DIGITAL SERVICES ACT E ARTIFICIAL INTELLIGENCE ACT: TENTATIVI DI FUTURO DA ARMONIZZARE

Di Sara Tommasi

ABSTRACT. ***Il saggio mira a dimostrare che i prestatori di servizi digitali pongono in essere attività e offrono servizi potenzialmente rientranti nell'ambito di applicazione sia del Digital Services Act sia dell'Artificial Intelligence Act. Ne consegue la necessità di un coordinamento tra le due discipline. Entrambe rappresentano diverse espressioni di un approccio basato sul rischio ed evidenziano i profili problematici dei sistemi di intelligenza artificiale che condizionano i comportamenti degli utenti dei servizi digitali.***

The essay aims to show that the activities of providers and the services they offer potentially fall within the scope of both the Digital Services Act and the Artificial Intelligence Act. Hence the need to coordinate these two disciplines. Both represent different expressions of a risk-based approach and highlight the problematic profiles of artificial intelligence systems that condition the behavior of users of digital services.

1. Premessa.

Il *Digital Services Act*[1] e l'*Artificial Intelligence Act*[2] sono un punto di riferimento imprescindibile nella regolamentazione del futuro che, proprio in ragione del veloce e inarrestabile cambiamento tecnologico, si presenta sempre più imprevedibile e diverso dal passato.[3] Entrambi gli atti normativi si basano su un modello incentrato sul rischio e sulla sua gestione.[4]

Il *risk approach*, nella prospettiva europea, consente di non ostacolare l'innovazione tecnologica attraverso restrizioni eccessive, ma di governarla con obblighi e responsabilità proporzionali al grado di rischio introdotto nel sistema.[5] L'obiettivo è delineare un quadro giuridico adeguato dinamicamente all'evoluzione tecnologica e all'emergere di nuove situazioni di preoccupazione nel rispetto dei diritti fondamentali e dei valori dell'Unione.[6]

[1] *Regulation (EU) 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)* in *https://eur-lex.europa.eu.* Per una illustrazione dettagliata e aggiornata delle nuove regole introdotte dal *Digital Services Act* si rimanda alla Circolare *Mercato unico dei servizi digitali: il Digital Services Act*, del 12 giugno 2023, dell'Associazione fra le società italiane per azioni, in *https://www.assonime.it/attivita-editoriale/circolari/Pagine/Circolare-17_2023.aspx.*

[2] COM (2021) 206 final*, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence. (Artificial Intelligence Act) and amending certain union legislative acts* in *https://eur-lex.europa.eu*. Il Regolamento è attualmente in fase di proposta, ma l'iter legislativo è in fase conclusiva. Si vedano gli *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1*, in *https://www.europarl.europa.eu.* Gli emendamenti di giugno 2023 sono stati preceduti dal *Draft Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* del 15 maggio 2023, in *https://www.europarl.europa.eu.*

[3] Cfr. A. De Franceschi, R. Schulze, M. Graziadei, O. Pollicino, F. Riente, S. Sica, Sirena (a cura di), *Digital Revolution. New Challenges for Law*, München, 2019; A. Iannarelli, *La regolazione privatistica delle relazioni di mercato nell'attuale contesto*, in *Riv. crit. dir. priv.,* 2020, 320 ss.

[4] G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Diritto dell'informazione e dell'informatica,* 2022, 303 ss. M. Cornils, *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries* in *https://algorithmwatch.org.,* 2020, 25, nota che «with regard to the risks for the news ecosystem arising from platform communication, the phenomena of so-called strategic communication can be distinguished from those of an unintended degeneration of democratic discourse inherent in the functioning and business models of intermediaries – especially social media platforms. While the former is – in principle – little disputed as a disturbing and potentially harming factor and thus, in principle, as a regulatory challenge, the possibility, necessity and legal justifiability of regulatory measures in the latter area are much less clear and more controversial». Cfr. J. Chamberlain, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *European Journal of Risk Regulation*, 2022, 1 ss. D. Iacovelli, M. Fontana, *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici,* in *Il diritto dell'economia*, 2022, 107 ss.

[5] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2022, 473 ss., affermano che ‹‹in the last years, risk has become a proxy and a parameter characterizing the European regulation of digital technologies. Nonetheless, the European risk-based regulation in the digital age is multi-faceted in the approaches it takes››.

[6] L'attenzione a uno sviluppo tecnologico che non avvenga a scapito del rispetto dei diritti fondamentali e dei valori dell'Unione Europea si riscontra in recenti provvedimenti, quali: *European Parliament resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020/2022(INI))* in *https://www.europarl.europa.eu.; European Declaration on Digital Rights and Principles for the Digital Decade, Brussels,* COM(2022) 28 final, in *https://ec.europa.eu*. Sul punto cfr. F. Z. Borgesius, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, in *The International Journal of Human Right*s, 2020, 2 ss. S. Tommasi, *La proposta di Dichiarazione europea sui diritti e i principi digitali per il decennio digitale COM(2022) 28 final del 26 gennaio 2022*, in *Persona e mercato, Diritto e nuove tecnologie. Rubrica di aggiornamento dell'OGID,* 2022, 168 ss.; R. Alfonsi, *La EU Interinstitutional declaration on digital rights and principles del 14.11.2022*, in *Persona e mercato, Diritto e nuove tecnologie. Rubrica di aggiornamento dell'OGID*, 2022, 707 ss.; G. Resta, *Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in *Diritto dell'Informazione e dell'Informatica*, 2022, 327. L'Autore afferma, con riferimento alla Proposta di Regolamento UE sull'intelligenza artificiale, che il cardine della proposta sembra risiedere nella definizione di un modello regolatorio finalizzato alla gestione ottimale dei rischi insiti nell'utilizzo dei dispositivi di intelligenza artificiale, con l'obiettivo primario di tutela dei diritti fondamentali e di salvaguardia del processo democratico. Cfr. sul punto C. Perlingieri, *Profili civilistici dei social networks*, Napoli, 2014, 84 ss.; N. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li, J. Maclaren, R. Piselli, K. Yeung, *How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act,* in *https://ssrn.com/abstract=3899991*, 2021, 14 ss.; D. Imbruglia, *Note sulla regolazione della IA*, in S. Orlando, G. Capaldo (a cura di), *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, 157 ss. A. F. Uricchio, G. Riccio, U. Ruffolo (a cura di), *Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea,* Bari, 2020; E. Calzolaio, *Introduzione*, in E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale,* Milano, 2020, 1*;* A. Alpini, *Sull'approccio umano-centrico all'intelligenza artificiale. Riflessioni a margine del "Progetto europeo di orientamenti etici per una IA affidabile"*, in *www.comparazionedirittocivile.it;* S. Tommasi, *L'intelligenza artificiale antropocentrica: limiti e*

Come nel *Digital Services Act*, anche nell'*Artificial Intelligence Act*, si delinea una logica proporzionale e cumulativa nell'imposizione di obblighi a mano a mano che aumentano i rischi. Segnatamente, nel *Digital Services Act* ha un ruolo centrale il rischio sistemico, mentre nell'*Artificial Intelligence Act* sono individuati quattro livelli di rischio*: unacceptable risk, high risk, limited risk and minimal risk*. I due poli opposti sono i sistemi che hanno un rischio inaccettabile, e in quanto tali sono vietati, e i sistemi che hanno un rischio minimo e, dunque, sono per lo più destinatari di soli obblighi di trasparenza, in modo da rendere gli utenti consapevoli del loro utilizzo. Nel mezzo si collocano i sistemi ad alto rischio che sono quelli per i quali sono previsti rigorosi obblighi prima della loro immissione nel mercato e un monitoraggio successivo.[7]

Si tratta, in ogni caso, di sistemi che sono in costante evoluzione e si inseriscono in un processo continuo che pone numerose difficoltà e che deve essere proporzionato al contesto specifico in cui si opera e all'impatto che tali sistemi possono avere. [8]

Un confronto tra il *Digital Services Act* e l'*Artificial Intelligence Act* è ormai indispensabile, considerato che i fornitori di servizi digitali utilizzano sempre più sistemi di intelligenza artificiale e quindi pongono in essere attività e offrono servizi potenzialmente rientranti nell'ambito di applicazione di entrambi gli atti normativi in oggetto.

2. Intermediazione nei servizi digitali e utilizzo di sistemi di intelligenza artificiale.

Numerosi sono gli esempi di utilizzo di sistemi di intelligenza artificiale da parte dei prestatori di servizi digitali.

Il Considerando 70) del *Digital Services Act* specifica che un elemento essenziale dell'attività di una piattaforma online consiste nel modo in cui le informazioni sono messe in ordine di priorità e presentate nell'interfaccia online per facilitare e ottimizzare l'accesso alle stesse da parte dei destinatari del servizio. A tal fine sono utilizzati algoritmi che classificano e mettono in ordine di priorità le informazioni, distinguendole attraverso testo o altre rappresentazioni visive oppure selezionando in altro modo le informazioni fornite dai destinatari.[9] Ciò avviene attraverso i sistemi di raccomandazione definiti, *ex* art. 3 (s) del *Digital Services Act*, come «quei sistemi interamente o parzialmente automatizzati che una piattaforma online utilizza per suggerire informazioni specifiche, tramite la propria interfaccia online, ai destinatari del servizio o mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate».[10]

I sistemi che utilizzano tali algoritmi non possono non ricadere anche nel campo di applicazione dell'*Artificial Intelligence Act*, se solo si considera la stessa definizione di sistema di intelligenza artificiale che, infatti, fa riferimento a un sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare *output* come raccomandazioni.[11]

opportunità, in *Juscivile*, 2020, 853 ss.; E. Fazio, *Intelligenza artificiale e diritti della persona*, Napoli, 2023.

[7] S. Orlando, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, in *Persona e Mercato*, 2022, 346 ss.

[8] Cfr. B. Wagner, *Ethics as an Escape from Regulation: From Ethics-washing to Ethics-shopping?*, in M. Hildebrandt (a cura di), *Being Profiled. Cogitas ergo sum*, 2018, in *https://pdfs.semanticscholar.org,* 1 ss. A. Jabłonowska, M. Kuziemski, A. M. Nowak, H. W. Micklitz, P. Pałka, G. Sartor *Consumer law and artificial intelligence: challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence: final report of the ARTSY project*, in *EUI Law*, 2018, 17. Ivi si afferma che «there is not one AI problem, and there will be not one solution to challenges posed by AI. On the contrary, the response will be different across the sectors, both regarding the substance and form of the potential regulatory response».

[9] C. Busch, V. Mak, *Putting the Digital Services Act in Context*, in *Journal of European Consumer and Market Law*, 2021, 109 ss.

[10] R. Montinaro, *Sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi,* in *Persona e Mercato*, 2022, 368 ss.

[11] In COM(2021) 206 final*, Proposal for a Regulation,* cit., si definisce sistema di intelligenza artificiale un software che, per un dato insieme di obiettivi definiti dall'uomo, genera risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce. La definizione è stata oggetto di vari emendamenti, fino all'emendamento 165 degli *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence*, cit. Non si fa più riferimento, infatti, ad ‹‹un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono››, ma ad ‹‹un sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare *output* quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali››. Una definizione di intelligenza artificiale si rinviene anche nella *Proposition de loi constitutionnelle relative à la Charte de l'intelligence artificielle et des algorithmes*, depositata il 15

Il prestatore di servizi digitali, dunque, qualora utilizzi sistemi di intelligenza artificiale, sarà destinatario di quanto previsto dall'*Artificial Intelligence Act*, indipendentemente, e a prescindere, da altre specifiche disposizioni del *Digital services Act* e anche dalla distinzione tra *hosting*, motori di ricerca e piattaforme online o motori di ricerca o piattaforme di grandi dimensioni, che è alla base dei diversi obblighi delineati dal *Digital services Act*.

Ai prestatori di servizi digitali potrebbe essere applicabile, per esempio, la previsione dell'art. 52 dell'*Artificial Intelligence Act*, nella misura in cui risultino utenti di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica al quale possono essere esposte persone fisiche. Queste, infatti, devono essere informate in merito al funzionamento del sistema. Inoltre, sempre ai sensi del citato articolo 52, anche ai prestatori di servizi digitali, che siano utenti di un sistema di intelligenza artificiale che genera o manipola immagini o contenuti audio o video che rappresentano persone che sembrano dire cose che non hanno detto o compiere atti che non hanno commesso, senza il loro consenso, sono tenuti a rendere noto in modo adeguato, tempestivo, chiaro e visibile che il contenuto è stato generato o manipolato.[12]

Un altro esempio di uso frequente di sistemi di IA da parte dei prestatori di servizi digitali è quello relativo alla moderazione dei contenuti. I *provider* si affidano spesso a tecniche e mezzi di ricerca automatizzati, pur nella consapevolezza di non riuscire a cogliere le peculiarità del contesto nel quale sono inserite determinate frasi, rischiando, per esempio, di bloccare contenuti erroneamente di natura offensiva.

Uno dei principali dilemmi per gli operatori degli algoritmi di rilevamento del contenuto è se dare la priorità agli errori di rimozione eccessiva, i cosiddetti falsi positivi, o agli errori di rimozione insufficiente, i cosiddetti falsi negativi. Una rigorosa politica di rimozione dei contenuti si tradurrà in un alto tasso di falsi positivi che danneggia la libertà di espressione della persona il cui contenuto è stato erroneamente rimosso. Una politica meno rigida si tradurrà in un alto tasso di falsi negativi che danneggia le vittime del contenuto che avrebbe dovuto essere rimosso[13].

Una certa cautela nell'utilizzo di strumenti automatizzati emerge chiaramente nel *Digital Services Act*. Ai sensi dell'art. 16, infatti, i prestatori di servizi di *hosting*, qualora usino strumenti automatizzati nel trattare le notifiche ricevute e adottare decisioni, devono necessariamente includere informazioni sull'uso di tali strumenti. Qualora, inoltre, un prestatore di servizi di *hosting* decida di rimuovere specifiche informazioni fornite dai destinatari del servizio o disabilitare l'accesso alle stesse, ai sensi dell'art. 17 del *Digital Services Act*, deve informare il destinatario della decisione, al più tardi al momento della rimozione o della disabilitazione dell'accesso, fornendo una motivazione chiara e specifica di tale decisione; motivazione che deve contenere informazioni sia sugli strumenti automatizzati usati per adottare la decisione, sia su eventuali contenuti individuati o identificati per mezzo di tali strumenti.

Inoltre, per quanto riguarda le piattaforme online, il *Digital Services Act* è esplicito nel vietare l'uso esclusivo di strumenti automatizzati nella gestione interna dei reclami e impone, tra gli obblighi di comunicazione trasparente per i fornitori di piattaforme online, ai fini della relazione di cui all'art. 15, di fornire informazioni su qualsiasi uso di strumenti automatizzati ai fini di moderazione dei contenuti, compresi la descrizione delle finalità precise, gli indicatori di accuratezza degli strumenti automatizzati nel perseguimento di tali scopi e le eventuali garanzie applicate. Il fine esplicito, come si evince dal comma 4 dell'art. 20, è che i reclami siano gestiti in modo non discriminatorio, sotto il controllo di personale qualificato e assicurando che le decisioni non siano prese avvalendosi esclusivamente di strumenti automatizzati.

Non c'è però ancora una adeguata attenzione alla figura dei moderatori dei contenuti, limitandosi l'art. 15 a prevedere, tra gli obblighi di comunicazione trasparente per i prestatori di servizi intermediari, anche quello relativo alle misure adottate per fornire formazione e assistenza ai membri del personale impegnato nella moderazione dei conte-

gennaio 2020, in Francia, presso l'*Assemblée Nationale,* ove si legge che «la présente charte s'applique à tout système qui se compose d'une entité qu'elle soit physique (par exemple un robot) ou virtuelle (par exemple un algorithme) et qui utilise de l'intelligence artificielle. La notion d'intelligence artificielle est entendue ici comme un algorithme évolutif dans sa structure, apprenant, au regard de sa rédaction initiale. Un système tel que défini au précédent alinéa n'est pas doté de la personnalité juridique et par conséquent inapte à être titulaire de droits subjectifs. Cependant les obligations qui découlent de la personnalité juridique incombent à la personne morale ou physique qui héberge ou distribue ledit système devenant de fait son représentant juridique».

[12] Si veda l'emendamento 486 degli *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence,* cit.

[13] W. MAXWELL, *Applying Net neutrality rules to social media content moderation systems*, in *Annales des Mines – Enjeux Numérique,* 2022, 90.

nuti.[14] Eppure, il ruolo dei moderatori è molto delicato, perché se da una parte garantiscono un controllo umano, dall'altra sono deputati ad assumere decisioni che, potendo incidere su diritti fondamentali, dovrebbero essere prese da soggetti, e secondo modalità, che assicurino adeguate garanzia di tutela.[15]

L'utilizzo di sistemi di intelligenza artificiale da parte degli intermediari di servizi digitale impone una riflessione sulla necessità di un coordinamento tra *Digital Services Act* e *Artificial Intelligence Act*.

3. *Digital Services Act* e *Artificial Intelligence Act*: la necessità di un coordinamento.

Un primo dato dal quale partire nella riflessione sulla necessità di un coordinamento tra i provvedimenti in oggetto è il rapporto tra rischi sistemici ai sensi del *Digital Services Act* e sistemi ad alto rischio così come definiti dall'*Artificial Intelligence Act*.

L'*Artificial Intelligence Act* contiene le regole di classificazione per i sistemi di intelligenza artificiale ad alto rischio. Segnatamente, ci sono tre casi nei quali un sistema di intelligenza artificiale può essere classificato ad alto rischio. Il primo caso è quello riconducibile all'art. 6, primo comma dell'*Artificial Intelligence Act*, ai sensi del quale un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione Europea elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di intelligenza artificiale, o il sistema di intelligenza artificiale stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi "related to risks for health and safety"[16] ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.[17]

Il secondo comma dell'art. 6 dell'*Artificial Intelligence Act* prevede che sono considerati ad alto rischio anche i sistemi di intelligenza artificiale di cui all'allegato III dello stesso *Artificial Intelligence Act* se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche. Qualora un sistema di IA rientri nell'allegato III, punto 2, è considerato ad alto rischio se presenta un rischio significativo di danno per l'ambiente.[18]

Ai sensi dell'allegato III dell'*Artificial Intelligence Act*, i sistemi di intelligenza artificiale ad alto rischio possono essere quelli elencati nei settori individuati dallo stesso allegato e segnatamente: sistemi biometrici e basati su elementi biometrici; gestione e funzionamento delle infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi; attività di contrasto; gestione della migrazione, dell'asilo e del controllo delle frontiere; amministrazione della giustizia e processi democratici.

La possibilità di classificare altri sistemi di intelligenza artificiale ad alto rischio è prevista dall'art. 7 dell'*Artificial Intelligence Act*. Prima degli emendamenti adottati dal Parlamento Europeo il 14 giugno 2023, si trattava di una possibilità limitata ai sistemi destinati a essere usati soltanto in uno dei settori indicati dall'allegato III. Le modifiche previste dagli emendamenti adottati dal Parlamento Europeo il 14 giugno 2023, in particolare dall'emendamento 238, consentono alla Commissione di aggiungere o modificare settori o casi d'uso di sistemi di intelligenza artificiale ad alto rischio, ‹‹se questi presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, sull'ambiente o sulla democrazia e sullo Stato di

[14] Su queste problematiche si rimanda a J. Franchi, *Gli obsoleti. Il lavoro impossibile dei mediatori di contenuti*, Milano, 2021.

[15] Sulla circostanza che il principale tipo di problema posto dalle nuove tecnologie derivi dall'attribuzione di potere normativo a quel potere diffuso, non conosciuto, insito nelle regole tecniche delle piattaforme si rimanda a A. Federico, *Il* nomos *della 'infosfera',* in *Rass. dir. civ*., 2022, 533 ss.; S. Thomas, *Horizontal Restraints on Platforms: How Digital Ecosystems Nudge into Rethinking the Construal of the Cartel Prohibition,* in *World Competition*, 2021, 53.

[16] Il riferimento specifico ai rischi per la salute e la sicurezza è un'aggiunta prevista nell'emendamento 233 degli *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence*, cit.

[17] Molti sistemi di intelligenza artificiale ad alto rischio sono utilizzati come componenti di sicurezza di prodotti già esistenti. In questo caso, anche al fine di evitare duplicazioni, non si procede a valutazioni di conformità specifiche, ma si terrà conto della valutazione di conformità già prevista in ciascun settore. Cfr. J. Mökander, M. Axente, F. Casolari, L. Floridi, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation. Minds & Machines,* 2021, 9.

[18] Emendamento 234 degli *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence*, cit.

diritto e tale rischio è, in relazione alla sua gravità e alla probabilità di insorgenza, equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio già indicati nell'allegato III››. L'emendamento è da accogliere con favore, dato che, anche se stride con la nostra sensibilità giuridica che gli effetti negativi sui diritti fondamentali siano relegati a settori indicati in un elenco, è un passo avanti la previsione che tale elenco non sia tassativo e possa essere ampliato.

I sistemi che incidono negativamente sui diritti fondamentali, in alcuni casi, possono rientrare tra quelli considerati ad alto rischio dall'*Artificial Intelligence Act* e generare quelli che per il *Digital Services Act* sono rischi sistemici. In entrambi i casi il rischio di effetti negativi sui diritti fondamentali non è considerato inaccettabile, ma solo un rischio rispetto al quale occorre prendere delle precauzioni. Ciò non significa che ci sia una perfetta coincidenza tra "rischio sistemico" ai sensi del *Digital Service Act* e "alto rischio" in base all'*Artificial Intelligence Act* e che non si pongano problemi di coordinamento. Basti pensare che, per il *Digital Services Act,* i rischi sistemici sono soltanto quelli che possono derivare dall'attività di piattaforme o motori di ricerca di dimensioni molto grandi, anche se indipendentemente da un elenco di settori.

Il *Digital Services Act* considera rischi sistemici, tra gli altri, gli eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare per l'esercizio dei diritti fondamentali alla dignità umana, al rispetto della vita privata e familiare, alla tutela dei dati personali, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, e alla non discriminazione, al rispetto dei diritti del minore e all'elevata tutela dei consumatori.[19] Ugualmente, è considerato rischio sistemico ‹‹qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona››.[20]

L'*Artificial Intelligence Act* riguarda tutti i soggetti che utilizzano sistemi di intelligenza artificiale e non solo le piattaforme di grandi dimensioni. Quindi il non essere piattaforma di grandi dimensioni esonera dagli adempimenti previsti dal *Digital Services Act* per i rischi sistemici, ma non dal doversi adeguare all'*Artificial Intelligence Act* nel caso di utilizzo di sistemi di intelligenza artificiale. A ciò è collegato un altro aspetto molto interessante che distingue il *Digital Services Act* dall'*Artificial Intelligence Act*. Nel *Digital Services Act*, infatti, sono previsti obblighi distinti in misura proporzionale anche alle dimensioni degli intermediari di servizi digitali.[21] L'*Artificial Intelligence Act* prevede, invece, medesimi obblighi a prescindere dalle dimensioni dell'impresa. Anche da questo punto di vista, dunque, c'è un difetto di coordinamento tra i due provvedimenti. La conseguenza è che imprese di piccole dimensioni avranno inevitabilmente molte più difficoltà a gestire gli oneri previsti dall'*Artificial Intelligence Act*, rispetto alle società di grandi dimensioni, con un ulteriore effetto discriminatorio nell'accesso al mercato.[22]

[19] Si veda l'art. 34 (B) del *Digital Services Act.*
[20] Si veda l'art. 34 (D) del *Digital Services Act.*

[21] Il *Digital Services Act* è complementare al *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital*, noto come *Digital Markets Act,* che è diretto principalmente a tutelare ‹‹smaller European competitors against US 'big tech'››. Nel *Digital Markets Act*, nonostante alcuni riferimenti espliciti anche alla protezione degli utenti finali, questi ultimi hanno solo dei benefici indiretti. La finalità del *Digital Markets Act* è prevedere azioni di enforcement "ex ante" per garantire mercati competitivi sotto la minaccia di multe molto elevate. In questo modo, i concorrenti più piccoli non avrebbero più bisogno di ricorrere all'attuale sistema di *enforcement ex post* contro gli abusi di potere monopolistico, che si ritiene non sia sufficientemente attrezzato per affrontare il potere monopolistico digitale. Sul punto cfr. P. BERGKAMP, *The Proposed EU Digital Markets Act: A New Era for the Digital Economy in Europe*, in *European Review of Private Law*, 2021, 152 ss.; V. A. AIGNER, *Der Digital Services Act der Eu- das neue Grundgesetz in digitalen Zeitalter?,* Universität Linz, 2021, 7 ss.; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in *Quaderni Aisdue*, 2021, 189 ss.

[22] Sul tema della non discriminazione nell'accesso delle imprese al mercato digitale si veda il *Digital Markets Act*, ove la non discriminazione è intesa come difesa della contendibilità, nel settore digitale, tra i prodotti e i servizi offerti dai diversi *"Business user".* Segnatamente nel *Digital Markets Act* si tiene conto della discriminazione nelle condizioni di accesso e permanenza delle imprese nel mercato digitale e si ritiene che questa discriminazione possa dipendere principalmente da due fattori. Il primo fattore è legato al fatto che i *gatekeeper* hanno un impatto significativo sul mercato interno, agiscono come un'importante via d'accesso per gli utenti commerciali per raggiungere gli utenti finali. Il secondo fattore è legato al fatto che l'accesso dei *gatekeeper* a dati di *ranking, query, click* e visualizzazioni costituisce un'importante barriera all'ingresso e all'espansione, che mina la contendibilità dei servizi dei motori di ricerca online. Si vedano, sul punto, I. GRAEF, *Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence*, in *Yearbook of European Law,* 2019, 448 ss., disponibile in *https://doi.org/10.1093/yel/yez008*; P. S. ATTRI, H. BAPUJI, *Digital Discrimination in Sharing Economy at the Base of the Pyramid,* in I. QURESHI, B. BHATT, D.M. SHUKLA, (a cura di), *Sharing Economy at the Base of the Pyramid,* Singapore, 2021, *available at https://doi.org/10.1007/978-981-16-2414-8_10;* D. BROUWER, *Towards a ban of discriminatory rankings by digital gatekeepers? Reflections on the proposal for a Digital Markets Act*, in *Internet Policy Review,* 2021, disponibile in *https://policyreview.info/articles/news/towards-ban-*

4. *Digital Services Act* e *Artificial Intelligence Act:* esigenze di coordinamento tra utilizzo di tecniche subliminali e influenza digitale.

Il *Digital Services Act* prevede che i fornitori di piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi devono valutare i rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'uso dei loro servizi, nonché dai potenziali abusi da parte dei destinatari dei servizi.[23] Si tratta di una valutazione funzionale ad adottare opportune misure di attenuazione dei rischi rilevati e dei conseguenti potenziali impatti negativi sulle persone, la società e il mercato.

Nel continuare a riflettere sulle esigenze di coordinamento tra *Digital Services Act* e *Artificial Intelligence Act* occorre evidenziare che non sarebbe coerente che i rischi inaccettabili ai sensi dell'*Artificial Intelligence Act* fossero accettabili per il *Digital Services Act* o qualificabili come rischi sistemici. Questi ultimi, infatti, ai sensi del *Digital Services Act* non sono vietati ma, piuttosto, considerati inevitabili, anche se da attenuare *ex* art. 35.

Ne consegue che un prestatore di un servizio digitale non possa usare sistemi di intelligenza artificiale che generano rischi inaccettabili, anche in assenza di una disposizione espressa del *Digital Services Act*.

Per esempio, un prestatore di un servizio digitalenon può usare un sistema di intelligenza artificiale che utilizzi ‹‹tecniche subliminali che agiscono senza che una persona ne sia 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 capacità della persona di prendere una decisione informata, inducendo pertanto la persona a prendere una decisione che non avrebbe altrimenti preso, in un modo che provochi o possa provocare a tale persona, a un'altra persona o a gruppo di persone un danno significativo››. Neppure può usarsi un sistema di intelligenza artificiale che sfrutti ‹‹la vulnerabilità di una persona o di un gruppo specifico di persone, comprese le caratteristiche note o previste della personalità o della situazione sociale o economica, dell'età, della capacità fisica o mentale di tale persona o di tale gruppo allo scopo o avente l'effetto di distorcere materialmente il comportamento di tale persona o di una persona appartenente tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno significativo››. L'utilizzo di tali sistemi rientra, infatti, tra le pratiche di intelligenza artificiale vietate dall'art. 5 dell'*Artificial Intelligence Act*. Tale articolo ha subito significative modifiche dagli emendamenti adottati dal Parlamento Europeo il 14 giugno 2023, in particolare dagli emendamenti 215 e 216, che fanno riferimento a un ‹‹danno significativo›› per la persona, e non più, come nella versione dell'*Artificial Intelligence Act* precedente a detti emendamenti, a sistemi di intelligenza artificiale che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento, in un modo che provochi o possa provocare un ‹‹danno fisico o psicologico›› a una persona o che ne sfrutti le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un ‹‹danno fisico o psicologico››.[24]

Nel prevedere gli elementi qualificanti di una pratica di intelligenza vietata, si è, dunque, passati dal dare rilievo al ‹‹danno fisico o psicologico›› di una persona al ‹‹danno significativo›› alla persona. Si tratta, dunque, di un'apertura che amplia l'ambito della possibile tutela, ma che necessita di un coordinamento con il *Digital Services Act* in termini diversi rispetto alla versione dell'*Artificial Intelligence Act* precedente agli emendamenti adottati dal Parlamento Europeo il 14 giugno 2023.

Il *Digital Services Act* attribuisce un rilievo autonomo, quale elemento qualificante di un rischio sistemico *ex* art. 34, ‹‹alle gravi conseguenze negative per il benessere fisico e mentale della persona››. L'*Artificial Intelligence Act* considera inaccettabile il rischio di un ‹‹danno significativo›› alla persona.

---

discriminatory-rankings-digital-gatekeepers-reflections-proposal-digital; ID., *A non-discrimination principle for rankings in app stores*, in *Internet Policy Review,* 2020, disponibile in *https://policyreview.info/articles/analysis/non-discrimination-principle-rankings-app-stores*. Con riferimento alle barriere di accesso ai mercati, a seguito dello sviluppo delle nuove tecnologie, cfr. B.T. SØRENSEN, *Digitalisation: An opportunity or a risk*?", in *Journal of European Competition Law & Practice,* 2018, 349 ss.

[23] C. CAMARDI, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista,* in *Juscivile,* 2021, 871 ss.

[24] *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence,* cit.

Il *Digital Services Act* considera rischio sistemico le ‹‹gravi conseguenze negative per il benessere fisico e mentale della persona›› in generale, senza esigere che siano il risultato di ‹‹tecniche subliminali›› o ‹‹tecniche volutamente manipolative o ingannevoli››, anche se l'art. 34 specifica che i fornitori di piattaforme *online* di dimensioni molto grandi devono valutare se, e in che modo, i rischi possano essere influenzati da manipolazioni intenzionali dei loro servizi, anche mediante lo sfruttamento automatizzato del servizio stesso.[25]

Nel non esigere che le ‹‹gravi conseguenze negative per il benessere fisico e mentale della persona›› siano dovute a ‹‹tecniche subliminali›› o ‹‹tecniche volutamente manipolative o ingannevoli››, la previsione dell'art. 34 del *Digital Services Act* è più ampia rispetto all'art. 5 dell'*Artificial Intelligence Act*. Quest'ultimo, però, risulta avere un ambito di applicazione più ampio da altri punti di vista, soprattutto nel dare rilievo, a seguito degli emendamenti del 13 giugno 2023, non più al ‹‹danno fisico o psicologico›› di una persona, ma al ‹‹danno significativo›› alla persona quale elemento qualificante di una pratica di intelligenza artificiale vietata.

Il confronto tra i dati normativi in oggetto rileva che le ‹‹manipolazioni intenzionali›› del servizio che hanno ‹‹gravi conseguenze negative per il benessere fisico e mentale della persona›› creano per il *Digital Services Act* dei rischi sistemici dal confine non sempre facilmente individuabile con le pratiche di intelligenza artificiale vietate *ex* art 5 dell'*Artificial Intelligence Act*. Il confine è dato dalla distinzione tra ‹‹manipolazione intenzionale›› e ‹‹benessere fisico e mentale della persona›› di cui all'art. 34 del *Digital Services Act* e ‹‹tecniche subliminali che agiscono senza che una persona ne sia 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 capacità della persona di prendere una decisione informata, inducendo pertanto la persona a prendere una decisione che non avrebbe altrimenti preso›› e ‹‹danno significativo›› *ex* art. 5 dell'*Artificial Intelligence Act*.

In ogni caso, un primo controllo al quale dovrebbe essere sottoposto l'uso di sistemi di intelligenza artificiale da parte dei prestatori di servizi digitali è che l'uso di tali sistemi non rientri nelle pratiche di intelligenza artificiale vietate ai sensi dell'art. 5 dell'*Artificial Intelligence Act*, anche in assenza di una specifica disposizione in tal senso del *Digital Services Act.*

Ma c'è di più, la valutazione dei rischi sistemici deve tenere conto, ai sensi del comma 2 dell'art. 34 del *Digital Services Act*, dei seguenti fattori: progettazione dei sistemi di raccomandazione e di qualsiasi altro sistema algoritmico pertinente; progettazione dei sistemi di moderazione dei contenuti; condizioni generali e loro applicazione; sistemi di selezione e presentazione delle pubblicità; pratiche del fornitore relative ai dati.

I sistemi di intelligenza Artificiale utilizzati dalle piattaforme online sono idonei a condizionare i comportamenti, anche economici, dei soggetti che interagiscono con le piattaforme.

Basti pensare che i sistemi di raccomandazione possono avere un impatto significativo sulla capacità dei destinatari di recuperare e interagire con le informazioni online, finendo, di fatto, per comprimere l'ambito delle opzioni cui i consumatori sono esposti.[26] Si tratta di sistemi che, come è stato efficacemente notato, non si limitano a raccomandare contenuti, ma più esattamente "curano" gli stessi,[27] discriminando nella selezione dei contenuti o dei relativi destinatari e nella limitazione delle opportunità di ricevere comunicazioni commerciali oppure offerte contrattuali alternative, attraverso forme di vera e propria manipolazione digitale. Ne consegue la possibilità di una menomazione

[25] R. A. ACHLEITNER, *Der künftige Digital Services Act der EU: Neue Pflichten und Verantwortlichkeiten für Anbieter digitaler Dienste*, in *Zeitschrift für Tarifrecht*, 2021, 1ss.

[26] È quanto si legge nel Considerando 70) del *Digital Services Act.*

[27] In questi termini R. MONTINARO, *I sistemi di raccomandazione,* cit. 348. Cfr. B. STARK, D. STEGMANN, P. JÜRGENS, M. MAGIN, *Are Algorithms a Threat to Democracy?*, cit., p 52 evidenziano che «as the debate about the impact of algorithmic news recommenders on democracy is still an ongoing process, diversity-sensitive design as part of a possible solution should be taken into account. For such solutions to work, it should be clear that different perspectives on the democratic role of news recommenders imply different design principles for recommendation systems, i.e., an explicit normative conception of the democratic potential is critical. It may also become clear, that we need to work towards a coherent mix of appropriate government regulation, co-regulation, and platform-specific self-regulation in order to minimize the negative effects of the discussed threats››. Cfr. D. LUPTON, *Digital risk society*, cit., 301 afferma che ‹‹members of some social groups are positioned in the literature on the 'digital divide' as at risk of disadvantage in relation to communication, education, information or better employment opportunities because they lack access to or interest or skills in using online technologies. This aspect of digital risk society may be characterized as "digital social inequality risks"››. L'Autrice pone l'attenzione anche ai cd. "risk of predictive privacy", ossia quei rischi ‹‹which involves individuals being adversely affected by assumptions and predictions that are made about them based on preexisting digital datasets››. Cfr. S.U. NOBLE, *Algorithms of Oppression: How Search Engines Reinforce Racism,* New York, 2018.

dell'autonomia degli utenti dei servizi, anche a causa di sistemi congegnati in modo tale da indurli a restare attivi online o porre la propria attenzione verso certi contenuti.[28]

Si tratta di un dato abbastanza evidente e del quale le normative di derivazione europea sembrano avere consapevolezza. Non è un caso che gli emendamenti adottati dal Parlamento Europeo il 14 giugno 2023 introducano all'allegato III, punto 8, la nuova lettera a) *ter*, che considera sistemi di intelligenza artificiale ad alto rischio quelli destinati a essere utilizzati dalle piattaforme di *social media*, che sono state designate come piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33 del *Digital Services Act*, per quanto concerne i loro sistemi diretti a raccomandare al destinatario del servizio i contenuti generati dagli utenti e disponibili sulla piattaforma. Si tratta di una novità che rende ancora più evidente la necessità di un coordinamento tra l'*Artificial Intelligence Act* e il *Digital Services Act,* anche in considerazione del fatto che non può non essere discutibile che i sistemi di IA destinati a essere utilizzati dalle piattaforme di *social media,* per quanto concerne i loro sistemi diretti a raccomandare al destinatario del servizio i contenuti generati dagli utenti disponibili sulla piattaforma, siano ad alto rischio sole se utilizzati da piattaforme di grandi dimensioni. Il rischio significativo di danno per i diritti fondamentali delle persone fisiche, elemento qualificante del fatto che un sistema sia ad alto rischio, può, nei fatti, prescindere dalle dimensioni delle piattaforme; dimensioni che invece sono rilevanti ai fini della qualificazione del rischio come sistemico ai sensi del *Digital Services Act.*

Esemplificativo della consapevolezza, da parte dell'Unione Europea, della possibilità di una menomazione dell'autonomia degli utenti dei servizi digitali, anche a causa dell'utilizzo di sistemi di intelligenza artificiale da parte dei prestatori di servizi digitali, è, altresì, l'art. 27 del *Digital Services Act,* che impone requisiti di trasparenza e prevede che i fornitori di piattaforme online che si avvalgono di sistemi di raccomandazione debbano specificare nelle loro condizioni generali, in un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione a disposizione dei destinatari del servizio che consenta loro di modificare o influenzare tali parametri. Questi ultimi devono chiarire il motivo per cui talune informazioni sono suggerite al destinatario del servizio e comprendere, quali elementi minimi, i criteri più significativi per determinare le informazioni suggerite al destinatario del servizio e le ragioni dell'importanza di alcuni parametri rispetto ad altri. Qualora siano disponibili diverse opzioni, per i sistemi di raccomandazione che determinano l'ordine relativo delle informazioni presentate ai destinatari del servizio, i fornitori di piattaforme online rendono disponibile anche una funzionalità che consente al destinatario del servizio di selezionare e modificare in qualsiasi momento l'opzione preferita. Tale funzionalità deve essere direttamente e facilmente accessibile dalla sezione specifica dell'interfaccia online della piattaforma online.

L'importanza dell'art. 27 del *Digital Services Act* è legata alla circostanza che la versione del *Digital Services Act* precedente agli emendamenti approvati dal Parlamento europeo il 20 gennaio 2022 individuava i rischi specifici legati all'uso dei *Recommender systems* solo con riferimento all'attività delle piattaforme di grandi dimensioni. La versione emendata invece, attraverso l'introduzione dell'articolo 27, estende gli obblighi di trasparenza relativi ai sistemi di raccomandazione a tutte le piattaforme online. Si tratta di un dato che evidenzia un'apertura del *Digital Services Act*, a fronte, invece, della limitazione alle sole piattaforme di grandi di dimensione della novità segnalata della nuova lettera A) *ter* dell'allegato III, punto 8, dell'*Artificial Intelligence Act*.

L'art 27 del *Digital Services Act* non è l'unico a rendere evidente la preoccupazione di garantire la trasparenza dei parametri che portano a determinati esiti della ricerca online. Nella stessa direzione muove l'art. 26 del *Digital Services Act*, ai sensi del quale i *providers of online platforms* devono garantire che i destinatari delle pubblicità visualizzate sulle interfacce online delle loro piattaforme dispongano di informazioni che consentano di rendersi conto che si tratta di pubblicità, di comprendere quali siano i principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità e se tali parametri siano modificabili. Sono tenuti, altresì, a fornire informazioni sulla persona fisica o giuridica per conto della quale viene presentato l'annuncio o che ha pagato l'annuncio stesso.

Il *Digital Services Act* prevede un doppio livello di tutela. Uno relativo ai rischi non sistemici, per i quali la tutela è approntata dall'art. 26 e 27 del

[28] Cfr. A. Fusaro, *La responsabilità giuridica alla prova delle neuroscienze*, Cacucci, 2018; C. Iorio, *Intelligenza artificiale e responsabilità: spunti ricostruttivi,* in *Tecnologie e Diritto*, 2021, 51 ss. S. Orlando, *Data vs capta: intorno alla definizione di dati*, in *Nuovo diritto civile*, 2022, 43. L'Autore avverte che con lo sviluppo delle tecnologie di produzione di informazione artificiale da altra informazione artificiale, si parlerà presto dei rischi, delle scommesse e dei fallimenti della conoscenza artificialmente derivata.

Digital Services Act, l'altro riferito ai rischi cd. sistemici posti in essere dalle piattaforme e dai motori di ricerca di grandi dimensioni. La sezione 5 del *Digital Services Act*, riferita appunto alle piattaforme e ai motori di ricerca di grandi dimensioni prevede, infatti, obblighi supplementari in materia di trasparenza della pubblicità online; obblighi che si sostanziano nel dovere delle piattaforme di garantire l'accesso del pubblico ai registri delle pubblicità visualizzate sulle loro interfacce online. Ciò al fine di facilitare la vigilanza e la ricerca sui rischi derivanti dalla distribuzione della pubblicità online, ad esempio in relazione alla pubblicità illegale o alle tecniche di manipolazione e di disinformazione che hanno ripercussioni negative reali e prevedibili sulla salute pubblica, sulla sicurezza pubblica, sul dibattito civico, sulla partecipazione politica e sull'uguaglianza.

La capacità delle piattaforme online di influenzare gli utenti è evidente anche se si pensa alle modalità di realizzazione delle interfacce grafiche delle piattaforme che hanno delle impostazioni assimilabili ai cosiddetti *deceptive design patterns* descritti nelle linee Guida dell'*European Data Protection Board (EDPB*) del 14 febbraio 2023.[29] Lo evidenzia chiaramente anche il Garante Privacy,[30] richiamando la potenzialità ingannevole, della scelta, non certo frutto di una mera casualità, di usare un carattere diverso per due opzioni che dovrebbero essere alternative e quindi rappresentate graficamente nello stesso modo. La realizzazione grafica di una determinata interfaccia presuppone che si conoscano, e si "sfruttino" intenzionalmente, i meccanismi che interagiscono con le capacità cognitive dell'utente. Non è un caso che il *Digital Services Act*, sensibile a tale problematiche, all'art. 25, richiami l'attenzione su particolari tipi di pratiche che possono essere poste in essere dai fornitori di piattaforme online e che si sostanziano: nell'attribuire maggiore rilevanza visiva ad alcune scelte quando si richiede al destinatario del servizio di prendere una decisione; nel chiedere ripetutamente che un destinatario del servizio effettui una scelta laddove tale scelta sia già stata fatta, specialmente presentando *pop-up* che interferiscano con l'esperienza dell'utente; nel rendere la procedura di disdetta di un servizio più difficile della sottoscrizione dello stesso.

L'articolo 25 del *Digital Services Act* prevede, inoltre, che i fornitori di piattaforme online non debbano progettare, organizzare o gestire 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. Il dato è evidente anche nel Considerando 67) del *Digital Services Act,* ove si avverte e che i percorsi oscuri sulle interfacce online delle piattaforme online ‹‹sono pratiche che distorcono o compromettono in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate. Tali pratiche possono essere utilizzate per convincere i destinatari del servizio ad adottare comportamenti indesiderati o decisioni indesiderate che abbiano conseguenze negative per loro››. Pratiche suddette dovrebbero essere vietate nella misura in cui ingannano i destinatari del servizio o distorcono o limitano l'autonomia, il processo decisionale o la scelta dei destinatari del servizio attraverso la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa.[31] Non si tratta evidentemente solo di ridurre la libertà del soggetto, ma di organizzarla e indirizzarla nella direzione voluta.[32]

[29] *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and them,* in *https://edpb.europa.eu.* La versione del 14 febbraio 2023 delle Guidelines *3/2022* aggiorna la precedente e presenta rilevanti novità, già a partire dalla sostituzione dell'espressione "*dark patterns"* con *"deceptive design patterns*". Sull'elaborazione della figura dei *dark patterns* nella letteratura informatica nordamericana e il recente cambio di nome in *deceptive design patterns* da parte del suo teorizzatore si rimanda a S. ORLANDO, *A proposito dei deceptive design (già dark) patterns*, in corso di pubblicazione. All'Autore si rimanda anche per alcuni esempi di *deceptive design patterns*. Si veda anche S. ORLANDO, *I lividi dei minorenni sparring partners di chatGPT e l'età minima per attivare il servizio in Italia,* in *Persona e Mercato,* 2023, 3. Sul *legal design* a tutela degli utenti dai *dark pattern*, si vedano L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il legal design come un rimedio ex ante*, in *Diritto dell'Informazione e dell'informatica*, 2020, 303 ss.; J. LUGURI, L. STRAHILEVITZ, *Shining a light on Dark Patterns*, in *Journal of Legal Analysis,* 2021, 43 ss.

[30] Provvedimento prescrittivo e sanzionatorio nei confronti di Ediscom S.p.A. - 23 febbraio 2023 in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870014,* 19.

[31] Il Considerando 67) del *Digital Services Act* specifica che le pratiche legittime, ad esempio nel campo della pubblicità, conformi al diritto dell'Unione non dovrebbero essere considerate di per sé percorsi oscuri. Tali norme sui percorsi oscuri dovrebbero essere interpretate come atte a disciplinare le pratiche vietate che rientrano nell'ambito di applicazione del *Digital Services Act* nella misura in cui tali pratiche non siano già contemplate dalla direttiva 2005/29/CE o dal Regolamento (UE) 2016/679.

[32] Interessanti sul punto le osservazioni di G. PISANI, *Piattaforme digitali e autodeterminazione. Relazioni sociali, lavoro e diritti al tempo della "governamentalità algoritmica",* Modena 2023, 42. L' Autore sottolinea la necessità di riaffermare una dimensione collettiva dell'autodeterminazione.

5. L' ‹‹influenza›› digitale: oltre l'autodeterminazione come fenomeno esclusivamente individuale.

Il singolo utente dei servizi online si trova spesso succube di un potere nascosto che non può affrontare da solo. L'unica alternativa, ormai concretamente non percorribile, è l'isolamento e la rinuncia alla socialità digitale.[33]

È marginale e residuale, infatti, l'ipotesi di un interesse a non essere inclusi nell'ecosistema digitale; ecosistema che, però, si presta, proprio grazie agli algoritmi finalizzati alla profilazione e al "bersaglio" dei profili individuati, a influenzare i comportamenti secondo modalità molto più incisive della pubblicità commerciale tradizionale.[34] Tanto è vero che si parla di *influencer*, di *influencer marketing* e di *marketer*, questi ultimi individuati in coloro che «disegnano strategie di marketing su stili di vita, abitudini e credenze delle persone (credenze storiche, religiose, politiche) in quanto indirettamente funzionali al comportamento che vogliono influenzare, alla risposta che vogliono ottenere».[35] Ancora più invasivo è il cd. *content marketing* che consiste in una strategia di marketing basata su contatti qualificati e contenuti in grado di convincere i potenziali *buyer* a diventare clienti. I contenuti del *marketing* sono il frutto dell'attività di esperti che riescono ad individuare i problemi di potenziali clienti e sanno guidarli nel risolvere i problemi che si frappongono al raggiungimento dei loro obiettivi. La maggiore pervasività di marketing è legata alla capacità di creare un legame di fiducia con i clienti, consentendogli di selezionare tra le molteplici informazioni di fronte alle quali si trovano quando si muovono sul web.[36]

Di fronte a questo scenario ben si comprendono le preoccupazioni alle quali cercano di dare risposta l'art. 34 del *Digital Services Act* e l'art 5 dell'*Artificial Intelligence Act*, sia pure nei limiti di coordinamento evidenziati. Il *Digital Services Act*, anche nel Considerando 69), evidenzia la circostanza che, per il tramite delle piattaforme online, possano essere poste in essere tecniche manipolative che hanno un impatto negativo su interi gruppi e sulla società, contribuendo a campagne di disinformazione e discriminazione. Di fronte a questo dato, uno sviluppo equilibrato delle tecnologie, necessita una riflessione sulla responsabilità da manipolazione come inadempimento dell'obbligazione di non manipolare; obbligazione che sorge dal fatto che lo spazio informativo digitale non è contrattuale perché in esso si agisca occasionalmente per contratto, ma perché è contrattuale la sua costituzione. [37]

[33] Sul punto si rimanda a M. Franzoni, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale,* in *Juscivile*, 2021, 6. L'Autore afferma che il concentrarsi della maggior parte degli interessi della persona nello spazio digitale comporta una sorta di "socialità obbligatoria" legata all'inevitabilità della circostanza che ‹‹qualcosa di sé debba costantemente esser condiviso con gli altri››, con inevitabili ripercussioni sul tradizionale diritto alla riservatezza che deve convivere oggi, al contrario di quanto accadeva prima della digitalizzazione della nostra vita quotidiana, con il fatto che certe informazioni debbano essere necessariamente comunicate a coloro con i quali si viene in contatto e al sistema che lo consente. S. Orlando, *Per un sindacato di liceità del consenso privacy,* in *Persona e Mercato*, 2022, 530, afferma che si è soliti sottolineare che, nella materia dell'innovazione digitale, la legge deve seguire la tecnologia che cambia. L'Autore precisa che questa osservazione rischia di essere intesa in senso limitativo. Il legislatore, infatti, deve comprendere non solo i cambiamenti tecnologici, ma anche quelli dei rapporti sociali che ne conseguono e tenere conto dell'idea di socialità, che cambia anch'essa col tempo. Cfr. L. Tomassini, *Il grande salto: l'uomo, il digitale e la più importante evoluzione della nostra storia*, Roma, 2020; A. Longo, G. Scorza, *Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà,* Milan, 2020.

[34] Si veda, quanto al rilievo del *marketing* per condizionare i comportamenti anche oltre le scelte di natura economica, COM (2021) 731 final, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica;* Cfr. *EDPB, Linee guida 8/2020 sul targeting degli utenti di social media, versione 2.0, adottate il 13 aprile 2021*, in *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_it.*

[35] S. Orlando, *Per un sindacato di liceità del consenso privacy,* cit., 533. Cfr. P. Kotler, S. Hollensen, M.O. Opresnik, *Social media marketing, Marketer nella rivoluzione digitale,* Milano, 2019.

[36] Sullo stretto legame tra *marketing* digitale e tendenza all'acquisto impulsivo dei consumatori online si vedano P. Ahadi, F. Saberian, *Comparative study of The effect of Content Marketing use on Social Networks and Traditional Marketing on Consumer Behavior*, in *Consumer Behavior Studies Journal,* 2021, 200 ss.; M. R. Ziarani, N. Janpors, S. M. Taghavi, *Effect of Digital Marketing on Customer Behavioral Intentions with the Mediation of Customer Relationship Management*, *International Conference on Entrepreneurship, Business and Online Marketing* 2023, disponibile in *https://ssrn.com/abstract=4320387.* Si vedano anche L. Hao, W. Chundong, S. Yongjie, *Survey on Personality Recognition Based on Social Media Data,* in *Journal of Frontiers of Computer Science and Technology,* 2023, 1002, dove si afferma che «personality is a stable construction, which is associated with thoughts, emotions and behaviors of human. Any technology involved in understanding, analyzing and predicting human behaviors may benefit from personality recognition. Accurately recognizing the personality will contribute to the research of human-computer interaction. Cfr. K. S. Kyaw, P. Tepsongkroh, C. Thongkamkaew, F. Sasha, *Business Intelligent Framework Using Sentiment Analysis for Smart Digital Marketing in the E-Commerce Era,* in *Asia Social Issues,* 2023, at *https://doi.org/10.48048/asi.2023.252965.*

[37] P. Femia, *Tumulti contrattuali. Collettivo "fluido" nei social media, socializzazione sinallagmatica, reticolarità, azione con-*

E, se è noto che i dati sono il nutrimento degli algoritmi, non è altrettanto percepito il fatto che l'uso illecito dei dati non è un problema soltanto dei singoli ma anche della collettività. Non si tratta solo del consenso dell'interessato al trattamento dei suoi dati o di un controllo sui suoi dati, ma di un problema che sta a monte e che riguarda l'interesse della collettività a che i sistemi di intelligenza artificiale non facciano un uso dei dati per finalità illecita, ossia per fini persecutori, distorsivi dei comportamenti e discriminatori o per consentire di «identificare e avvantaggiarsi di situazioni soggettive di vulnerabilità decisionale e comportamentale delle persone».[38]

I rischi di distorsione comportamentale e di discriminazione, legati all'uso di algoritmi o di sistemi di intelligenza artificiale da parte dei prestatori di servizi digitali, impongono di non dare un ruolo decisivo al solo consenso al trattamento dei propri dati da parte dell'interessato, sia pure libero, specifico, informato e inequivocabile, ma anche al fatto che il consenso sia prestato per specifiche finalità di trattamento legittime.[39] Ne consegue, per esempio, che non basta un consenso per "finalità di marketing", "finalità di profilazione" o "finalità di targeting". Tali finalità, nella loro genericità, possono essere sia legittime sia illegittime. Saranno illegittime, per esempio, se poste in essere per individuare e sfruttate specifiche vulnerabilità o per fini discriminatori.[40]

In un contesto nel quale gli algoritmi sono progettati per perseguire specifiche finalità e nel quale l'Unione Europea ha scelto, sia nel *Digital services Act*, sia nell'*Artificial Intelligence Act*, un approccio basato sul rischio di effetti negativi sui diritti fondamentali, la legittimità del consenso al trattamento dei dati non può prescindere dalla liceità delle finalità perseguite per il trattamento stesso. La prospettiva deve essere quella della tutela di un interesse non solo privato ma anche della collettività.

6. L'uso di algoritmi da parte dei prestatori di servizi digitali e il difficile delinearsi di un loro ruolo meramente passivo.

L'uso di algoritmi da parte dei prestatori di servizi digitali incide sulle loro responsabilità, nonostante il *Digital Sevices Act* sia esplicito nel chiarire che, non solo non pregiudica, ma si fonda in primo luogo sulla Direttiva 2000/31/CE e sull'assenza di un obbligo generale di sorveglianza, il cd. *no general monitoring or active fact-finding obligations.*[41] In altri termini, il *Digital Services Act*, sia pure rima-

trattuale comune, in C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale,* cit., 135. Secondo l'Autore manipolare significa omettere di vigilare sulle conseguenze dannose delle proprie modalità comunicative. Sul diritto alla corretta informazione si rimanda a P. PERLINGIERI, *L'informazione come bene giuridico,* in *Rass. dir. civ.,* 1990, 329. Cfr. F. DI CIOMMO, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. COMANDÉ (a cura di), *Persona e tutele giuridiche*, Torino, 2003, 3 ss. *Sulle responsabilità delle piattaforme nei contratti della platform economy*, si veda S. Martinelli, *Le responsabilità delle piattaforme nei contratti della platform economy*, Torino, 2023, 191 ss.

[38] Il dato è evidenziato da S. ORLANDO, *Per un sindacato di liceità del consenso privacy,* cit., 537. L' Autore dice chiaramente che «dobbiamo in definitiva mettere bene a fuoco che l'uso illecito di dati personali - e per uso illecito intendo anche l'addestramento di sistemi di IA lesivi di diritti fondamentali di persone diverse dall'interessato - è da vietarsi nel superiore interesse della collettività, perché non vogliamo che il nuovo volto della nostra società sia costruito da sistemi di IA distorsivi e discriminatori, addestrati con i dati personali (anonimizzati o meno: non importa) di nessuno: nell'epoca dei sistemi di IA (addestrati con dati personali, anonimizzati o meno) non è più in gioco soltanto il controllo sui propri dati personali, ma l'uso che ne fanno i sistemi di IA».

[39] S. ORLANDO, *Per un sindacato di liceità del consenso privacy,* cit., 527 e ss. propone interessanti esempi delle conseguenze legate a un approccio non funzionale al tema del consenso dell'interessato al trattamento dei propri dati. Gli esempi proposti si rilevano particolarmente significativi in quanto tratti da un confronto con *l'EDPB, Linee guida 8/2020 sul targeting degli utenti di social media, versione 2.0, adottate il 13 aprile 2021.* All'Autore si rimanda anche per l'esame del parere congiunto *EDPB-GEPD n. 5/2021 del 18 giugno 2021 sulla proposta di Artificial Intelligence Act,* in *https://edpb.europa.eu/our*

[40] Cfr. S. ORLANDO, *Per un sindacato di liceità del consenso privacy,* cit., 537. C. PERLINGIERI, *Creazione e circolazione del bene prodotto dal trattamento algoritmico dei dati*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, 177.

[41] A modello è stata presa la sezione 512 del *Digital Millennium Copyright Act (DMCA*). Sul punto si veda R. PETRUSO, *Responsabilità delle piattaforme online, oscuramento di siti web e libertà di espressione nella giurisprudenza della Corte europea dei diritti dell'Uomo,* in *Diritto dell'Informazione e dell'Informatica*, 2018, 511 ss. Sul punto si veda R. COSIO, *La responsabilità del prestatore di servizi di* hosting, in *www.juscivile.com*, 2020, 898. Ivi si analizza la giurisprudenza della Corte di giustizia in base alla quale si ritiene che non si ponga in contrasto con l'esclusione dall'obbligo generale di sorveglianza attiva *ex ante* dei contenuti pubblicati dagli utenti, previsto dall'art. 15 della direttiva, l'ordine del giudice al gestore del *social network* di rimozione delle informazioni dal contenuto identico e/o equivalente a quello di un'informazione precedentemente dichiarata illecita, ove sia assicurato il rispetto di due condizioni. Da una parte, la sorveglianza e la ricerca attiva sia limitata a contenuti, in sostanza, invariati rispetto a quelli che hanno dato luogo all'accertamento di illiceità. Dall'altra parte, i contenuti equivalenti da rimuovere vengano individuati dall'autorità giurisdizionale o amministrativa in maniera chiara e precisa, in modo tale che il prestatore di servizi non debba essere costretto a effettuare una valutazione autonoma sugli stessi, potendo ricorrere a procedure automatizzate.

nendo fedele all'impianto della Direttiva 2000/31/CE con riferimento al cd. *hosting provider* passivo, sembra delineare una figura di *provider* nella maggior parte dei casi necessariamente attivo in quanto pone in essere una serie di attività che vanno al di là dalla semplice intermediazione[42]. Si pensi al disposto dell'art. 14 del *Digital Services Act*. La norma prevede che i fornitori di servizi di intermediazione sono tenuti a informare su eventuali politiche, procedure, misure e strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana. Nell'applicare eventuali restrizioni previste nelle condizioni generali del servizio, relative a tali eventuali politiche e procedure, i fornitori di servizi devono agire in modo diligente, obiettivo e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, compresi i diritti fondamentali dei destinatari del servizio.

Questa norma, che tra l'altro si applica indistintamente a tutti i fornitori di servizi di intermediazione, sembra interpretabile nel senso che la previsione di strumenti di moderazione di contenuti implica di per sé, necessariamente, il compimento di un'attività, tra l'altro particolarmente delicata, in quanto necessariamente attenta ai diritti e agli interessi legittimi di tutte le parti coinvolte.

Ulteriori specifici obblighi per i *providers of online platforms*, incompatibili con loro ruolo meramente "passivo" sono funzionali al raggiungimento degli obiettivi di interesse pubblico perseguiti dal *Digital Services Act*. Tra questi obiettivi c'è la tutela dei minori.[43] Il nuovo articolo 28 è, infatti, specificatamente dedicato alla *online protection of minors* e, sebbene, i *providers of online platforms* non siano obbligati a trattare dati personali ulteriori per valutare se il destinatario del servizio sia minore, devono mettere in atto adeguate e proporzionate misure per garantire che nel fornire i loro servizi sia assicurato un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori.[44]

I prestatori di servizi digitali destinati principalmente ai minori, ad esempio, attraverso la progettazione o la commercializzazione del servizio, o che sono utilizzati prevalentemente da minori, dovrebbero compiere sforzi particolari per rendere la spiegazione delle loro condizioni generali facilmente comprensibile ai minori.[45]

Alle piattaforme *online* e alle *very large online platforms* non può che attribuirsi un ruolo attivo se si considerano tutte le nuove previsioni della sezione 4 relativa ai *providers of online platforms allowing consumers to conclude distance contracts with traders*.

L'articolo 30 del *Digital Services Act* prevede che piattaforme *online* - qualora consentano agli operatori commerciali di utilizzare i propri servizi per pubblicizzare o offrire prodotti ai consumatori - devono ottenere le informazioni necessarie per l'identificazione del professionista secondo il modello del cd. "*Know your customer*". Rispetto a tali informazioni, il ruolo delle piattaforme *online* non può essere meramente passivo, in quanto sono tenute a compiere i massimi sforzi possibili, ai sensi dell'art. 30, per stabilire se le stesse siano attendibili. Si tratta della cd. tracciabilità degli operatori commerciali, finalizzata a contrastare la vendita di prodotti contraffatti *online*. L'attenzione alla tracciabilità del professionista è garantita anche da spe-

[42] P. ROTT, *New Liability of Online Marketplaces Under the Digital Services Act?*, in *European Review of Private Law*, 2022, 1039 ss. S. TOMMASI, *The Liability of Internet Service Providers in the Proposed Digital Services Act*, in *European Review of Private Law*, 2022, 925 ss. G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell' hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo*, in *Federalismi.it*, 2020, 108.

[43] Il problema è molto complesso e riguarda, più in generale, il rapporto tra i minori e l'uso delle tecnologie digitali. Su questi temi si rimanda a R. BOGANI, B. SCHAFER, *Artificial Intelligence and Children's Rights*, in M. IENCA, O. POLLICINO, L. LIGUORI, E. STEFANINI, R. ANDORNO (a cura di), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights,* Cambridge, 2022, 215 ss. Di particolare rilievo è quanto si legge in V. CHARISI, S. CHAUDRON, R. DI GIOIA, R. VUORIKARI, M. ESCOBAR-PLANAS, I. SANCHEZ, E. GOMEZ, *Artificial Intelligence and the Rights of the Child. Towards an Integrated Agenda for Research and Policy*, *Report by the Joint Research Centre (JRC), European Commission's science and knowledge service*, Luxembourg, 2022. Il report si sofferma sull'obiettivo ‹‹to connect scientific evidence with policymaking, to gain insights of the interplay between different stakeholders, and to go beyond the identification of ethical guidelines towards methods for practical future implementations››. Si veda COM/2020/624 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *Digital Education Action Plan 2021-2027. Resetting education and training for the digital age,* in *https://eur-lex.europa.eu.* See also COM(2021) 142 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, *EU strategy on the rights of the child*, in *https://eur-lex.europa.eu*, ove si legge che «children's rights are human rights. Every child in Europe and across the world should enjoy the same rights and be able to live free of discrimination, recrimination or intimidation of any kind. This is a social, moral and human imperative on which children – who account for almost one in five people living in the EU and one in three in the world – and the wider community depends on».

[44] L. GUIBAULT, N. HELBERGER, M. LOOS, C. MAK, L. PESSERS, B. VAN DER SLOOT, *Digital Consumers and the Law. Towards a Cohesive European Framework*, Alphen aan den Rijn, 2012.

[45] È quanto previsto dal Considerando 46) del *Digital Services Act.* Sul punto è di particolare interesse anche il Considerando 83) con riferimento agli obblighi verso i minori.

cifiche prescrizioni in tema di *compliance by design*, in quanto i fornitori di piattaforme *online* devono progettare e organizzare la propria interfaccia in modo da consentire ai professionisti di fornire ai consumatori alcune informazioni rilevanti per essere identificabili. Ma non solo, ai sensi dell'art. 31, i *providers of online platforms allowing consumers to conclude distance contracts with traders* devono anche compiere sforzi ragionevoli per verificare, sia pure in modo casuale, se i prodotti o servizi offerti sono stati identificati come illegali in qualsiasi *database online* ufficiale, liberamente accessibile e leggibile da dispositivo automatico o interfaccia *online*.[46]

Esemplificativo è anche il caso dell'attività che consiste nell'ottimizzare la presentazione delle offerte in vendita o nel promuoverle nel mercato online.[47] Anche se con specifico riferimento alle sole piattaforme online, il *Digital Services Act* si presenta molto rigoroso nel disciplinare le transazioni commerciali intermediate online. Nel Considerando 23) e all'articolo 6 (3) si prevede, infatti, che se le piattaforme online consentono ai consumatori di concludere contratti a distanza con operatori commerciali, non possono beneficiare dell'esenzione dalla responsabilità nella misura in cui presentino le relative informazioni in modo tale da indurre un consumatore medio a ritenere che siano a conoscenza delle informazioni o le controllino, anche se in realtà potrebbe non essere così.[48]

[46] Si fa un passo in avanti rispetto ad altre, sia pure recenti, normative europee. Si pensi alla Direttiva (UE) 2019/2161, ai sensi della quale, per effetto dell'introduzione dell'art. 6 *bis*, par. 1, lett. b, della Direttiva 2011/83, il fornitore di un mercato online ha l'obbligo di informare i consumatori se il terzo che offre beni, servizi o contenuti digitali sia un professionista o meno, avvertendo che, qualora non si interfacci con un professionista, non potrà godere della tutela riservata ai rapporti tra consumatore e professionista. E, se è vero che il fornitore del mercato *online* non fornisce alcuna garanzia sulla qualifica del terzo, limitandosi a riportare la dichiarazione da questi pervenutagli, è altrettanto vero che l'informazione circa la qualità soggettiva del terzo assume un carattere di tale rilevanza che la sua omissione può integrare gli estremi di una pratica commerciale ingannevole. Cfr. S. TOMMASI, *The 'New Deal' for Consumers: Towards More Effective Protection*, in *Eur. Rev. Priv. Law*, 2020, 329 ss.; G. HIWATASHI DOS SANTOS, *A "New Deal for Consumers"? The European Regulatory Framework for Online Search Queries and Rankings under the Omnibus Directive (Directive (EU) 2019/2161),* in *Anuário do NOVA Consumer Lab,* 2020, 73 ss. In giurisprudenza si veda *Autorité de la concurrence, Decision 19-MC-01 of 3 January 2019 regarding a request for interim measures from Amadeus*, in *http://www.autoritedelaconcurrence.fr.*

[47] Si veda ECJ 12 luglio 2011, *L'Orèal v. Ebay*. Nel caso di specie la Corte afferma che *Ebay* non aveva posto in essere una mera vetrina *online*, ma svolto un'attività di organizzazione delle offerte, promozione dei prodotti e indicizzazione dei risultati della ricerca tale da attribuirgli un ruolo diverso da quello che giustifica il *favor* della direttiva 2000/31/CE. Sul punto si rimanda a P. V. EECKE, *Online service providers and liability: a plea for a balanced approach,* in *Common Market Law Review,* 2011, 1455 ss, ove si afferma che sarebbe opportuno un approccio equilibrato in cui il regime di protezione dell'intermediario possa essere salvaguardato, pur tutelando i terzi che possono vedere violati i loro diritti su *Internet.* Nota è anche ECJ 23 marzo 2010, *Google v. Luis Vuitton,* in *curia.europa.eu/juris*. In relazione alla responsabilità di un privato prestatore di servizi di locazione e registrazione di indirizzi IP che consentiva di utilizzare anonimamente nomi di dominio e siti *internet* non si è escluso che il giudice di rinvio possa, alla luce dell'insieme degli elementi di fatto e di prova pertinenti, verificare che questi svolga un ruolo attivo in quanto consente ai destinatari dei servizi di ottimizzare la loro attività di vendita online. In questa direzione muove, in particolare, ECJ 7 agosto 2018, *Cooperatieve Vereniging Snb-React U.A. v. Deepak Mehta47,* C-521/17. In molti casi, l'attenzione del consumatore è concentrata sul rapporto instauratosi con la piattaforma che funge da intermediario (il rapporto p2c: *Platform to consumer*), piuttosto che sul secondo rapporto conclusosi con il fornitore del bene o servizio offerto sulla piattaforma. In questi termini G. VERSACI, *Le tutele a favore del consumatore digitale nella "Direttiva omnibus"*, in *Persona e Mercato*, 2021, 586 ss. Cfr. sul punto A. PALMIERI, *Profili giuridici delle piattaforme digitali. La tutela degli utenti commerciali e dei titolari di siti web aziendali*, Torino, 2019, 18 ss.

[48] Cfr. ECJ, (Grand Chamber) 22 dicembre 2022*, Christian Louboutin v. Amazon Europe Core Sàrl and Othersn*. La Corte di Giustizia, con la pronuncia in questione, chiarisce i dubbi dei giudici nazionali affermando che l'uso di un marchio da parte del gestore di una piattaforma può essere vietato dal titolare del marchio se le attività di questo operatore della piattaforma portino il consumatore della piattaforma stessa, normalmente informato e attento, a stabilire un legame fra i servizi del gestore e il marchio in questione. Secondo la Corte, questo caso si verifica in particolare quando il cliente ha l'impressione che sia il gestore stesso della piattaforma a commercializzare per proprio conto i prodotti recanti il marchio. Si veda anche Cal. Ct. App., 13 agosto 2020, 4th Dist., No. D075738 – *Bolger vs Amazon.com Inc*., in *https://www.courts.ca.gov/4dca.htm,* 26. La Corte, pur ribadendo l'impostazione tradizionale in base alla quale l'operatore di servizi di marketplace non è responsabile dei danni causati da prodotti venduti da altri tramite la piattaforma, ha, però, specificato, che nel caso di specie, Amazon è «an integral part of the overall producing and marketing enterprise», può essere «the only member of that enterprise reasonably available to the injured plaintiff» e, inoltre, assume «the best position to ensure product safety». Per un primo commento si vedano G. BERTELLI, M. CORSI, *Amazon è responsabile per i danni causati dalla merce venduta in California. Analisi della sentenza ed applicabilità al contesto normativo europeo,* in *www.iusinitinere.it.* R. PETRUSO, *Danno da prodotto difettoso e responsabilità delle piattaforme*, cit., 61, afferma che *Court of Appeal* della California nel caso *Bolger v. Amazon* e la più recente decisione resa il 26 aprile 2021 nel caso *Loomis v. Amazon*, 6 5th Dist., 466 accorciano lo iato tra progresso tecnico e sociale e realtà giuridica nella nuova filiera distributiva delle vendite a distanza dominate da piattaforme di *e-commerce.* In direzione analoga si è mosso anche il Tribunale di Milano con ordinanza del 19 ottobre 2020, accogliendo il ricorso proposto dal produttore di alcuni prodotti di profumeria di lusso offerti in vendita, promozione e pubblicizzazione sul *marketplace* online di Amazon. In particolare, il Tribunale ha ritenuto che Amazon abbia ruolo attivo quando, come nel caso di specie, agisce in modo tale che i consumatori possano ritenere esistente un le-

7. Le diverse espressioni dell'approccio basato sul rischio e l'importanza delle regole dell'attività.

L'*Artificial Intelligence Act* e il *Digital Services Act,* sebbene condividano lo stesso obiettivo di tutela dei diritti fondamentali e dei valori democratici come controlimiti al predominio delle logiche di puro mercato nella società algoritmica, rappresentano espressioni molto diverse dell'approccio basato sul rischio nell'UE.[49] Il dato è emerso anche nel confronto con l'approccio basato sul rischio nel Regolamento generale sulla protezione dei dati (*GDPR*).[50] Segnatamente, quest'ultimo segue una prospettiva che può dirsi di *bottom-up*, nel senso che la valutazione del rischio e la scelta delle misure di mitigazione non sono definite dalla legge, ma sono principalmente lasciate alla discrezionalità degli stessi destinatari della regolazione, vale a dire ai titolari e ai responsabili del trattamento dei dati. In tal senso, il principio di *accountability*[51] è il risultato di una strategia legislativa volta a ridurre fortemente l'imposizione di oneri provenienti "dall'alto".[52] L'*Artificial Intelligence Act* assume un punto di vista molto diverso, poiché individua direttamente le diverse categorie di rischio e i gradi di responsabilità, secondo un approccio che può chiamarsi di *top-down*, in quanto non lascia il compito di valutare tale rischio ai soggetti regolamentati. Il *Digital Services Act* mira a creare un sistema ibrido, che mescoli le due opposte prospettive del *GDPR* e dell'*Artificial Intelligence Act*, individuando dall'alto verso il basso quattro categorie di rischio per i fornitori di servizi di intermediazione, lasciando loro ampio margine di manovra per scegliere quali misure adottare per ridurre le esternalità negative che le loro attività comportano.[53]

Ci troviamo di fronte a varie aggettivazioni del rischio, non accompagnate da una uniforme e chiara definizione di cosa si intenda per rischio, così che si finiscono per lasciare dei nodi irrisolti e per affidarsi troppo alla costruzione di un complesso quadro burocratico costretto a lavorare su labili distinzioni.[54]

Si lega l'alto rischio alla probabilità che si verifichino eventi considerati negativi. In questa prospettiva però si dà rilievo a problemi propri della statistica e non del rischio, eppure la statistica riguarda il passato, mentre il rischio è proiettato nel futuro.[55]

Il rischio, inoltre, non deve confondersi con il pericolo. Il rischio è un vincolo del futuro che rende possibile l'agire alle condizioni del non sapere alle

game tra Amazon e le aziende produttrici dei prodotti venduti sulla piattaforma. Può ritenersi sussistere tale legame quando Amazon gestisce un servizio clienti per le inserzioni di vendita di terzi, che costituisce l'unico servizio di cui il cliente dispone per potersi interfacciare con il venditore oppure è responsabile di un'attività promozionale anche tramite inserzioni su siti internet di terzi.

[49] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches,* cit., 473 ss. Per un confronto tra la *Proposed Artificial Intelligence Act* e l'*EU data protection acquis*, si vedano G. Mazzini, S. Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts,* in C. Camardi, *La via europea per l'intelligenza artificiale,* Milano, 2022, 35 ss.

[50] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), in *https://eur-lex.europa.eu.*

[51] Cfr. G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale,* cit., 30. L'Autrice evidenzia che si tratta di un modello già scelto nel *Gdpr* con la differenza che nel *Gdpr* il sistema di gestione è basato sull'*accountability* e sulla valutazione del rischio da parte del titolare del trattamento dei dati, in quanto soggetto che si trova nella migliore posizione per gestire il rischio. Nell'*Artificial intelligence Act* l'approccio è diverso perché è il legislatore che decide quali sono i sistemi ad alto rischio e come il rischio che essi procurano debba essere affrontato.

[52] In questi termini G. De Gregorio, P. Dunn, *The European Risk-Based Approaches,* cit., 476.

[53] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches,* cit., 477. Cfr. A. Mantelero, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big data e delle applicazioni di Artificial intelligence*, in A. Mantelero, D. Poletti, *Regolare la tecnologia il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna,* Pisa, 2018, 299 ss. Z. Li, *Affinity-based algorithmic pricing: A dilemma for EU data protection law*, in *Computer Law & Security Review*, 2022, 4, evidenzia che le norma sul *GDPR* hanno il vantaggio di basarsi su meccanismi di tutela *ex ante* e non solo *ex post* ‹‹taking a risk-based approach to prevent the misuse of personal data›.

[54] Cfr. D. Lupton, *Digital risk society*, in J. Zinn, A. Burgess, A. Alemanno (a cura di), *Handbook of Risk Studies,* Londra, 2016, 301 afferma che ‹‹as social life and social institutions have become experienced and managed via novels forms of digital technologies, and as both public and personal spaces as well as human bodies have become increasingly monitored by digital surveillance devices and sensors, a new field of risk inquiry has opened up in response to what might be termed 'digital risk society'››.

[55] Solo nel *Draft Compromise Amendments* del 16 maggio 2023, cit., si trova una definizione di rischio. Si legge all'articolo 3 che ‹‹risk' means the combination of the probability of an occurrence of harm and the severity of that harm››. La definizione è stata confermata dagli *Amendments adopted by the European Parliament on 14 June 2023*, cit., ove si trova anche una definizione di rischio significativo (emendamento 167), come ‹‹‹un rischio che è significativo per la combinazione della sua gravità, intensità, probabilità che si verifichi e della durata dei suoi effetti e della sua capacità di incidere su una persona, su una pluralità di persone o su un particolare gruppo di persone››.

quali nel presente si effettuano le scelte.[56] Il rischio non è pensato come un dato oppure una sorta di realtà sotterranea che scorre occulta al di sotto dell'agire, né come l'opposto della sicurezza cioè di ‹‹una condizione artificiale di stabilità e di certezza che si assume come razionale››.[57]

Il rischio, in altri termini, non è una realtà ma la possibilità di un evento dannoso che un'altra decisione avrebbe potuto evitare. Se ho la possibilità di scelta si tratta di rischio, altrimenti se è inevitabile che il danno si verifichi sono di fronte a un pericolo.[58] Il rischio, allora, non va visto come la rottura di un ordine che, altrimenti, continuerebbe a sussistere, ma, piuttosto, un modo attraverso il quale i sistemi sociali si adattano alla complessità del loro ambiente e la società moderna è società del rischio nel senso che ‹‹ha realizzato condizioni che le permettono di costruire futuri differenti, di mantenere alta la contingenza degli eventi, cioè di tenere aperte sempre più possibilità e, quando in conseguenza di una decisione si verifica un eventuale danno che si sarebbe voluto evitare, di sapere che un'altra decisione avrebbe potuto evitarlo››.[59]

L'alternativa al rischio, dunque, non è la sicurezza ma il pericolo,[60] a ulteriore conferma che rischio e pericolo non sono assimilabili. Tanto è vero che, quanto più si incrementano le misure di sicurezza più si incrementano i rischi.[61]

In questa prospettiva il rischio è un'opportunità, perché, a differenza del pericolo, presuppone la possibilità di incidere sull'evento finale. Il dato, riferito e applicato alle problematiche poste dai si-

[56] R. De Giorgi, *Il rischio nella società contemporanea*, in *Temi di filosofia del diritto*, vol. II, Lecce, 2015, 56. N. Luhmann, *Sociologia del rischio,* Milano, 1996, afferma, 14, che se si cercano definizioni del concetto di rischio ci si trova subito nella nebbia fitta e si ha l'impressione di non poter vedere al di là del proprio naso. Basti pensare che, con riferimento al tema del rischio, si pone il problema di quale idea di razionalità, di decisione, di tecnica, di futuro o semplicemente di tempo sia presupposta. L'impossibilità di enunciare principi generali in termini di rischio è stata evidenziata anche con riferimento a singoli ambiti. Si pensi nello specifico a quello contrattuale, in quanto ogni tipo di contratto reca in sé criteri specifici di ripartizione del rischio che obbediscono a ragioni di giustizia distributiva. Si consideri il rischio dell'inadempimento, legato alla circostanza che una delle prestazioni non venga eseguita oppure al rischio di diminuita soddisfazione economica dell'affare per la preesistenza o sopravvenienza di circostanze che non comportano inadempimento in senso tecnico ma sconvolgono l'economia originaria dell'affare. Sul punto cfr. G. Alpa, *Rischio,* in *Enc. dir.,* 1989, vol. 40, 1144 ss.; Id., *Rischio contrattuale*, in *Noviss. Dig*., Appendice, Torino, 1986, vol. VI, 863 ss.; M. Bessone, *Adempimento e rischio contrattuale*, Milano, 1975; Alpa, Bessone e Roppo, *Rischio contrattuale e autonomia privata*, Napoli, 1982; R. Nicolò, *Alea, Enciclopedia del diritto*, Milano, 1958, I, 1024 ss. Con il complicarsi di tali problematiche a seguito degli sviluppi dei sistemi di IA, l'attenzione degli interpreti si incentra anche sulla circostanza che tali sistemi possano ridurre i rischi legati all'esecuzione del contratto, in quanto si viene a creare una situazione simile a quella derivante dalla clausola *solve et repete*. Sul punto cfr. D. Di Sabato, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e Impresa*, 2017, 378 ss. e in G. Perlingieri, A. Fachechi, (a cura di), *Ragionevolezza e proporzionalità nel diritto contemporaneo*, I, Napoli, 2017, 387 ss.; T. Pellegrini, *Prestazioni auto-esecutive. Smart contract e dintorni*, in *Comparazione e diritto civile*, 2019, 843 ss. Più in generale, sull'impatto delle nuove tecnologie nella formazione del contratto, si vedano F. Della Rocca, *Il contratto tra tecnologia e diritti fondamentali*, in *Tecnologie e Diritto,* 2022, 250 ss. M. Durovic, A. Janssen, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law,* in *European Review of Private Law,* 2018, 753. Per una riflessione sulla storia del rischio si veda M. Alabrese, *Riflessioni sul tema del rischio nel diritto agrario,* Pisa, 2009, 4. Nel senso che il rischio inerisca più alle obbligazioni che al contratto è G. Gorla, *Del rischio e pericolo nelle obbligazioni*, Padova, 1934, 19 ss. In diversa prospettiva G. Pacchioni, *Obbligazioni*, Milano, 1898, 344. Sul rapporto tra rischio e perdite economiche cfr. M. Bessone, *Adempimento e rischio contrattuale*, Milano, 1975; E. Gabrielli, *Alea e rischio nel contratto*, Napoli, 1997, 115; Id., *Il rischio contrattuale*, in *I contratti in generale*, Torino, 1991, 634 ss.; S. Orlando, *Rischio e vendita internazionale,* Milano, 2002; P. Corrias, *Garanzia pura e contratti di rischio,* Milano, 2006, 288, afferma che quando si parla di rischio contrattuale, in generale, si intende l'eventualità che gli interessi divisati nel contratto non si realizzino a causa di una serie di fattori non imputabile ad alcuna delle parti. Sul punto si rimanda al pensiero di E. Betti, *Teoria generale delle obbligazioni.* I. *Prolegomeni: funzione economico-sociale dei rapporti d'obbligazione*, Milano, 1953, 154.

[57] R. De Giorgi, *Il rischio nella società contemporanea*, cit., 61.

[58] Con particolare riferimento al nesso tra sistemi di intelligenza artificiale e responsabilità, quando la prima assume decisioni imprevedibili e indipendenti dalla persona, si veda E. Caterini, *Artificial Intelligence, persona e soggetto,* in *Tecnologie e Diritto,* 2022, 207.

[59] R. De Giorgi, *Il rischio nella società contemporanea*, cit., 62.

[60] Sulla distinzione tra rischio e pericolo si rimanda a N. Luhmann, *Sociologia del rischio,* cit., 14 ss., ove si afferma che rispetto all'incertezza in riferimento ai danni futuri, ci sono due possibilità: o l'eventuale danno viene visto come conseguenza della decisione, cioè viene attribuito ad essa e parliamo allora di rischio, per la precisione di rischio della decisione; oppure si pensa che l'eventuale danno sia dovuto a fattori esterni e viene quindi attribuito all'ambiente: parliamo ora di pericolo.

[61] I sistemi di intelligenza artificiale ci pongono davanti a un non sapere. R. De Giorgi, *Il rischio nella società contemporanea*, in *Temi di filosofia del diritto*, vol. II, Lecce, 2015, 56, fa notare che quanto più si estende il sapere, tanto più si estende il non sapere, dato che più si estende la conoscenza, più si estende il non sapere delle conseguenze e, dunque, il rischio. L'Autore afferma che l 'attualità è esemplificativa sul punto ‹‹la scoperta di un virus rende evidente il non-sapere del trattamento e quindi il rischio del contagio. La scoperta del trattamento rende evidente il non-sapere delle conseguenze, la scoperta di alcuni effetti rende evidente il non-sapere di altri››. Cfr. M. Borrello, *La rappresentazione del rischio e il non sapere saputo,* in R. De Giorgi (a cura di), *Limiti del diritto,* Lecce, 2018, 499 ss.

stemi di intelligenza artificiale, risulta particolarmente interessante perché evidenzia la centralità dell'*human oversight* e la necessità di una forma di coinvolgimento umano rispetto all'*output* prodotto da un sistema di intelligenza artificiale.[62] Altrimenti, se escludiamo ogni forma di controllo sul meccanismo della decisione e ogni tipo di intervento umano, allora non c'è possibilità di partecipazione umana alla decisione e, dunque, dovremmo rassegnarci e abbandonarci a sistemi di intelligenza artificiale pericolosi.

Di fronte a un'attività organizzata per incidere sulle decisioni del soggetto, non bastano le regole del rapporto, così che è da evidenziare l'attualità del pensiero di quanti, già agli albori della legislazione di derivazione europea, segnalavano che è riduttiva una lettura che non tenga conto che, in presenza di una attività di impresa, il processo della negoziazione, cui si indirizza l'operatore economico, acquista, in ragione proprio del suo carattere di massa, un rilievo autonomo e temporalmente anticipato rispetto alle singole effettive operazioni negoziali.[63] Il che implica che non siano sufficienti le regole dell'atto, ma occorrono anche quelle dell'attività e dei rischi che la stessa pone in essere semplicemente per il fatto che si svolge.[64] Anche con riferimento all'attività di prestazione di servizi digitali, l'ontologica incidenza di massa dell'attività, da un lato favorisce l'individuazione di specifici interessi collettivi da tutelare, dall'altro giustifica tecniche di tutela anche preventive, ossia in grado di intervenire ancor prima che l'attività preparatoria della commercializzazione si sia esaurita avendo trovato sbocco nella stipula dei singoli contratti.[65]

I limiti legati alla mancanza di una considerazione sistemica dell'attività sono evidenziati anche nel settore del trattamento dei dati personali, ove ci si è resi conto che il tema deve essere trattato non solo secondo la prospettiva della lesione dei diritti della personalità, ma anche a un livello più generale, con riferimento alla tenuta e alla affidabilità del sistema di circolazione dei dati personali e dei rischi ai quali è esposto il ‹‹mercato›› dei dati personali.[66] Le pra-

[62] L'*Artificial Intelligence Act* è esplicito nel riconoscere un ruolo centrale all'*Human oversight*. Si prevede, infatti, per alcuni *high-risk AI systems*, l'insufficienza anche del coinvolgimento di una sola persona umana, esigendosi che ‹‹no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons››. Cfr. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F. P. PATTI, O. POLLICINO, S. QUATTROCOLO, D.SIMEOLI, P. SIRENA, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Rivista di BioDiritto*, 2019, 13. J. DAVIS, *AI, Ethics, and Law: A Way Forward*, in M. IENCA, O. POLLICINO, L. LIGUORI, E. STEFANINI, R. ANDORNO (a cura di), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights,* Cambridge, 2022, 304. L'*Human oversight,* d'altronde, è uno dei sette requisiti fondamentali per un'intelligenza artificiale affidabile. Lo si evince già dalla Comunicazione della Commissione Europea del 2019, COM (2019) 168 final, ma il dato è reso esplicito nella Risoluzione del Parlamento europeo del 20 ottobre 2020, sulla legge sui servizi digitali. Ivi si prevede espressamente che occorre rispettare il principio del controllo dell'uomo sulla macchina per prevenire l'aumento dei rischi per la salute, la sicurezza, la discriminazione, l'indebita sorveglianza, gli abusi e le potenziali minacce ai diritti e alle libertà fondamentali. E. GIORGINI, *Algorithms and Law*, in *The Italian Law Journal*, 2019, 145. Sull'uomo come presupposto essenziale destinato a misurare l'essenza della giuridicità si veda C. PERLINGIERI, *L' incidenza dell'utilizzazione della tecnologia robotica nei rapporti civili,* in *Rass. dir. civ.,* 2022, 1235.

[63] Cfr. A. IANNARELLI, *Il contratto in generale ed i contratti agrari tra disciplina municipale e normativa comunitaria*, in *Riv. crit. dir. priv*., 1995, 231; ID., *La disciplina dell'atto e dell'attività: i contratti tra imprese e tra imprese e consumatori*, in N. LIPARI (a cura di), *Trattato di diritto privato europeo, III, L'attività e il contratto*, Padova, 2003, 6; F. ALCARO, L'*attività. Profili ricostruttivi e prospettive applicative,* Napoli, 1999; ID., *La categoria dell'attività: profili ricostruttivi (Atti e attività. L'attività di impresa)*, in *Riv. crit. dir. priv*., 1995, 417; ID., *Attività e soggettività: circolarità funzionale*, in *Rass. dir. civ*., 2007, 883.

[64] A. IANNARELLI, *La tutela dei consumatori nella negoziazione fuori dai locali commerciali: introduzione generale*, in A. IANNARELLI (a cura di), *Le vendite aggressive. Vendite stipulate fuori dei locali commerciali e vendite stipulate a distanza nel diritto italiano ed europeo*, Napoli, 1995, 30. Ivi si nota che già l'art. 11 del d. lg. n. 50 del 1992, nel disporre misure appropriate per la tutela dei consumatori qualora non venga fornita l'informazione sul diritto di recesso, ha tenuto distinte le conseguenze miranti a sanzionare la violazione della disciplina dettata per l'attività di negoziazione, da quelle direttamente volte a proteggere i consumatori vittime in concreto di quella medesima violazione. Quanto alla considerazione dell'attività come serie di atti, si vedano G. AULETTA, *Attività*, in *Enc. dir*., Milano, 1958, III, 982; V. COLUSSI, *Capacità e impresa, I, L'impresa individuale*, Padova, 1974, 8; N. RONDINONE, *L'«attività» nel codice civile*, Milano, 2001, spec. 385. Nel senso della necessità di non esaurire il rilievo dell'attività nella serie degli atti che la compongono è F. ALCARO, L'*attività,* cit., p. 35. L' Autore afferma che l'attività è svolgimento di per sé stesso significante, fisiologicamente permanente, non destinato a esaurirsi in un risultato statico finale di cui costituisca il logico e naturale antecedente.

[65] Cfr. IANNARELLI, *Presentazione,* in S. TOMMASI, *Le pratiche commerciali scorrette e disciplina dell'attività negoziale* Bari, 2012, 12.

[66] V. RICCIUTO, *La gestione del rischio nell'attività di trattamento dei dati personali,* in *Responsabilità d'impresa,* 2022, 7. L'Autore afferma che il discorso sulla gestione del rischio non può limitarsi al tema della mera pericolosità dell'attività in termini civilistici classici, ma deve essere affrontato con riguardo alla natura e al contenuto degli obblighi che caratterizzano lo svolgimento di una determinata attività. Sul punto si rimanda a P. PERLINGERI, *Privacy digitale e protezione dei dati personali tra foro e mercato*, in *Foro. Nap*., 2018, 481; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 54 ss.; ID., *L'equivoco del-*

tiche invasive diventano *routine* attraverso esposizioni ripetute che ci abituano a essere vulnerabili,[67] spesso anche nell'errata percezione di aver accesso gratuitamente a servizi digitali erogati, in realtà, in cambio di dati.[68]

A fronte dello scenario descritto non stupisce che emerge un nuovo concetto di vulnerabilità, non legato a *deficit* fisiologici-cognitivi degli esseri umani, ma alla loro stessa condizione di esseri umani che operano in un ambiente digitale.[69] Vulnerabilità che si accentuano a causa di sistemi in grado di delineare profili digitali in base ai quali alcune persone, che si trovano in situazioni di disagio o bisogno, finiscono per essere escluse dalle opportunità tradizionali, come il lavoro, l'istruzione e l'alloggio e possono essere presi di mira per servizi e prodotti predatori, così da sollevare profonde questioni di giustizia sociale che, non potendo essere risolte a livello di singolo contratto e singola operazione economica, devono essere affidate anche alle regole dell'attività di prestazione di servizi digitali e di utilizzo di sistemi di intelligenza artificiale. [70]

la privacy. Persona vs dato personale, Napoli, 2022. G. CARAPEZZA FIGLIA, *"L'equivoco della privacy". Circolazione dei dati personali e tutela della persona*, in *Jus Civile*, 2022, 1372 ss.; R. SENIGAGLIA, *"L'equivoco della privacy" tra consenso e capacità*, ivi, 1378 ss. Con particolare riferimento alle problematiche relative al consumatore, si rimanda a A. DE FRANCESCHI, *Consumers' Vulnerability in the Digital Economy: Personal Data as Counterperformance and Digital Obsolescence*, in *European Journal of Consumer Law*, 2022, 73-93.

[67] *W. HARTZOG, E. SELINGER, J. GUNAWAN, Privacy Nicks: How the Law Normalizes Surveillance, in www.ailawblawg.com.*

[68] Sul punto cfr. *I. DOMURATH, Platform Economy and Individual Autonomy*, in *European Review of Private Law*, 2022, 951 ss.; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. civ.*, 2019, 499 ss.; G. DE CRISTOFARO, *40 anni di diritto europeo dei contratti dei consumatori: linee evolutive e prospettive future*, in *I Contratti,* 2019, 187 ss. Sulla necessità di una rilettura in chiave evolutiva della nozione di prezzo e degli obblighi di informazione precontrattuale si rimanda a A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1393 ss.; ID., *La circolazione dei dati personali nella proposta di direttiva UE sulla fornitura dei contenuti digitali*, in D. POLETTI, A. MANTELERO (a cura di), *Regolare la tecnologia: il regolamento UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna, Studi in tema di Internet ecosystem*, Pisa, 2018, 203 ss. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva 2019/770 e il Regolamento 2016/679, in Annuario del contratto, 2018,* 127 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, *passim*. Per una accurata ricostruzione dell'ampia bibliografia in argomento si rimanda a S. ORLANDO, *Per un sindacato di liceità del consenso privacy,* cit., 527 ss.

[69] L. GATT, I. A. CAGGIANO, *Consumers and digital environments as a structural vulnerability relationship,* in *European Journal of Privacy Law & Technologies (EJPLT),* 2022, 8 ss. Cfr. M. PÉREZ-ESCOLAR, F. CANET, *Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework*, in *Univ Access Inf. Soc.,* 2022, 11 ss. Per una riflessione interdisciplinare si rimanda a S. TURNER, *Vulnerability and human righst*, University Park, 2006. A. MOLLO, *La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici*, in *European Journal of Privacy Law & Technologies*, 2021, 199 ss.; B. RABAI, *The role of technology and innovation in digital and social inclusion. The case of disability in a public perspective,* in *Rivista di Diritto dei Media*, 2022, 199; P. PASSAGLIA, *La problematica definizione dell'accesso a Internet e le sue ricadute su esclusioni sociali e potenziali discriminazioni,* in *Rivista di Diritto dei Media*, 2021, 1 ss.

[70] M. E. GILMAN, *Poverty Lawgorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities*, in *Data & Society*, 2020, e in *https://ssrn.com/abstract=3699650.*