GIUSTIZIA INSIEME

Diritto e Processo Amministrativo

Utilizzo di sistemi automatizzati in assenza di sorveglianza umana

di Lorenza Tomassi

10 gennaio 2025

Utilizzo di sistemi automatizzati in assenza di sorveglianza umana. AGCOM e Meta: la storia infinita (nota a TAR Lazio, sez. IV, 24 gennaio 2024, n. 1393)

di Lorenza Tomassi

Sommario: **1.** Premessa; **2.** I fatti controversi; **3.** La ricostruzione del quadro normativo: la distinzione tra hosting provider attivo e passivo; **4.** La configurazione come hosting provider passivo in virtù dell'utilizzo di sistemi automatici di verifica; **5.** Considerazioni critiche: i punti deboli dell'attuale inquadramento giuridico; **6.** Riflessioni di carattere generale: i rischi connessi all'assenza di sorveglianza umana rispetto all'uso di sistemi automatici anche alla luce dell'IA ACT.

1. Premessa

Nella infinita querelle tra Agcom e le c.d. Big Tech (i.e. Meta Platforms e Google)[i], interviene una nuova pronuncia del giudice amministrativo che, oltre a confermare orientamenti già espressi, consente, almeno a parere di chi scrive, di spostare la riflessione sotto un profilo diverso, legato all'uso di sistemi automatizzati, in sostituzione dell'uomo, ai fini della verifica dei contenuti pubblicati sulle loro piattaforme.

Come si avrà modo di approfondire in questa sede, infatti, sembrerebbe che la sostituzione dell'uomo con la "macchina" nell'assolvimento delle funzioni di vigilanza rispetto ai contenuti immessi**[ii]**, giustificherebbe l'assenza di responsabilità da parte della società che ospita il contenuto, anche qualora sia accertata, in una fase successiva, la natura illecita dello stesso.

Lungi dal voler affrontare la questione in chiave civilistica**[iii]**, tale assunto rappresenta lo spunto per riflettere, ancora una volta, in che termini l'uso di sistemi automatizzati, capaci di sostituire l'uomo nell'assolvimento delle sue funzioni, possa essere consentito senza correre il rischio di generare dei coni d'ombra in cui venga meno la riferibilità dell'operato della macchina all'uomo**[iv]**.

Da qui, la questione se l'intelligenza artificiale sia davvero strumentale all'uomo e, come tale, trasferisce su quest'ultimo sempre la responsabilità del suo operato o, diversamente, se non sia da considerarsi sostitutiva, generando zone franche rispetto al regime della titolarità delle azioni o delle operazioni da essa compiute.

2. I fatti controversi

A seguito di una attività di monitoraggio avviata d'ufficio, l'AGCOM rilevava come, in più occasioni, nel periodo di maggio 2022, Facebook aveva ospitato contenuti "sponsorizzati" e, dunque, a pagamento, idonei a promuovere e pubblicizzare attività di gioco e scommesse online con vincite in denaro**[v]**.

Ne conseguiva, da parte dell'Autorità, un atto di contestazione (n. 6/22/DSDI - Proc 8/FDG) nei confronti di Meta Platforms per la violazione dell'art. 9, rubricato "Divieto di pubblicità giochi e scommesse", del d.l. n. 87 del 2018 (c.d. Decreto Dignità), in base al quale è disposto il divieto di qualsiasi forma di pubblicità, anche indiretta, relativa a giochi o scommesse con vincite di denaro nonché al gioco d'azzardo, comunque effettuata e su qualunque mezzo, compresi i social media.

La stessa disposizione, al comma successivo, dispone che sono responsabili dell'illecito il "committente", il "proprietario del mezzo o del sito di diffusione", il "proprietario del mezzo o del sito di destinazione" e "l'organizzatore della manifestazione, evento o attività". Si tratta quindi di un divieto generale che introduce per l'ordinamento italiano una responsabilità oggettiva in capo ad una pluralità di soggetti tutti egualmente responsabili.

Meta procedeva, di conseguenza, a rimuovere i contenuti contestati, riconoscendo la violazione delle normative del Servizio Facebook e, altresì, manifestava la propria disponibilità ad

instaurare un dialogo con l'autorità stessa affinché quest'ultima potesse segnalare in modo più agevole eventuali e presunte violazioni della disposizione sopra richiamata.

Ciononostante, la società rilevava che l'atto di contestazione si poneva manifestamente in contrasto con le previsioni della Direttiva 2000/31/EC, cd. Direttiva E-Commerce, recepita nell'ordinamento nazionale con il D. Lgs. n. 70/2003, c.d. Decreto E- Commerce. In particolare, evidenziava la società che, ai sensi degli artt. 14 e 15 della Direttiva, trasposti, rispettivamente, negli artt. 16 e 17 del Decreto E-Commerce, gli hosting providers, come Facebook, "(i) non possano essere ritenuti responsabili della correttezza delle informazioni caricate sulla piattaforma e (ii) non possano essere soggetti ad un obbligo generale di sorveglianza sulle informazioni che gli utenti trasmettono o memorizzano, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite".

Ulteriormente, la società sosteneva che, nonostante in capo ad essa ricorresse un onere di rimozione dei contenuti vietati, una volta portati a sua conoscenza, ciò non determina un onere di verifica e ispezione rispetto a tutti i contenuti pubblicati sulla piattaforma di cui è gestore. Proprio l'assenza di tale obbligo, qualificherebbe Meta come Hosting provider passivo che lo esonera dalla responsabilità dei contenuti, anche quelli lesivi, diffusi per il suo tramite.

Emerge così che le parti in causa ritengono sussistere l'applicazione di due disposizioni differenti.

Secondo Meta, infatti, nel caso controverso non dovrebbe trovare applicazione la disciplina recata dall'art 9 del Decreto Dignità, ma piuttosto, quella espressa nella Direttiva 2000/31/CE, c.d. Direttiva E- commerce, recepita nel nostro ordinamento attraverso il D.lgs. n. 70/2003, c.d. Decreto E-commerce, che esclude proprio la responsabilità degli hosting provider per i contenuti caricati da terzi sulle loro piattaforme**[vi]**.

Di parere contrario, invero, si pone l'Agcom che, richiamando il Decreto Dignità, ritiene sussistere una responsabilità oggettiva scaturita dal divieto assoluto di diffusione su qualunque mezzo, anche i social media, di "qualsiasi forma di pubblicità, anche indiretta" relativa al gioco di azzardo.

Non troverebbe applicazione, poi, secondo l'autorità il decreto E- commerce dal momento che lo stesso esclude il suo campo di applicazione ai giochi d'azzardo, che implicano una posta pecuniaria, i giochi di fortuna, compresi il lotto, le lotterie, le scommesse i concorsi pronostici e gli altri giochi come definiti dalla normativa vigente, nonché quelli nei quali l'elemento aleatorio è prevalente" (art. 1, comma 2, lett. g), d.lgs. n. 70/03)**[vii]**.

In particolare, da parte dell'Autorità vi sarebbero due considerazioni ulteriori che confermano la colpevolezza della società: in primo luogo i contenuti contestati erano "sponsorizzati", vale a dire delle inserzioni pubblicizzate da Meta previo pagamento di utenti business. In secondo luogo, poi, rispetto a queste inserzioni pubblicitarie, il caricamento sulla piattaforma non è immediato ma, al contrario, sono necessarie ventiquattro ore affinché la società intermediaria possa verificare se il contenuto rispetti le norme pubblicitarie della piattaforma**[viii]**. Tale controllo avviene generalmente attraverso tecnologie automatizzate ma, in alcuni casi non specificati, è richiesto il controllo da parte di persone fisiche.

La combinazione di tali considerazioni ha, quindi, indotto ulteriormente l'autorità a ritenere che Meta fosse a conoscenza del contenuto ospitato e, pertanto, con delibera n. 422/22/CONS, ha sanzionato la società al pagamento di 750 mila euro, cui ha fatto seguito l'impugnazione del provvedimento da parte della società sanzionata.

Da qui, il giudizio in commento.

3. La ricostruzione del quadro normativo: la distinzione tra hosting provider attivo e passivo

Nell'accogliere il ricorso presentato da Meta Platforms, annullando la sanzione comminata da AGCOM, il giudice amministrativo si è principalmente soffermato sul regime della responsabilità degli hosting provider secondo quanto stabilito dalla direttiva 2000/31/CE, c.d. direttiva e-commerce e dalle successive modifiche.

In questa sede, pare opportuno dare conto dell'evoluzione del quadro normativo di riferimento al fine di comprendere quali sono state le logiche che hanno ispirato il legislatore nel corso degli anni.

La direttiva sull' e-commerce risale al 2000, vale a dire un'epoca in cui la rete non aveva ancora assunto quella posizione così centrale che riveste oggi. Per queste ragioni, la ratio del legislatore europeo era stata, sin dall'inizio, volta a configurare un quadro giuridico entro il quale favorire lo sviluppo della libera circolazione dei servizi elettronici**[ix]**nonché le misure ivi previste si limitavano, evocando il principio di proporzionalità, "al minimo necessario" per raggiungere l'obiettivo del buon funzionamento del mercato interno**[x]**.

All'interno della direttiva, i prestatori di servizi vengono distinti a seconda che l'attività svolta sia di semplice trasporto (c.d. mere conduit)**[xi]**, di memorizzazione temporanea delle informazioni (c.d. caching)**[xii]** o di hosting**[xiii]**, intesa come memorizzazione permanente delle informazioni

[xiv]. Meta, nella fattispecie incriminata, svolge una attività di hosting dal momento che la propria piattaforma prevede la memorizzazione definitiva delle informazioni caricate.

Sulla base di queste condizioni, la direttiva prevedeva una generale disciplina di esonero della responsabilità in capo ai prestatori di servizi in qualità di hosting provider, la cui attività era di ordine meramente tecnico, automatico e passivo, e che si limitava, così, alla memorizzazione delle informazioni trasmesse**[xv]**. Rispetto a tale tipologia di servizio, l'art. 14 escludeva la responsabilità nei casi in cui i fornitori di servizi non fossero stati a conoscenza delle attività illecite che avvengono tramite i propri servizi ed a condizione che, avutane conoscenza, agivano immediatamente per rimuovere i contenuti illeciti. Tale regime si combinava, poi, con quanto disposto dal successivo articolo 15, in cui era sancita l'assenza di un obbligo generale di sorveglianza.

Nei medesimi termini si poneva, a livello nazionale, il D.lgs. n. 70/2003, adottato in attuazione della direttiva, negli artt. 16 e 17, oggi definitivamente abrogati dal D.lgs. n. 50/2024.

La scelta di sottrarre l'hosting provider a un generale dovere di controllo preventivo, a cui facesse seguito l'attribuzione di un regime di responsabilità per i contenuti illeciti ospitati, ha ben presto evidenziato i suoi limiti, in ragione principalmente dal repentino sviluppo tecnologico che ha mutato profondamente il rapporto tra utenti e piattaforme**[xvi]**. Anche la letteratura sul tema ha, a più riprese, riconosciuto l'obsolescenza dalla disciplina recata nella direttiva e-commerce, ritenendo necessario un ripensamento della stessa**[xvii]**. In particolare, è emersa l'esigenza di fornire adeguate forme di tutela rispetto ai diritti degli utenti che "navigano" in rete ma che, più propriamente, sapesse cogliere i rischi specifici, connessi a questa nuova realtà virtuale, in cui le piattaforme offrono innumerevoli servizi**[xviii]**.

Su questi presupposti è stato adottato, nel 2022, il Digital Service Act, vale a dire il nuovo regolamento sui servizi digitali, UE 2022/2065**[xix]**, nel quale si evidenzia che un comportamento responsabile e diligente da parte dei prestatori di servizi intermediari è essenziale per un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea siano efficacemente tutelati e l'innovazione sia agevolata, contrastando la diffusione di contenuti illegali online e i rischi per la società che la diffusione della disinformazione o di altri contenuti può generare**[xx]**.

Nonostante i buoni propositi, la normativa prevista al suo interno, pur introducendo nuovi obblighi in materia di trasparenza**[xxi]**, è stata strutturata sulla falsa riga della precedente, sollevando, in dottrina, le medesime criticità osservate in precedenza. Permane, infatti, all'art. 6,

un generale esonero dalla responsabilità degli *hosting* per i contenuti "caricati" dai terzi, e altresì, si estende tale esenzione nelle ipotesi in cui i *providers* svolgano di propria iniziativa attività volte a individuare e a rimuovere contenuti illegali memorizzati dagli utenti**[xxii]**.

All'interno di questo quadro normativo si colloca la sentenza in esame che, aderendo a consolidati orientamenti europei e nazionali**[xxiii]**, si è soffermata sulla distinzione tra hosting provider attivo e hosting provider passivo, ricavata principalmente in via interpretativa del dato normativo di cui si è appena dato conto**[xxiv]**.

Secondo i giudici, si configura come hosting provider passivo, il prestatore di servizi che svolge una mera attività di prestazioni di servizi di ordine principalmente tecnico e automatico che non si traduce in una attività di controllo delle informazioni trasmesse né tantomeno questo determina la conoscenza delle informazioni stesse. Rispetto, quindi, ai contenuti immessi, il prestatore rimane pressoché neutrale**[xxv]**, con la conseguenza che l'attività svolta non gli consente di sapere se si sia in presenza di attività illecite o meno.

Ne consegue, quindi, che l'hosting provider passivo può essere considerato responsabile dei contenuti illeciti ospitati nei soli casi in cui non li abbia rimossi una volta che ne sia venuto a conoscenza.

Al contrario, l'hosting provider attivo manipola le informazioni che sono inserite sulla propria piattaforma e, come tale, esercita una funzione di controllo in piena conoscenza dei contenuti memorizzati. Il controllo e la conoscenza determinano, conseguentemente, la sussistenza della responsabilità dell'hosting in ordine alle informazioni immesse.

I giudici riconoscono che il fine perseguito da tale legislazione è quello di evitare che il provider venga considerato attivo per il solo fatto di promuovere di propria iniziativa delle forme di controllo dei contenuti memorizzati dagli utenti e che possa, conseguentemente, essere indotto a non adottare alcun sistema diretto a prevenire l'immissione di contenuti illegali nella rete, stante la responsabilità che gli verrebbe imputata in virtù di tale condotta.

4. La configurazione come hosting provider passivo in virtù dell'utilizzo di sistemi automatici di verifica

Poste queste premesse, il giudice si è, quindi, domandato se il sistema di controllo di cui Meta disponesse sia tale da conferirgli la natura di hosting provider attivo, attribuendogli la responsabilità dei contenuti immessi o, al contrario, aderendo a consolidata giurisprudenza **[xxvi]**, la natura tecnica ed automatica dei suoi meccanismi sia tale da conferirgli un ruolo

neutrale rispetto a tali informazioni.

Su tali aspetti, i giudici hanno in primo luogo osservato nella sentenza de qua che i sistemi utilizzati dalla società sanzionata sono principalmente automatici, con la conseguenza che il controllo manuale, da parte di una persona fisica, da cui dipende il riconoscimento della responsabilità, avviene solo in ipotesi residuali rispetto, peraltro, a un numero di contenuti certamente esiguo se si considera la mole di inserzioni che Facebook ospita ogni giorno.

L'intervento umano, secondo quanto sostenuto da Meta, verrebbe richiesto proprio dal software, seppur non chiarendo in base a quali meccanismi e presupposti, tanto nei casi di verifica manuale delle inserzioni quanto ai fini del miglioramento e dell'addestramento del sistema automatizzato utilizzato per le predette finalità.

Sulla base di questi presupposti, perciò, i giudici hanno negato la natura di hosting provider attivo alla società ricorrente, giacché l'attività svolta dal gestore è avvenuta in via del tutto automatizzata tale da non consentire alla stessa la manipolazione e, quindi, la conoscenza dei dati memorizzati sulla propria piattaforma.

Deve essere osservato, poi, che secondo i giudici una manipolazione dalle informazioni si avrebbe, oltre all'ipotesi dell'intervento della persona fisica, anche nei casi in cui il sistema automatizzato procedesse a rifiutare la condivisione del contenuto, perché contrario agli Standard della community. In questo modo, il prestatore verrebbe declinato in termini di hosting provider attivo dal momento che la sua attività sarebbe funzionale ad impedire la condivisione di contenuti illeciti e, quindi, la fruizione di questi agli utenti.

Qualora, al contrario, l'attività svolta dal software sia volta nel senso di accogliere una inserzione, non essendoci alcuna manipolazione, verrebbe a mancare il ruolo attivo su cui fondare la responsabilità del gestore. Trattandosi di un accertamento tecnico ed automatico, il gestore, come nel caso de qua, non può venire a conoscenza del contenuto illegale creato dall'utente e, di conseguenza, non ha la possibilità di attivarsi per rimuoverlo.

Nelle considerazioni dei giudici, tale interpretazione troverebbe conferma nel fatto ulteriore che AGCOM non sarebbe stata in grado di provare che il caso controverso riguarderebbe una di quelle limitate ipotesi in cui al controllo automatizzato abbia fatto seguito l'intervento manuale della persona fisica, c.d. revisione umana, tale da giustificare il passaggio da passivo ad attivo dell'hosting provider.

In definitiva, dunque, non essendo stato provato da parte dell'autorità l'intervento del funzionario umano da cui dipende la conoscenza effettiva da parte di Meta dei contenuti illeciti ospitati, i giudici hanno accolto il ricorso, annullando, di conseguenza, la sanzione di Agcom imposta nei confronti della società ricorrente**[xxvii]**.

5. Considerazioni critiche: i punti deboli dell'attuale inquadramento giuridico.

La sentenza in commento, pur aderendo a precedenti ormai consolidati nel nostro ordinamento, rappresenta il presupposto, come si anticipava in premessa, per riflettere sulla opportunità e sulla adeguatezza del quadro normativo in riferimento all'utilizzo di sistemi automatizzati per l'esercizio di attività di controllo dei contenuti immessi nella rete ma, più in generale, per indagare sul rapporto che intercorre tra l'uomo e la macchina qualora quest'ultima svolga funzioni prima esercitate dall'uomo.

Deve essere osservato in primo luogo, che, a parere di chi scrive, sebbene l'orientamento espresso dai giudici sia coerente con il quadro normativo di riferimento, quest'ultimo risulta essere ancora non del tutto aderente ai mutamenti e al consolidamento che ha assunto l'intelligenza artificiale, ormai, a livello globale, negli ambiti più disparati.

Come visto, l'esenzione della responsabilità del soggetto che utilizza i sistemi automatizzati di controllo può essere invocata ogniqualvolta questo non sia a conoscenza degli illeciti ammessi per il tramite di tali sistemi.

Ciononostante, non può farsi a meno di notare che la disciplina recata in tale contesto presenti alcune debolezze. Come è emerso, il prestatore del servizio rimane passivo nei casi in cui l'inserzione, pur dal contenuto illecito, venga pubblicata a seguito del controllo automatico; al contrario, qualora dallo stesso controllo automatico emerga il rifiuto del caricamento dell'inserzione sulla piattaforma, allora il prestatore assume le vesti di hosting provider attivo. Ciò troverebbe giustificazione nel fatto che, secondo costante orientamento dai giudici, in questo secondo caso si è verificata una manipolazione del contenuto da parte dell'internet service provider.

Tale assunto, a parere di chi scrive, presenta alcune criticità. Deve essere evidenziato, infatti, che tanto nei casi in cui il contenuto sia ammesso, quanto in quelli in cui ne sia disposto il divieto, il prestatore non opera alcuna attività di manipolazione del dato. In entrambi i casi, il dato resta immutato dal momento che l'attività svolta non "arricchisce" la fruizione dei contenuti**[xxviii]**. A mutare, invero, è la capacità del sistema automatizzato di controllo di rilevare un potenziale illecito. L'attività posta in essere dal sistema, sia in caso di ammissione che di diniego di

condivisione dell'inserzione, è la medesima, sostanziandosi in un meccanismo automatico e passivo di controllo. In entrambe le attività, di fatto, non si è verificata nessuna revisione da parte della persona fisica che, come visto, per espressa previsione legislativa e costante orientamento dei giudici, rappresenta il presupposto per qualificare l'hosting provider come attivo e a cui faccia seguito l'applicazione del regime della responsabilità.

A fronte di questo, la scelta di distinguere la natura dell'hosting provider a seconda se il contenuto sia stato ammesso o vietato, trova la sua ragion d'essere, almeno a parere di chi scrive, nella volontà legislativa di prevedere un regime di favore nei casi in cui il prestatore di servizi non sia stato in grado, attraverso l'uso di un sistema automatizzato, di riconoscere un illecito.

E questo mette in luce due questioni ulteriori: l'una, relativa alla capacità dei sistemi di autoapprendimento di riconoscere la violazione delle norme e, l'altra, relativa alla riferibilità dell'attività realizzata da tale modello all'uomo, che, in questo specifico caso, coincide con la società di intermediazione.

Rispetto alla prima, deve osservarsi che nel dibattito scientifico, i modelli di autoapprendimento, c.d. machine learning, vengono esaltati per la loro capacità intrinseca di auto apprendere dalla loro esperienza. Detto diversamente, tali sistemi dovrebbero essere in grado, allenandosi sulla elevata quantità di dati immessi, di generare degli output che non scaturiscono da comandi precedentemente prescritti dal *data scientist* ma che, al contrario, sono generati da una autonoma capacità del modello di combinare le variabili al suo interno. Questo, operando secondo regole statistiche, dovrebbe rendere una determinazione che dovrebbe essere, tra quelle possibili, quella più probabile.

In questi termini si colloca anche il recente Regolamento sull'Intelligenza Artificiale secondo cui i sistemi di intelligenza artificiale si distinguono dai tradizionali software per la loro capacità inferenziale, intesa come abilità di generare output, quali previsioni o decisioni, che possono influenzare gli ambienti fisici e virtuali**[xxix]**.

Questa caratteristica propria del sistema dovrebbe consentirgli una costante capacità di adattamento ai mutamenti del dato normativo e alla sua successiva applicazione sul piano pratico. Ciò vuol dire, dunque, che un sistema di autoapprendimento adeguatamente allenato dovrebbe essere capace di riconoscere quando una fattispecie soddisfi le caratteristiche di una violazione disciplinata a livello normativo**[xxx]**.

Ciononostante, non sono pochi i casi in cui l'AGCOM sanzioni gli internet service provider perché i sistemi di controllo e monitoraggio di cui dispongono non sono in grado di riconoscere una

violazione commessa dagli utenti**[xxxi]**. Il che solleva non poche perplessità da un lato, circa la capacità di questi modelli di saper interpretare il dato normativo applicato alle esperienze pratiche e, dall'altro lato, con riguardo alla capacità degli utilizzatori di addestrare tali modelli.

Nel caso in commento, infatti, la fattispecie incriminata conteneva evidenti elementi (quali, ad esempio, il richiamo di vincite di ingenti somme di denaro) sulla pubblicità relativa al gioco d'azzardo che un modello adeguatamente addestrato, si ritiene, avrebbe dovuto riconoscere.

Evidenza, tra l'altro, confermata dal fatto che, una volta intervenuto il funzionario fisico, si è provveduto a rimuovere immediatamente l'inserzione, stante il suo contenuto chiaramente illecito.

Una volta in più sembrerebbe, quindi, che l'apporto umano, nell'interpretazione delle norme, sia ancora essenziale e questo induce a indagare con cautela l'impianto normativo attualmente in vigore, in cui, di fatto, non si imputano a nessuno i costanti errori commessi dai modelli automatici di controllo.

È chiaro che rispetto all'elevato numero di contenuti che la rete e le singole piattaforme ospitano ogni giorno diventa arduo, se non impossibile, garantire un controllo efficiente, specie se questo fosse delegato ad una persona fisica; ciononostante, tali condizioni non possono rappresentare il presupposto per giustificare l'assenza di forme adeguate di controllo e, altresì, per non ricondurre la riferibilità delle azioni esperite per il tramite di modelli automatizzati all'uomo. Se così fosse, il rischio è che, come correttamente osservato in dottrina, la rete diventi un "far web", dal momento che la difficoltà di "controllare" dia luogo ad una zona d'ombra, il c.d. cyberspazio, in cui la violazione delle norme e dei diritti fondamentali sarebbe difficilmente accertabile per le ragioni sinora esposte**[xxxii]**.

Da qui se ne può trarre una ulteriore riflessione, vale a dire valutare l'opportunità di rendere responsabile il soggetto che utilizza tali modelli, non tanto per le violazioni commesse da parte di terzi quanto piuttosto per l'evidente incapacità o obsolescenza dei sistemi utilizzati di comprendere e prevenire eventuali violazioni. Di fatto, lo stato di sviluppo di questi sistemi automatizzati dipende non solo dalla capacità stessa del modello di auto apprendere dalla propria "esperienza" ma, principalmente, dipende dalla tipologia del modello utilizzato, da come questo viene programmato dal *data scientist* e dalla quantità e dalla qualità dei dati immessi **[xxxiii]**; operazioni queste che discendono da scelte organizzative umane e, come tali, a questi imputabili.

Se nel vigente quadro normativo, l'orientamento è quello di non caricare eccessivamente di responsabilità gli hosting provider per violazioni commesse da terzi, si ritiene che l'attribuzione, invero, della titolarità degli errori commessi da un sistema automatizzato di monitoraggio può rappresentare un giusto compromesso. In questo modo di operare, infatti, il soggetto utilizzatore di sistemi di autoapprendimento sarebbe continuamente sollecitato ad aggiornare e a migliorare i sistemi di cui fa utilizzo, nonché ricondurrebbe la titolarità delle operazioni commesse dal modello artificiale a chi ne fa uso, riducendo i rischi di generare potenziali zone franche, sottratte al rispetto del diritto**[xxxiv]**.

6. Riflessioni di carattere generale: i rischi connessi all'assenza di sorveglianza umana rispetto all'uso di sistemi automatici anche alla luce dell'AI Act

La disciplina appena analizzata consente, altresì, di inquadrare le riflessioni sin qui esposte in una prospettiva di sistema, specie con riferimento all'utilizzo di modelli di autoapprendimento per l'assolvimento di determinate funzioni in sostituzione dell'uomo.

Deve essere messo in evidenza che, non solo i più recenti interventi dello stesso giudice amministrativo**[xxxv]**, ma anche quelli legislativi**[xxxvi]**, sono orientati a riferire l'utilizzo dell'intelligenza artificiale alla persona fisica.

Applicata al potere pubblico, infatti, l'intelligenza artificiale è stata interpretata in funzione principalmente servente e strumentale alla attività realizzata dal funzionario umano**[xxxvii]**.

In questo senso, i giudici amministrativi hanno configurato le tecnologie, nell'esercizio dell'attività amministrativa, alla stregua "di modulo organizzativo, di strumento procedimentale ed istruttorio, soggetto alle verifiche tipiche di ogni procedimento amministrativo, il quale resta il modus operandi della scelta autoritativa, da svolgersi sulla scorta delle legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico, titolare del potere"**[xxxviii]**. Da questi presupposti ne consegue che l'utilizzo delle tecnologie "impone un controllo umano del procedimento, in funzione di garanzia (cd. human in the loop), in modo che il funzionario possa in qualsiasi momento intervenire per compiere interlocuzioni con il privato, per verificare a monte l'esattezza dei dati da elaborare, mantenendo il costante controllo del procedimento" **[xxxix]**.

Da questi richiami emerge che la tutela dell'interesse pubblico, bilanciato con altri interessi individuali, non può essere "spersonalizzata"; vuol dire, al contrario, che l'amministrazione rimane sempre il soggetto titolare del potere conferito dal legislatore e, come tale, l'attività istruttoria o decisoria condotta da un modello automatizzato, sarà sempre ad essa riferita,

salvaguardando così le pretese di chiunque entri in contatto con l'amministrazione "artificiale" **[xl]**.

In questo modo di operare, il risultato computazionale non coincide mai con il risultato finale ma, piuttosto, rappresenta il presupposto istruttorio su cui fondare la determinazione finale assunta dal funzionario persona fisica. Quest'ultimo potrà decidere di aderire alle risultanze rese dal sistema automatico e, quindi, di fatto, sovrapponendo il risultato computazionale con quello finale o, al contrario, potrà discostarsene, giungendo ad una determinazione nuova. In entrambi i casi si tratta, come evidente, di scelte volitive umane e, come tali, imputabili alla persona fisica che le avrà rese.

Questo impianto trova conferma nella stessa legge sul procedimento amministrativo, la l. n. 241/1990, laddove, all'art. 6, attribuisce al responsabile del procedimento, persona fisica, diversi compiti volti principalmente ad assicurare un corretto e partecipato svolgimento della attività istruttoria e decisionale. Tra questi rileva, in particolare, il divieto, per chi assume la decisione finale, di discostarsi dalle risultanze dell'istruttoria se non indicandone la motivazione nel provvedimento finale.

In questi termini si colloca, più in generale, anche l'articolo 22 del Regolamento generale sulla protezione dei dati, che riconosce un limite intrinseco all'uso di modelli automatizzati, laddove si impone che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona**[xli]**.

Ma tutto ciò sembra trovare definitiva conferma nel più recente Regolamento europeo sull'intelligenza artificiale che prevede, per i sistemi classificati ad alto rischio**[xlii]**, un obbligo di sorveglianza umana**[xliii]**.

Tale obbligo impone che i sistemi di IA siano sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani**[xliv]**. A tale principio il regolamento dedica una apposita disposizione, l'art. 14, in cui è stabilito che tali sistemi sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.

Nello specifico, la disposizione prevede alcune accortezze nei confronti della persona fisica a cui è affidata la sorveglianza umana. In questo senso, l'articolo dispone in primo luogo che la

persona in questione deve essere messa nella condizione di poter comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento**[xlv]**, al fine principale di evitare che si faccia un eccessivo affidamento sull'output prodotto dal sistema di (c.d. distorsione dell'automazione)**[xlvi]**. Con la ulteriore conseguenza, quindi, che la persona che sorveglia il sistema deve poter essere in grado di interpretare correttamente l'output del sistema di IA ad alto rischio**[xlvii]**. Questo vuol dire che, non solo, il sorvegliante umano deve ignorare, annullare o ribaltare l'output quando secondo proprie valutazioni ciò si rende opportuno**[xlviii]** ma, altresì, che deve intervenire sul sistema, anche arrestandolo, quando ragioni di funzionamento lo richiedono**[xlix]**.

Da questi richiami normativi, seppur sommari, emerge con tutta evidenza che i modelli di intelligenza artificiale, pur nella consapevolezza legislativa di essere capaci di funzionare in via del tutto autonoma, devono essere affiancati e monitorati sempre dalla persona fisica che resta il titolare del potere attribuito dal legislatore e, come tale, titolare anche dell'attività svolta per il tramite di tali modelli.

Se è vero, infatti, che la tecnologia e l'automatizzazione possono apportare notevoli benefici in termini di riduzione dei tempi istruttori e decisionali, rispetto soprattutto a procedure seriali, come lo è potenzialmente la fattispecie in esame, è altrettanto vero che va verificato se, a tale modo di operare, non faccia seguito una potenziale compressione dei diritti fondamentali.

In altri termini, va verificato se questi modelli intelligenti siano capaci di rilevare eventuali violazioni di legge.

Allo stato attuale sembra che le tecnologie, dalle più semplici alle più evolute, abbiano, in più occasioni, dimostrato una scarsa capacità di tutelare gli interessi coinvolti. Questo si è verificato, ad esempio, nelle procedure di reclutamento del personale docente, ove l'algoritmo utilizzato non è stato in grado di combinare correttamente i punteggi dei candidati, unitamente alle preferenze espresse**[l]**; è avvenuto nelle ipotesi di concessione del mutuo bancario, ove sistemi predittivi hanno generato, per il richiedente, un punteggio negativo (c.d. *scoring*) sulla capacità di ripagarlo, senza indicare sulla base di quali elementi tale punteggio fosse stato ottenuto e l'incisività di ogni variabile**[li]**; così come nelle ipotesi delle prenotazioni dei c.d. "riders" nel caso Deliveroo, in cui l'algoritmo Frank ha favorito le prenotazioni per i riders con un punteggio più elevato, a discapito di riders con un punteggio più basso**[lii]**; o nei casi in cui sulle piattaforme digitali non siano stati rimossi contenuti chiaramente discriminatori**[liii]**.

Negli esempi richiamati, occorre osservare, l'errore del sistema è dipeso tanto da un errore "umano", inteso come incapacità di programmare il sistema e di monitorarne l'utilizzo, quanto dalla c.d. "black box" del modello che non permette di risalire al procedimento istruttorio al fine di verificare come le variabili inserite al suo interno siano state combinate tra loro.

Queste condizioni evidenziano come la tecnologia, semplice o evoluta che sia, per poter trovare un suo positivo spazio, ha bisogno in primo luogo di persone capaci di programmarla correttamente e successivamente di intervenire sul modello quando ciò si rende opportuno.

L'intervento umano, infatti, dovrebbe essere previsto in ogni fase di utilizzo e, quindi, dal momento di costruzione del modello sino all'adozione della determinazione finale, al fine quantomeno di ridurre gli errori e correggere il sistema quando questo lo renda possibile.

Non sembra, pertanto, essere coerente con tale quadro la disciplina prevista per gli hosting provider.

Seppur novellata di recente, infatti, permane una grave lacuna sul regime della responsabilità delle decisioni assunte per il tramite di sistemi automatici di apprendimento**[liv]**. La disciplina ricostruita con la sentenza in commento, infatti, sembra favorire uno spazio entro il quale le azioni commesse per il tramite di strumenti di intelligenza artificiale non siano riconducibili a nessuno, collocando lo strumento non in via strumentale all'uomo, ma in una funzione ad esso sostitutiva. Con la naturale conseguenza che, eventuali violazioni normative, come di fatto si verifica, non sono imputabili a nessuno e restano, perciò, non sanzionabili.

[i] Per una ampia e aggiornata ricostruzione sul tema v., per tutti, A. ZURZOLO, *La nuova frontiera della regolazione delle piattaforme digitali: le sanzioni contro Google e Meta*, in *Dir. Mer. Tecn.*, 22 febbraio 2023.

[ii] Il dibattito è particolarmente accesso in ambito amministrativo. In argomento sia consentito rinviare a L. TOMASSI, M. INTERLANDI, *La decisione amministrativa algoritmica*, in A. Contieri (a cura di), *Approfondimenti di diritto amministrativo*, ES, Napoli, 2022. V., ex multis, G. GALLONE. *Riserve di umanità e funzioni amministrative*, Milano, Cedam, 2023; G. AVANZINI, *Decisioni amministrative e algoritmi informatici*, ES, Napoli, 2019, A. DI MARTINO, *Tecnica e potere nell'amministrazione per algoritmi*, ES, Napoli, 2023; M.C. CAVALLARO, G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, n.1/2019; M. D'ANGELOSANTE, *La consistenza del modello dell'amministrazione 'invisibile' nell'età*

della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni, in S. Civitarese Matteucci, L. Torchia (a cura di), *La Tecnificazione,* Firenze, 2016.

[iii] In tal senso si rimanda, ex multis, a G.M. RICCIO, *La responsabilità civile degli internet providers,* Giappichelli, Torino 2002.

[iv] M. OLIVETTI, *Diritti fondamentali e nuove tecnologie*, in *Journal of institutional studies*, n.2/2020, 396 ss., mette in evidenza che internet e il diritto non sono, tra loro, due entità mutuamente estranee e malgrado l'autonomia del cyberspazio o del mondo «virtuale», che è certamente portatore di codici di comportamento da esso stesso generati (ed intrinsecamente connessi con la sua dimensione tecnica), la pretesa estrema, avanzata da alcuni operatori di tale mondo, secondo la quale esso sarebbe portatore di una normatività autonoma (una sorta di lex informatica, che richiamerebbe la ben nota lex mercatoria), o addirittura di una rivendicazione (anarchica) di esenzione dalla normatività generata dalle istituzioni del mondo «reale», si rivela insostenibile, proprio in quanto lo stesso fenomeno di Internet presuppone una serie di meccanismi regolativi, che rendono possibili le attività svolte mediante esso.

[v] Su questa vicenda v. anche A. ZURZOLO, *La nuova frontiera della regolazione delle piattaforme digitali: le sanzioni contro Google e Meta,*op. cit., 41 ss.

[vi] Su questi argomenti v. F. DI IORIO, *La responsabilità dell'hosting provider nella vendita on line di biglietti sui mercati secondari (nota a Sentenza Consiglio di Stato, Sez. VI, 05/12/2023, n. 10510),* in questa rivista, 28 marzo 2024.

[vii] La sanzione comminata da Agcom, inoltre, faceva leva su una precedente pronuncia del giudice amministrativo, in cui si osservava che non esiste una puntuale normativa comunitaria sul gioco d'azzardo online e sulla relativa pubblicità, con la conseguenza che gli Stati membri hanno il diritto di determinare le modalità di organizzazione e regolamentazione a livello nazionale dell'offerta di servizi di gioco d'azzardo online, nonché il diritto di applicare tutte le misure che considerano necessarie contro i servizi di gioco d'azzardo illegali. Cfr. Tar Lazio, sez. III ter, 28 ottobre 2021, n. 11036, par. 8.3.1.

[viii] Ciò trova conferma anche negli Standard della community resi pubblici al seguente link: **https://transparency.meta.com/it-it/policies/community-standards**.

[ix] Cfr. Considerando 8 Direttiva 2000/31/CE.

[x] Cfr. Considerando 10 Direttiva 2000/31/CE.

[xi] Cfr. art. 12.

[xii] Cfr. art. 13.

[xiii] Cfr. art. 14.

[xiv] Sulla disciplina della responsabilità civile e delle diverse figure v., *ex multis*, G.M. RICCIO, *La responsabilità civile degli internet service providers*, op.cit.; G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service providers*, in *Danno e resp*., 2002, p. 5 ss.; V. ZENO ZENKOVICH, *Profili attivi e passivi della responsabilità dell'utente in* Internet, in A. PALAZZO, U. RUFFOLO (a cura di), *La tutela del navigatore,* Milano, 2002; F. DI CIOMMO, *Evoluzione tecnologica e Regole di responsabilità civile,* Napoli, 2003; M. GAMBINI, *La responsabilità civile dell'internet service provider,* Napoli, 2006;

[xv] M. GAMBINI, *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *www.costituzionalismo.it*, n.2/2011, 2 ss., riconduce l'assenza di una generale responsabilità degli Internet service providers al fatto che, diversamente, ciò condurrebbe ad un aumento eccessivo dei costi dei servizi offerti e di selezione degli operatori, con la conseguenza che solo quelli economicamente più forti potrebbero continuare ad operare. Senza considerare che il riconoscimento della responsabilità degli intermediari avrebbe conseguenze negative anche rispetto all'esercizio dei diritti e delle libertà fondamentali degli utenti e, in primo luogo, della libertà di manifestazione del pensiero.

[xvi] Sulla centralità della rete v., in particolare, L. FLORIDI, *The online manifesto, Being human in a hyperconnected era*, Springer, Londra, 2014. Sulla evoluzione che ha interessato la rete negli ultimi anni v. G. CORASANITI, *Regolazione, autoregolazione, sovraregolazione della rete: dal "far" web al "fair" web*, in *Diritto di Internet*, Gli atti digitali di "gli stati generali del diritto di internet", luiss 16, 17, 18 dicembre 2021**,** il quale osserva che la rete ha perso gran parte delle sue caratteristiche originarie "trasformandosi da luogo di sperimentazione a luogo della speculazione, da laboratorio globale a vero e proprio mercato globale".

[xvii] O. POLLICINO, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli Internet service provider*, in *Consulta Online,* 2014,mette in evidenza che la disciplina recata dalla direttiva del 2000 ha evidenziato i suoi limiti nel momento in cui la dimensione partecipativa della rete si è sempre più estesa, al punto da mettere in discussione la tenuta dell'inquadramento degli internet service provider così come previsto nella direttiva e- commerce. L'A. osserva che la rete, nella sua dimensione attuale, sfuma i confini tra produzione di contenuti e prestazioni di servizi e ciò conduce a interrogarsi sulla presunta estraneità degli ISP rispetto ai contenuti ospitati, su

cui si basa principalmente la disciplina europea. F. DONATI, *Verso una nuova regolazione delle piattaforme digitali*, in *Rivista della Regolazione dei mercati*, n. 2/2021, 238 ss., osserva che la crescente rilevanza assunta dalle piattaforme online le identifica come grandi centri di potere che esercitano una crescente influenza su aspetti importanti della vita di milioni di persone. Ciò impone, pertanto, una regolazione chiara e precisa e che faccia fronte ai rischi a cui gli utenti vengono esposti. A. PIROZZOLI, *La responsabilità dell'internet service provider. il nuovo orientamento giurisprudenziale nell'ultimo caso Google*, in *Rivista AIC*, n. 3/2012, 7, sostiene che la disciplina recata dalla direttiva sia incompleta e impreca, specie laddove l'intenzione del legislatore sia quella di sottrarre agli hosting provider una responsabilità troppo gravosa che avrebbe potuto provocare sgradite conseguenze sulle scelte economiche e sugli investimenti dei gestori di servizi, oltre che indirizzarli verso un'indiscriminata selezione di contenuti all'ombra del timore che potessero rivelarsi lesivi dei diritti degli utenti. Nei medesimi termini v. anche G. D'ALSONSO, *Verso una maggiore responsabilizzazione dell'hosting provider tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo,* in *Federalismi.it,* n. 2/2020, 115 ss., il quale rileva che "la disciplina europea si caratterizza per l'assenza di chiarezza di certe regole, derivante dalla necessità di contemperare interessi contrapposti, quali: da un lato, la salvaguardia dell'indipendenza della rete, comunemente definita come «*marketplace of ideas*» – dal momento che, caratterizzandosi per l'assenza di limiti, l'immediatezza e l'economicità, assurge a luogo quanto più libero di circolazione di idee ed informazioni-, e dunque la libertà di espressione e la protezione della *privacy* dei cibernauti; dall'altro lato, l'interesse a non rinunciare del tutto al controllo sui contenuti pubblicati sulle piattaforme digitali e a proteggere i soggetti che potrebbero essere danneggiati da contenuti illeciti". Lo stesso mette in dubbio, inoltre, la circostanza entro la quale un hosting provider sia effettivamente al corrente di un fatto illecito, verificatosi nello spazio che intermedia.

[xviii] La stessa Commissione europea, ad esempio, già a partire dalla COM (2017) 555 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online" stabiliva una serie di orientamenti e principi affinché le piattaforme online intensifichino la lotta contro i contenuti illegali online in cooperazione con le autorità nazionali, gli Stati membri e i portatori d'interessi pertinenti. Su questi presupposti, la commissione sollecitava l'attuazione di buone pratiche per prevenire, individuare, rimuovere e disabilitare l'accesso a contenuti illegali al fine di garantire l'efficace rimozione di contenuti illegali, una maggiore trasparenza e la tutela dei diritti fondamentali online. In altri termini, tale misura sollecitava l'azione di misure proattive volte a individuare,

rimuovere o disabilitare l'accesso a contenuti illegali.

[xix] Tale Regolamento fa parte, assieme al Digital Market Act (Regolamento (UE) 2022/1925), del Digital Services Package che si pone due principali obiettivi: 1) creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali di tutti gli utenti dei servizi digitali; 2) creare condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel Mercato unico europeo che a livello globale.

[xx] Considerando 3, Regolamento UE 2022/2065.

[xxi] Ad esempio, già con l'adozione del Regolamento 2019/1150/UE, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, l'art. 3, rubricato "Termini e Condizioni" indica in modo puntuale le misure a cui tali soggetti sono tenuti a conformarsi al fine di assicurare trasparenza in ogni fase della contrattazione con gli utenti che si interfacciano nel portale. Ugualmente, il Regolamento UE 2022/2065, al considerando 48 i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi dovrebbero fornire le loro condizioni generali nelle lingue ufficiali di tutti gli Stati membri in cui offrono i loro servizi e dovrebbero altresì fornire ai destinatari dei servizi una sintesi concisa e facilmente leggibile dei principali elementi delle condizioni generali. Tali sintesi dovrebbero individuare gli elementi principali dei requisiti in materia di informazione, compresa la possibilità di derogare facilmente alle clausole opzionali. Nel considerando successivo, si impone ai prestatori di servizi intermediari di rendere pubblica una relazione annuale in un formato leggibile elettronicamente, in merito alla moderazione dei contenuti da loro intrapresa, comprese le misure adottate a seguito dell'applicazione e dell'esecuzione delle loro condizioni generali. Nel considerando 66, invero si statuisce che la Commissione dovrebbe mantenere e pubblicare una banca dati contenente le decisioni e le motivazioni dei fornitori di piattaforme online quando rimuovono le informazioni o limitano in altro modo la loro disponibilità e l'accesso alle stesse.

[xxii] Cfr. Art. 6, Regolamento UE 2022/2065: "I prestatori di servizi intermediari non sono considerati inammissibili all'esenzione dalla responsabilità prevista agli articoli 3, 4 e 5 per il solo fatto di svolgere indagini volontarie o altre attività di propria iniziativa volte ad individuare, identificare e rimuovere contenuti illegali o a disabilitare l'accesso agli stessi, o di adottare le misure necessarie per conformarsi alle prescrizioni del diritto dell'Unione, comprese quelle stabilite nel presente regolamento".

[xxiii] In Corte di giustizia UE, 12 luglio 2011, C-324/09, L'Orèal c. eBay International, par. 114, la Corte ha precisato che, affinché il prestatore di un servizio su Internet possa rientrare nell'ambito di applicazione dell'art. 14 della direttiva 2000/31, è necessario che egli sia un «prestatore intermediario» nel senso che questo si limita ad una fornitura neutra del servizio, mediante un trattamento puramente tecnico e automatico dei dati forniti dai suoi clienti. Tale impostazione conferisce al prestatore un ruolo passivo tale per cui non è a conoscenza dei dati che ospita. Nei medesimi termini si esprime la corte nella pronuncia Corte di Giustizia UE 23 marzo 2010, da C-236/08 a C-238/08, Google c. Luis Vuitton, par. 114 secondo cui al fine di verificare se la responsabilità del prestatore del servizio di posizionamento possa essere limitata ai sensi dell'art. 14 della direttiva 2000/31, occorre esaminare se il ruolo svolto da detto prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza. Nei medesimi termini v. anche Corte di Giustizia UE, 7 agosto 2018, Cooperatieve Vereniging SNBREACT U.A. c. Deepak Mehta, C-521/17, par. 47; Corte di Giustizia UE, 23 marzo 2010, Google France e Google, da C-236/08 a C-238/08, par. 113 e Corte di Giustizia UE, del 15 settembre 2016, Mc Fadden, C-484/14, par. 62. Nel nostro ordinamento, sulla falsariga di quella europea, si segnala Cass. Civ., Sez. I civ., Ord. 13 dicembre 2021 n. 39763, in cui i giudici hanno accolto la nozione di hosting provider attivo, così come declinata in sede di giustizia europea, riferendola a tutti quei casi che esulano da un'attività di ordine meramente tecnico, automatico e passivo, in cui l'internet service provider (ISP) non conosce, né controlla, le informazioni trasmesse o memorizzate dalle persone alle quali fornisce i suoi servizi, e ha affermato che tali limitazioni di responsabilità non sono applicabili nel caso in cui un prestatore di servizi della società dell'informazione svolge un ruolo attivo. Si può quindi parlare di hosting provider attivo, sottratto al regime privilegiato, quando sia ravvisabile una condotta di azione, nel senso ora richiamato; gli elementi idonei a delineare la figura o indici di interferenza, da accertare in concreto ad opera del giudice del merito, sono le attività di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare e arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati. Così anche Cass. civ., Sez. I, 19 marzo 2019, n. 7708. In sede di giustizia amministrativa, altresì, si segnala la pronuncia del Consiglio di Stato, sez. VI, 13 settembre 2022 n. 7949, che ha aderito a quanto sinora ricostruito, riconoscendo due tipi di hosting provider: a) l'hosting provider "passivo", il quale pone in essere

un'attività di prestazione di servizi di ordine meramente tecnico e automatico, con la conseguenza che detti prestatori non conoscono né controllano le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i loro servizi; b) l'hosting provider "attivo", che si ha quando, tra l'altro, l'attività non è limitata a quanto sopra indicato ma ha ad oggetto anche i contenuti della prestazione resa.

[xxiv] Il regime delle limitazioni della responsabilità è escluso dalla giurisprudenza sulla base del Considerando 42 della Direttiva E-commerce, il quale dispone che "le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate"

[xxv] Vi è chi ha messo in dubbio la natura neutrale degli Internet Service Provider, così come riscostruita dai giudici. In T. SCANNICCHIO, N.A. VECCHIO, *I limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell'*hosting *attivo,* in *MediaLaws*, n.1/2019, 256 ss., si osserva che "la figura dell'hosting c.d. "attivo" è frutto di uno sviluppo giurisprudenziale praeter legem, senza alcun dato positivo che riesca a chiarire i termini del discrimen rispetto al suo omologo "passivo", con il rischio concreto di dar luogo a un'interpretatio abrogans della normativa vigente, essendo (quasi) sempre possibile rinvenire, nell'attuale modello di provider, quel quid pluris che neutralizzerebbe l'esonero di responsabilità".

[xxvi] Vedi nota 23.

[xxvii] Per questioni di completezza va precisato che, al momento in cui si scrive, la sentenza de qua è stata appellata da Agcom e, su impulso di questa, il Consiglio di Stato ha emesso una ordinanza cautelare che sospende l'efficacia della sentenza di primo grado. Cfr. Consiglio di Stato, sez. VI, ord. 23 agosto 2024, n. 1974.

[xxviii] Come si evince nella già citata Corte di Cassazione, 19 Marzo 2019, n. 7708 si può parlare di hosting provider attivo, sottratto al regime privilegiato, quando sia ravvisabile una condotta di azione, che abbia, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati.

[xxix] Cfr. considerando 12, Regolamento (UE) 2024/1689.

[xxx] Su questi argomenti, indagati in una prospettiva tecnica, v. C. D'URSO, *I profili informatici nella valutazione della responsabilità dell'Hosting Provider*, in *Riv. It. Inf. Dir*., n.1/2021, in part. 84 ss. V. anche S. LAVAGNINI, *La responsabilità degli Internet Service Provider e la nuova figura dei prestatori di servizi di condivisione online (art. 17),* in Id (a cura di) *Il diritto d'autore nel mercato unico digitale*, Giappichelli, 2022, 228, che mette in evidenza come i principali *hosting provider* abbiano adottato sistemi tecnologici di riconoscimento dei contenuti (quantomeno quelli di tipo musicale o audiovisivi), definiti come sistemi di c.d. *content id recognition*. Questi strumenti rendono possibile l'identificazione dei contenuti postati dagli utenti, in modo tale che sia possibile per il sistema, ad ogni istanza di ricarica da parte degli utenti stessi, riconoscere il contenuto ed impedirne il successivo ricaricamento. In pratica, i titolari dei diritti forniscono al *provider* o a terzi fornitori dei servizi tecnologici di riconoscimento dei *file* di riferimento delle opere di loro titolarità, i metadati che descrivono il contenuto e l'azione che essi desiderano attuare nel momento in cui il sistema di *Content ID* trova una corrispondenza appropriata. Queste azioni possono essere il blocco del contenuto, che quindi non viene messo a disposizione del pubblico, la sua monetizzazione, che avviene generalmente associando il contenuto ad un contenuto pubblicitario, ovvero il semplice tracciamento statistico (con il quale il contenuto viene mantenuto a disposizione a titolo gratuito, ma raccogliendo i dati relativi alle sue utilizzazioni).

[xxxi] Vedi nota 23.

[xxxii] L'espressione è di G. CORASANITI, *Regolazione, autoregolazione, sovraregolazione della rete: dal "far" web al "fair"web,* op. cit.

[xxxiii] Sulla funzione dei dati v. G D'ACQUISTO, *Qualità dei dati e intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati,* in F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018; V. BERLINGÒ, *Il fenomeno della datafication e la sua giuridicizzazione*, in *Riv. Trim. Dir. Pubbl*., n.3/2017; G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa,* Milano, Giappichelli, 2018; M. FALCONE, *La funzione conoscitiva nella rivoluzione dei dati,* in R. CAVALLO PERIN (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale,* Torino, 2021.

[xxxiv] Del resto, in questi termini, si era espressa anche la Commissione europea nella già richiamata COM (2017) 555 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Lotta ai contenuti

illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online", in cui osservava che le piattaforme online dovrebbero inoltre garantire il continuo aggiornamento dei loro strumenti, al fine di assicurare la individuazione di tutti i contenuti illegali, in linea con le tattiche e il comportamento mutevoli dei criminali e degli altri soggetti coinvolti nelle attività illecite online.

[xxxv] Tar Lazio, sez. III bis,10 settembre 2018 n. 9230; Tar Lazio, sez. III bis, 10-13 settembre 2019, n. 10964; Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270; Consiglio di Stato, sez. VI, del 4 febbraio 2020, n. 881; Tar Campania, sez. III, del 14 novembre 2022, n. 7003.

[xxxvi] Cfr. Regolamento (UE) 2024/1689 e, a titolo esemplificativo, a livello nazionale, il D. lgs. n. 36/2023, Codice dei contratti pubblici, che all'art. 30, c.3, lett. c) rubricato "Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici" cristallizza il principio di non esclusività della decisione algoritmica, per cui nel processo decisionale è necessario un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata.

[xxxvii] M.C. CAVALLARO, *Imputazione e responsabilità delle decisioni automatizzate*, in *Erdal*, n. 1-2/2020,70 ss., secondo cui "spetta quindi all'amministrazione, e in particolare al responsabile del procedimento ovvero all'organo competente all'adozione dell'atto finale, il dovere di verificare l'attendibilità del risultato fornito dal software per scongiurare il rischio di un errore della macchina ed eventualmente correggere la soluzione. Il responsabile del procedimento deve quindi monitorare la procedura automatizzata, per assicurare la trasparenza, la conoscibilità e la partecipazione da parte del privato: al termine della procedura, l'organo competente alla decisione può conformarsi alle risultanze dell'istruttoria che si sostanzia in un algoritmo, e in tal caso ne assumerà la relativa responsabilità".

[xxxviii] Consiglio di Stato, sez. VI, del 4 febbraio 2020, n. 881.

[xxxix] Cfr. Tar Campania, sez. III, del 14 novembre 2022, n. 7003.

[xl] In tal senso sia consentito rinviare a L. TOMASSI, M. INTERLANDI, *La decisione amministrativa algoritmica*, op. cit. In questi termini v. S. CIVITARESE MATTEUCCI, *«Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità*, in *Dir. Pubb.* n.1/2019,22, che enuclea il principio antropomorfico in base al quale il potere decisionale è sempre riferito ad un atto intenzionale umano; R. ROLLI. F. D'AMBORSIO, *La necessaria lettura antropocentrica della rivoluzione 4.0*, in *Pa persona e amministrazione*, n.1/2021, 587 ss., secondo cui non solo "il controllo umano diviene così garanzia del fondamentale principio di «autonomia umana»" ma, ulteriormente, riconosce che l'imputabilità giuridica della decisione e la eventuale

e connessa responsabilità amministrativa devono essere necessariamente attribuiti al titolare del potere decisorio. In tal senso v. anche G. GALLONE, *Riserve di umanità e funzione amministrativa,* op. cit., 65 ss., che pur riconoscendo l'assenza di una formale consacrazione della "riserve di umanità" nello svolgimento delle funzioni amministrative, sostiene sia una prospettiva implicitamente accolta e consacrata all'interno del nostro ordinamento. Tra le varie argomentazioni a sostegno di tale prospettiva l'autore richiama il binomio "imputazione – organo" in base al quale l'attività amministrativa ha sempre coinciso con l'attività umana dal momento che l'ente pubblico esercita le sue funzioni per il tramite un funzionario persona fisica che assume la posizione di organo.

[xli] Cfr. art 22, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. In argomento v. F. PIZZETTI, *Intelligenza artificiale, protezione dei dati e regolazione*, Torino, Giappichelli, 2018.

[xlii] All'interno del considerando 48, Regolamento (UE) 2024/1689, sono considerati ad alto rischio, tutti quei sistemi di Intelligenza artificiale che possono produrre effetti negativi sui diritti fondamentali protetti dalla Carta dei diritti fondamentali dell'Unione europea. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione.

[xliii] Art 14, Regolamento (UE) 2024/1689.

[xliv] Cfr. considerando 27, Regolamento (UE) 2024/1689.

[xlv] Cfr. art 14. c.4, lett. a).

[xlvi] Cfr. art 14. c.4, lett. b).

[xlvii] Cfr. art 14. c.4, lett. c).

[xlviii] Cfr. art 14. c.4, lett. d).

[xlix] Cfr. art 14. c.4, lett. e).

[l] Cfr., ex multis, Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270.

[li] Cfr. Corte di Giustizia Ue, sentenza C-634/21 Schufa Holding, 7 dicembre 2022.

[lii] Cfr. Trib. Ord. Bologna, sez Lavoro, ord. Del 31 dicembre 2020, in cui è stato rilevato che alcuni rider hanno visto penalizzate le loro statistiche indipendentemente dalla giustificazione della loro condotta e ciò per la semplice motivazione, espressamente riconosciuta da Deliveroo, che la piattaforma non conosce e non vuole conoscere i motivi per cui il rider cancella la sua prenotazione, realizzando una discriminazione indiretta che pone "una determinata categoria di lavoratori (in questo caso quelli che prendono parte ad iniziative sindacali di astensione dal lavoro) in una posizione di potenziale svantaggio".

[liii] Cfr. Corte di Cassazione pen., Sez. III, 17 dicembre 2013, n. 5107.

[liv] Sulla esigenza di riforma v. T. SCANNICCHIO, N.A. VECCHIO, *I limiti della neutralità: la Corte di giustizia e l'eterno ritorno dell'*hosting *attivo,* op.cit., 258 ss., in cui si riflette se l'esenzione di tali intermediari, fondata sulla loro asserita "neutralità" – dopo numerose e contraddittorie sentenze in materia - costituisca ancora la soluzione regolatoria ottimale ovvero se sia opportuno prendere atto del suo superamento, modulando di conseguenza anche la relativa disciplina. In questo senso gli autori ribadiscono un ruolo degli Internet service provider assolutamente non neutro, così mai neutre sono anche le scelte di policy: la costruzione normativa compiuta con la direttiva 2000/31, infatti, non rappresentava la constatazione di una realtà tecnologica, bensì l'espressione di un preciso favor per gli ISP, scegliendo di coniugare il generale esonero di responsabilità ex ante con un (minimale) meccanismo di notice-and-take-down, oggi probabilmente meritevole di venire riformato.