo a giustificare sul piano razionale la nullità del contratto che viola un determinato disposto di legge<sup>67</sup>. Ed in effetti il DSA indica il Coordinatore dei servizi digitali, da istituirsi in ciascuno Stato membro e la Commissione europea quali controllori del rispetto degli obblighi di tale regolamento (cons. 110, 113, 130-151, artt. 49-60 DSA). Non solo: l'art. 74 DSA attribuisce alla Commissione, successivamente alla decisione di non conformità di cui all'art. 73 DSA, il potere di infliggere al fornitore di piattaforme online e di motori di ricerca, entrambi molto grandi, sanzioni pecuniarie, con un limite massimo, in caso di violazione delle disposizioni del regolamento tra cui, certamente, quella contenuta nell'art. 25 DSA<sup>68</sup>.

Anche l'AI-Act prevede che ciascuno Stato membro debba designare almeno un'autorità di notifica e un'autorità di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del regolamento sull'IA; si prevedono anche altre autorità, sebbene ampi poteri spettino alla Commissione che opera tramite il suo

<sup>66</sup> A. ALBANESE, *Violazione di norme imperative e nullità del contratto*, Napoli, 2003, p. 6 ss. si sofferma a lungo sull'individuazione dei criteri in forza dei quali si debba qualificare imperativa una norma di legge. Egli sostiene che per affermare il carattere imperativo di una norma, occorre previamente accertare la sussistenza di uno specifico elemento di indisponibilità, che può essere dato dal carattere generale dell'interesse protetto, sebbene occorra l'indisponibilità della disciplina dell'atto nullo quale connotato essenziale della nullità; da qui l'inderogabilità, ai fini della sussistenza della imperatività, della regola della rilevanza d'ufficio (per cui il «salvo diverse disposizioni di legge» di cui all'art. 1421 c.c. sarebbe da riferire solo alla legittimazione assoluta). Rileva S. ORLANDO, *Consensus al trattamento e liceità*, cit., p. 344 ss., che sono diverse le norme imperative nel diritto europeo sul digitale che pongono limiti in funzione del rafforzamento dell'autonomia privata.

<sup>67</sup> Così A. ALBANESE, *Violazione di norme imperative e nullità del contratto*, cit., p. 45-59, il quale si sofferma sugli indici espressivi della imperatività. In prospettiva diversa più incentrata sugli interessi coinvolti dalla disposizione di legge G. PASSAGNOLI, *Nullità speciali*, Padova, 1995, 180 ss.

<sup>68</sup> Cfr. anche l'art. 75 DSA sulla «vigilanza rafforzata delle misure correttive tese a rispondere alle violazioni degli obblighi di cui al capo III sezione 5» in cui si prevedono gli obblighi a carico dei fornitori di piattaforme online (e di motori di ricerca) di dimensioni molto grandi di valutare preventivamente i rischi e di adottare misure volte ad attenuarli.

ufficio per l'IA (cons. 152-167 e art. 101 AI-Act). Si disciplina altresì un sistema di sanzioni pubblicistiche (artt. 99 ss. AI-Act), piuttosto articolato, in cui si prevede una sanzione amministrativa pecuniaria a seguito della violazione dell'art. 5 AI-Act.

Deve ammettersi, quindi, che chi utilizza sistemi tecnologici per sfruttare una vulnerabilità dell'utente online, inducendolo a concludere un contratto, si esponga a un'azione di nullità del medesimo.

Non è possibile sviluppare compiutamente in questa sede la questione della disciplina applicabile a tale nullità; la rinvio ad altra sede, anticipando che soltanto l'utente online è legittimato ad agire, configurandosi una nullità di protezione<sup>69</sup>, categoria, questa, predicabile al di là dei casi espressamente previsti dalla legge. Più opportuno è richiamare quel pensiero dottrinale, alimentato dalle disposizioni qui analizzate sul divieto di manipolazione, secondo il quale occorre costruire attorno al consenso privacy, stante la prevalenza nella gerarchia delle fonti del GDPR<sup>70</sup>, «una teoria dell'atto di autonomia privata di diritto europeo»<sup>71</sup>.

Tornando però al tema dei rimedi, oltre alla nullità del contratto, deve ammettersi anche, quale domanda concorrente o autonoma, la risarcibilità dei danni eventualmente subiti dall'utente online. Il cumulo dei rimedi discende da quegli studi dottrinali, penetrati nella giurisprudenza, secondo i quali «esiste una dimensione giuridica diversa dalla fattispecie» sulla validità/efficacia del contratto. Si vuol dire che i comportamenti delle parti, estranei alla fattispecie contrattuale, possono essere rilevanti anche rispetto a un contratto valido ed efficace<sup>72</sup>.

Questa impostazione dottrinale e giurisprudenziale consente una considerazione ulteriore: se il comportamento rileva a prescindere dalla fattispecie contrattuale, un tale rilievo deve valere anche rispetto a un contratto nullo<sup>73</sup>, come ha chiarito la Corte di Giustizia<sup>74</sup>. L'autonomia

<sup>69</sup> M. GIROLAMI, *Nullità di protezione, Enc. dir. (I tematici), Contratto*, Milano, 723, considera la nullità di protezione come una figura autonoma, un *tertium genus* di invalidità che si aggiunge, «senza scardinare l'assetto tradizionale della materia», alla nullità classica e all'annullabilità. Diverse sono le posizioni in dottrina sulla configurabilità della nullità di protezione oltre i casi previsti dalla legge; quella che si va affermando l'ammette. Cfr. in aderenza al tema L. TAFARO, *Neuromarketing e tutela del consenso*, cit., 128 ss.

<sup>70</sup> Sono diversi i riferimenti normativi contenuti nel DSA e nell'AI-Act in cui si fa salva l'applicazione del GDPR.

<sup>71</sup> S. ORLANDO, *Consenso al trattamento e liceità*, cit., 362-364.

<sup>72</sup> Cass., 29.9.2005, n. 19024, in *Foro it.*, 2006, I, c. 1105 ss. e Cass., S.U. 19.12.2007, n. 26724-26725, in *Violazione degli obblighi di informazione nei servizi di investimento e rimedi contrattuali (a proposito di Cass., S.U., 19 dicembre 2007, nn. 26724 e 26725)*, in *Contr. e impr.*, 2008, 4-5, p. 936 ss. Queste pronunce sono state commentate da un'ampia larga parte della dottrina. Successivamente cfr. F. RENDE, *Violazione di regole informative e rimedi a dieci anni dalle sentenze Rordorf*, in *I contratti*, 2017, n. 2, 201 ss.

<sup>73</sup> G. BENEDETTI, *La rescissione*, cit., p. 48 e G. VETTORI, *Autonomia privata e contratto giusto*, in *Riv. dir. priv.*, 2000, 1, 21 ss. concordano nel ritenere che l'ottica della fattispecie «non assorbe tutta la problematica dell'area contrattuale, specie con riferimento ai rimedi giudiziali, sicché essa non può costituire impedimento ad altre prospettive». Si ritrova una traccia significativa di questa teoria anche in un passaggio di Cass., S.U., 11.11.2008, n. 26972/2008, in *Contr. e impr.*, 2009, 3, 589 ss., con nota di S. MAZZAMUTO, *Il rapporto tra gli artt. 2059 e 2043 c.c. e le ambiguità delle Sezioni unite a proposito della risarcibilità del danno non patrimoniale*, la quale, com'è noto, ha accolto la lettura costituzionalmente



dell'azione risarcitoria rispetto a quella demolitoria si fonda sulla diversità dei titoli e quindi della fonte di responsabilità; titoli che trovano una rispondenza nella legge.

Questo punto è stato chiarito, oltre che dalla dottrina, dalla sentenza Cir/Fininvest<sup>75</sup>, la quale ha ammesso la legittimità di un'autonoma azione di risarcimento del danno ai sensi dell'art. 2043 c.c. in luogo dell'impugnazione della transazione – basata su una sentenza corrotta, pure impugnabile ai sensi dell'art. 395 c.p.c. – per errore di fatto o ai sensi dell'art. 1972, co. 2, c.c. L'autonomia rimediabile è giustificata dalla impossibilità di esperire le impugnative contrattuali perché inutili o scarsamente soddisfacenti ai fini della tutela dell'interesse leso, venendo, a tal proposito, in rilievo il principio costituzionale di effettività della tutela<sup>76</sup>. Principio che, come è stato affermato, non si sostituisce al diritto o all'obbligazione, ma contribuisce alla conversione del fatto in diritto, fornendo al contempo una tutela adeguata<sup>77</sup>.

Questa soluzione trova sostegno, secondo la sentenza CIR/Fininvest, oltre che nell'art. 402 c.p.c. – che menziona le restituzioni nella fase rescissoria e non il risarcimento del danno sottendendone l'autonomia – soprattutto nell'art. 30 del codice della giustizia amministrativa (d. lgs. n.

---

orientata dell'art. 2059 c.c. fornita dalle sentenze gemelle della Cassazione n. 8827 e n. 8828/2003, completandola. Sostengono le Sezioni unite che «anche nella materia della responsabilità contrattuale è dato il risarcimento dei danni non patrimoniali» (§ 4.1), senza necessità del cumulo dei rimedi. Si afferma, infatti, che «se l'inadempimento dell'obbligazione determina, oltre alla violazione degli obblighi di rilevanza economica assunti con il contratto, anche la lesione di un diritto inviolabile della persona del creditore, la tutela risarcitoria del danno non patrimoniale potrà essere versata nell'azione di responsabilità contrattuale, senza ricorrere all'espedito del cumulo di azioni». La stessa condotta, quindi, stante la causa concreta del contratto, lede due disposizioni di legge, facendo scattare due rimedi.

<sup>74</sup> Corte di Giustizia, 20.9.2001, causa C-453/99, caso *Courage*, in *eur-lex.europa.eu*.

<sup>75</sup> Cass., 17.9.2013, n. 21255, sez. III civ., in *Danno e resp.*, 2015, 11, 1029 ss., con note di G. PAGANO, G. PONZANELLI e M. FRANZONI; in *Danno e resp.*, 2014, 2, 139 ss., con note di P. SANTORO, G. PONZANELLI, G. IMPAGNATIELLO, G. VETTORI, A. PALMIERI-R. PARDOLESI-A. ROMANO, G. LENER, B. TASSONE, R. SIMONE, P.G. MONATERI. Cfr. anche V. ROPPO, *Spunti in tema di responsabilità «pericontrattuale»*, *Dialogo con Giorgio De Nova a margine della sentenza di cassazione sul lodo Mondadori*, in *Resp. civ. prev.*, 2014, 1, 16 ss.; C. SCOGNAMIGLIO, *Effettività della tutela e rimedio risarcitorio per equivalente: la Cassazione sul caso Cir c. Fininvest*, *ivi*, 42 ss.; G. IUDICA, *Contratto e responsabilità civile. A margine della sentenza della Cassazione n. 21255 del 2013*, *ivi*, 8 ss. La vicenda giudiziaria, complessa e notissima, muove dalla contesa della proprietà azionaria del Gruppo Mondadori tra Cir e Fininvest.

<sup>76</sup> Cass., 17.9.2013, n. 21255, sez. III civ., cit., § 3.4.2, p. 69-70, intende il principio di effettività «come diritto a un rimedio adeguato al soddisfacimento del bisogno di tutela, di quella specifica, unica, talvolta irripetibile situazione sostanziale di interesse giuridicamente tutelato».

<sup>77</sup> G. VETTORI, *Effettività delle tutele*, in *Enc. dir., Annali X*, Milano, 2017, 395 e 403-405, reca molti esempi tratti della giurisprudenza, interna e sovranazionale, in cui l'apporto del principio di effettività alla conversione del fatto in diritto e alla individuazione del rimedio più adatto all'interesse protetto – due facce della stessa medaglia – è piuttosto evidente. L'A. chiarisce altresì che in questa conversione di cui Egli discorre è possibile dar rilievo a interessi «non formalizzati nella fattispecie o che la fattispecie non ha saputo indicare in modo pieno» (p. 404).



104/2010), in cui il risarcimento del danno è considerato unitamente alla (o separatamente dalla) azione demolitoria.

È senz'altro vero che quest'ultima disposizione esprime un principio di settore, ma ad essa si è aggiunto un dato normativo nuovo che avvalorata la conclusione dell'autonomia del rimedio risarcitorio da quello invalidante: è l'art. 3 della direttiva (UE)/2019/2161, c.d. direttiva *omnibus*, il cui punto 5 ha modificato la direttiva sulle pratiche commerciali scorrette, prevenendo l'inserimento in quest'ultima dell'art. 11-*bis*, a tenore del quale: «i consumatori lesi da pratiche commerciali sleali devono avere accesso a rimedi proporzionati ed effettivi, compresi il risarcimento del danno subito dal consumatore e, se pertinente, la riduzione del prezzo o la risoluzione del contratto». Il risarcimento del danno, quindi, sembra aggiungersi ad altri rimedi «proporzionati ed effettivi», tra cui può ben esservi la nullità del contratto compiuto per effetto della manipolazione/sfruttamento della vulnerabilità<sup>78</sup>.

Anche l'art. 14 («rimedi») della sopra menzionata Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale pone l'accento sulla pluralità dei rimedi; esso stabilisce che gli Stati parte, in ossequio agli obblighi internazionali e in coerenza con il proprio sistema giuridico, adottano o mantengono «misure per garantire la disponibilità di rimedi accessibili ed efficaci per le violazioni dei diritti umani derivanti dalle attività del ciclo di vita dei sistemi di intelligenza artificiale».

È noto che il diritto europeo e internazionale non ponga limiti teorici all'utilizzo dei rimedi e lasci gli Stati liberi di decidere, purché i rimedi, al plurale, siano di agevole utilizzo, efficaci ed effettivi. Ma pur volendo mantenere il discorso sul piano della teoria del diritto, è proprio il concetto di procedimento, più ampio e dinamico rispetto a quello di fattispecie<sup>79</sup>, che consente di superare l'assenza di effetti giuridici (non già l'inesistenza)<sup>80</sup> del contratto nullo; procedimento nel quale rileva il rapporto tra le parti, le cui dinamiche possono evocare gli artt. 1337, 2043 o 2059 c.c. e quindi la risarcibilità del danno<sup>81</sup>.

La mancanza di effetti del contratto non esclude necessariamente la possibilità di richiedere il risarcimento del danno in caso di violazione di un obbligo legislativo, come quello di valutare preventivamente i rischi connessi all'impiego di una certa tecnologia digitale, o il rischio di ledere un diritto fondamentale come la salute.

<sup>78</sup> G. VETTORI, *Validità, responsabilità e cumulo dei rimedi*, in *Persona e mercato*, 2013, 4, 279 ss., argomenta, tendendo conto delle posizioni dottrinali contrarie, a favore del cumulo dei rimedi, perché regole di validità e di responsabilità sono autonome; le une non assorbono le altre nei limiti della compatibilità. ID., *Effettività delle tutele*, cit., p. 390.

<sup>79</sup> G. BENEDETTI, *La rescissione*, cit., 46; G. VETTORI, *Anomalie e tutele nei rapporti di distribuzione tra imprese*, cit., 75 ss. e p. 112; F. BENATTI, *La responsabilità precontrattuale*, 1963, rist. anastatica, a cura di P. Perlingieri, Napoli, 2012, 108-109.

<sup>80</sup> G. FILANTI, *Inesistenza e nullità del negozio giuridico*, Napoli, 1983, 19 ss.

<sup>81</sup> Cass., 17.9.2013, n. 21255, sez. III civ., cit., § 3, 101, afferma che «le regole di comportamento [la cui fonte è il contratto, l'art. 1337 o l'art. 2043 c.c.] sono disciplina non di fattispecie ma di rapporto, non attengono al fatto rilevante per i terzi e per l'ordinamento, ma alla vicenda obbligatoria che intercorre(rà) tra le parti».



L'utente online manipolato potrà dunque richiedere la nullità del contratto e il risarcimento del danno oppure soltanto quest'ultimo rimedio, a seconda dell'interesse fatto valere e del titolo giustificativo della pretesa risarcitoria<sup>82</sup>.

---

<sup>82</sup> Il tema del risarcimento del danno presenta diversi aspetti controversi e delicati; in questa sede non si può che effettuare un rinvio a G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, cit., 60 ss. e, per un approfondimento, a T. DE MARI CASARETO DAL VERME, *Intelligenza artificiale e responsabilità. Uno studio sui criteri di imputazione*, Napoli, 2024. Sul tema della soggettività digitale cfr.: G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019 e le considerazioni, scettiche sulla soggettivizzazione, di G. PASSAGNOLI, *Ragionamento giuridico e tutele nell'intelligenza artificiale*, in *Persona e mercato*, 2019, 3, 79 ss. (in part. 82).



