Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Daniele Imbruglia nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (https://web.uniroma1.it/deap/ogid - jodi.deap@uniroma1.it).

* Contributo non sottoposto a referaggio ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

1. La "rivoluzione digitale" e lo *European Democracy Action Plan* del 03.12.2020.

Con la comunicazione COM790 (2020) final del 3 dicembre 2020 (la "**Comunicazione**"), la Commissione europea ha presentato il suo "Piano d'azione per la democrazia europea" finalizzato alla fortificazione della democrazia in tutta l'Unione Europea, a fronte di quella che nella Comunicazione viene definita come la "trasformazione digitale delle nostre democrazie" e anche la "rivoluzione digitale". Questo piano costituisce una delle principali iniziative dell'agenda politica del Presidente della Commissione von der Leyen.

Il tema centrale della Comunicazione è quello dei pericoli in cui incorrono le democrazie europee a causa degli abusi del potere mediatico, con la rivoluzione digitale in corso. In particolare, il piano ha il fine di promuovere ulteriormente una società in cui le persone siano messe nelle condizioni di compiere scelte libere ed esprimere le proprie opinioni in un contesto in cui, allo stesso tempo, i canali di comunicazione non diventino strumenti di manipolazione facenti capo a pochi centri di interesse.

Più in dettaglio, nella Comunicazione viene detto che la crescita delle campagne elettorali *online* e le modalità di utilizzo delle piattaforme di comunicazione hanno reso più difficile preservare l'integrità delle elezioni, garantire media liberi e plurali, e proteggere il processo democratico dalla disinformazione e da altre interferenze. Si osserva che la digitalizzazione consente la diffusione di nuovi e non monitorabili metodi di finanziamento ai partiti, i *cyber*-attacchi possono prendere di mira le "infrastrutture elettorali" e le false informazioni possono essere diffuse rapidamente sui social media, anche attraverso campagne di disinformazione coordinate. Si aggiunge che l'impatto di alcuni di questi fenomeni è amplificato dall'uso di algoritmi non trasparenti i quali sono controllati da piattaforme aventi *network* diffusi a livello globale.

In risposta a ciò, il piano d'azione per la democrazia europea individua tre aree di intervento. Esso stabilisce misure per promuovere elezioni libere ed eque, rafforzare il pluralismo dei media e contrastare la disinformazione. Per quanto riguarda il rafforzamento dell'integrità delle elezioni politiche, la Commissione propone di introdurre una legislazione sulla trasparenza dei contenuti politici sponsorizzati e intende rivedere le regole sul finanziamento dei partiti politici europei, mirando a rafforzare la cooperazione tra gli Stati membri. Per difendere il pluralismo mediatico, invece, la Commissione innanzitutto riconosce la necessità di supportare l'intera classe dei giornalisti contro minacce o cause legali pretestuose intentate col mero fine di dissuadere quest'ultimi dal prender parte all'offerta di informazione nell'interesse della collettività. Nella medesima direzione vanno le linee di proposta volte a rafforzare la trasparenza relativa agli assetti proprietari dei media, attraverso un nuovo osservatorio *ad hoc*, e alla pubblicità statale.

Infine, il piano della Commissione comprende la necessità di rivedere il *Code of Practice on Disinformation*, vale a dire il codice di condotta, contenente gli standard regolamentari per combattere la disinformazione, a cui le piattaforme *online*, i principali *social network*, gli inserzionisti e l'industria pubblicitaria possono vincolarsi su base volontaria. La revisione fornirà un quadro di obblighi e responsabilità a carico delle piattaforme digitali, in linea con il *Digital Services Act* (su cui v. *infra* in questa Rubrica sub **3.**). Questi sforzi sono diretti anche a contrastare le crescenti interferenze straniere all'interno dei singoli Stati Membri, rese possibili con l'avvento della rivoluzione digitale, attraverso la costituzione di strumenti per imporre sanzioni ai perpetratori di eventuali attacchi alla democrazia europea.

DOMENICO PIERS DE MARTINO

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423

2. La strategia digitale della Risoluzione del Parlamento Europeo del 25.11.2020 "*Verso un mercato unico più sostenibile per le imprese e i consumatori*"

La Risoluzione del Parlamento Europeo del 25 novembre 2020 sul tema "*Verso un mercato unico più sostenibile per le imprese e i consumatori*" (2020/2021 INI) (la "**Risoluzione**") si inserisce in un quadro di evoluzione della normativa dell'Unione Europea, volto a costruire una rinnovata opzione macroeconomica di sistema che faccia propria la dimensione della sostenibilità, attraverso un insieme di regole e di riconoscimenti di diritti e tutele fondamentali. La Risoluzione dedica un capo alla strategia digitale

confermandone il carattere di infrastruttura del mercato sostenibile.

Nei considerando R e S della Risoluzione si parla delle piattaforme *online* e del tema strategico dell'informazione. L'accesso alle piattaforme e la diffusione delle informazioni possono rappresentare la garanzia non solo per i consumatori, ma anche per costruire un diverso tipo di democrazia, se non diretta, certamente maggiormente partecipata. E le garanzie di cui devono essere dotate le informazioni e i processi connessi alle piattaforme *online* devono tener conto di queste implicazioni. Il considerando T ribadisce la necessità di valutare l'impatto ambientale dell'infrastruttura digitale.

Nel capo della Risoluzione dedicato alla strategia digitale al servizio di un mercato sostenibile, al par. 21, si segnala che l'Unione Europea accoglie con favore l'annuncio di uno spazio comune europeo dei dati per le *applicazioni circolari intelligenti* e vuole sviluppare appunto un *passaporto dei prodotti digitale* per migliorare tracciabilità e accesso alle informazioni sulle condizioni di produzione di un prodotto, la durabilità, la composizione di un prodotto, il riutilizzo, la riparazione e tutta una serie di aspetti che possono riguardare la riparabilità e anche lo smaltimento, eventualmente, del prodotto. In questo quadro, lo spazio europeo dei dati per le applicazioni circolari intelligenti fornirà l'architettura e il sistema di *governance* per stimolare applicazioni e servizi, quali i passaporti dei prodotti, la mappatura delle risorse e l'informazione ai consumatori. Di fatto il par. 21 risponde all'esigenza di creare un sistema di dati che consenta di tracciare e accedere alle informazioni relative alla produzione di un certo prodotto, il che può essere costruito attraverso la tecnologia *Blockchain*. Strettamente correlato a questo tema c'è quello della certificazione, cui il passaporto offre una base documentata.

L'economia circolare, al par. 22, rappresenta una delle linee della trasformazione industriale verso temi centrali della sostenibilità, quali la neutralità climatica e la competitività a lungo termine, sfruttando le tecnologie digitali per quanto riguarda la tracciabilità, la rintracciabilità e la mappatura delle risorse e delle tecnologie verdi. A fronte del significativo impatto ambientale del settore digitale, il par. 23, per quanto concerne la produzione di beni e la fornitura di servizi, invita la Commissione a valutare in che misura un indice di sostenibilità del digitale europeo che sia basato su un'analisi del ciclo di vita dei prodotti possa ottimizzare la produzione e il consumo sostenibili di tecnologie digitali, in quanto è estremamente importante scegliere un adeguato criterio di valutazione. Il par. 24 riguarda la potenziale impronta ambientale dei dati che non siano necessari e cioè applicazioni, o file, video, foto, messaggi di posta elettronica che siano indesiderati e che quindi, avendo una qualunque impronta ambientale causino un eccessivo dispendio energetico. Il par. 25 contempla i sistemi di ricarica universale per ridurre la produzione e ridurre anche i rifiuti e i rifiuti elettronici.

Un ulteriore elemento degno di nota riguarda la digitalizzazione degli appalti, al paragrafo 26.

GIUSEPPINA CAPALDO

https://www.europarl.europa.eu/doceo/document/A-9-2020-0209_IT.pdf

3. Verso il *Digital Services Act*: la Proposta di Regolamento sul "mercato unico dei servizi digitali" del 15.12.2020

La significativa evoluzione del settore digitale si accompagna al delinearsi di un modello di *business* nel quale alcuni operatori assumono un ruolo strategico. Sono in grado, infatti, di indirizzare le scelte dei consumatori e controllare l'accesso e la permanenza sul mercato delle imprese. Partendo da tale consapevolezza, è sempre più avvertita l'esigenza di una regolamentazione, fino ad ora prevalentemente affidata alla direttiva 2000/31/CE sul commercio elettronico e al regolamento (UE) 2019/1150, che promuova equità e trasparenza per gli utenti dei servizi di intermediazione *online*.

In questo scenario si colloca la recente proposta del cd. *Digital Services Act* ossia la *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, COM(2020) 825 final del 15 dicembre 2020.

Si tratta di un provvedimento molto complesso che mira a stabilire regole uniformi per un ambiente *online* sicuro, prevedibile e affidabile, soprattutto dopo le singole iniziative legislative intraprese da alcuni Stati membri, quali, per esempio, il tedesco *Netzwerkdurchsetzungsgesetz* (c.d. *NetzDG*) del 2017 e la francese *Loi contre les contenus haineux sur internet* (c.d. *Loi Avia*) del 2020 (su cui v. il numero 2/2020 di questa Rubrica sub **6.** http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf).

Nelle intenzioni della relativa proposta, il *Digital Services Act* ("**DSA**") è complementare al c.d. *Digital Markets Act* (su cui v. *infra* in questo

numero di questa Rubrica sub **4.**), che si occupa, in modo più specifico, dei comportamenti delle aziende che hanno assunto una rilevanza sistemica come c.d. *gatekeeper*.

Entrambi i provvedimenti si inseriscono nel percorso segnato dallo *Shaping Europe's Digital Future*, con il quale la Commissione europea si è impegnata ad aggiornare le norme che definiscono le responsabilità e gli obblighi dei fornitori di servizi digitali, e in particolare delle piattaforme *online*.

La proposta di Regolamento sul DSA prevede: "a) un quadro per l'esenzione condizionata dalla responsabilità dei prestatori di servizi intermediari; b) norme relative a specifici obblighi in materia di dovere di diligenza adattati a determinate categorie di prestatori di servizi intermediari; c) norme sull'attuazione e sull'esecuzione del presente regolamento, anche per quanto riguarda la cooperazione e il coordinamento tra le autorità competenti." (art. 1, para. 1).

Il DSA si pone in continuità con le scelte di base della direttiva sul commercio elettronico e, in particolare, con quelle relative al principio del mercato interno di cui all'articolo 3 e all'assenza di un obbligo generale di sorveglianza a carico dei prestatori di servizi di intermediazione *ex* art. 15.

È proposta la soppressione, è vero, degli articoli dal 12 al 15 della direttiva sul commercio elettronico, ma, conformemente all'interpretazione della Corte di giustizia dell'Unione, vengono previste disposizioni sulle condizioni in base alle quali i fornitori di servizi di *conduit*, *caching* e di *hosting* sono esentati dalla responsabilità per le informazioni di terzi che trasmettono e memorizzano.

Filo conduttore della nuova regolamentazione, proposta con il DSA, è l'adeguamento degli obblighi di diligenza al tipo e alla natura del servizio di intermediazione interessato. A tal fine, si prevedono obblighi di base applicabili a tutti i fornitori di servizi di intermediazione, ma anche obblighi aggiuntivi per le piattaforme *online*, con specifiche disposizioni per le piattaforme *online* di dimensioni molto grandi (*very large online platforms*). Si delinea una logica proporzionale e cumulativa nell'imposizione di obblighi, che aumentano e si sommano a mano a mano che i fornitori di servizi di intermediazione siano qualificabili come *hosting*, piattaforme *online* o *very large online platforms*.

La sottocategoria delle piattaforme *online* è costituita dai fornitori di servizi di *hosting* che, non solo memorizzano le informazioni fornite dai destinatari del servizio su loro richiesta, ma diffondono anche tali informazioni al pubblico.

Le *very large online platforms* sono quelle che prestano i loro servizi a un numero medio mensile di destinatari attivi nell'Unione pari o superiore a 45 milioni (art. 25).

Il primo livello di obblighi riguarda quelli applicabili a tutti i fornitori di servizi di intermediazione. Si tratta di obblighi di trasparenza e obblighi di coordinamento. Questi ultimi sono volti a favorire comunicazioni dirette ed efficaci con le Autorità degli Stati membri, la Commissione e il "Comitato europeo per i servizi digitali" (in inglese lo *European Board for Digital Services*), di cui è prevista l'istituzione a mezzo dello stesso DSA *ex* art. 47 (il "**Comitato**"). In particolare, i fornitori di servizi di intermediazione devono istituire un "punto di contatto unico" che consenta la comunicazione diretta, per via elettronica, con le autorità degli Stati membri, la Commissione e il Comitato, e rendere pubbliche le informazioni necessarie per identificarlo (art. 10).

I *provider* che non hanno stabilimenti nell'Unione, ma che offrono i propri servizi all'interno della stessa, dovranno, *ex* art. 11, designare un legale rappresentante, dotato di poteri e risorse necessarie per cooperare con le Autorità degli Stati membri, la Commissione e il Comitato. Tale rappresentante sarà responsabile, ai sensi del co. 3 dell'art. 11, in caso di mancato rispetto degli obblighi previsti dal DSA.

Una significativa novità è apportata dagli obblighi di trasparenza imposti a tutti gli intermediari e riguardanti eventuali limitazioni all'uso dei servizi offerti. Tali limitazioni, infatti, devono essere incluse nei termini e nelle condizioni contrattuali. Queste ultime devono, altresì, contenere informazioni su eventuali procedure, misure e strumenti di moderazione dei contenuti (*content moderation*), specificando se questi siano sottoposti ad *algorithmic decision-making* o a *human review*. Alla *content moderation* è dedicata particolare attenzione sia in quanto si impone annualmente, *ex* art. 13, di produrre relazioni chiare, facilmente comprensibili e dettagliate sulle attività di moderazione dei contenuti, sia in quanto si specifica che i fornitori di servizi di intermediazione devono agire in modo diligente, obiettivo e proporzionato nell'applicare e far rispettare le eventuali restrizioni all'uso del loro servizio.

Gli obblighi aumentano poi, proporzionalmente, con le disposizioni aggiuntive riguardanti i prestatori di servizi di *hosting*, comprese le piattaforme *online*. L'obiettivo è armonizzare la normativa relativa alla lotta e alla gestione dei contenuti illegali *online* ed evitare che vengano erroneamente rimossi contenuti legali. A tal fine è previsto che i prestatori di servizi di *hosting*

debbano predisporre meccanismi di facile accesso e uso per consentire a qualsiasi persona o ente di notificare la presenza di contenuti illegali.

La comunicazione di un contenuto illecito deve avvenire in modo sufficientemente preciso e con adeguata motivazione. L'art. 14 prevede, infatti, un minuzioso "Meccanismo di notifica e azione" (*Notice and action mechanisms*) che mira a superare i tanti dubbi interpretativi posti dall'art. 14 della direttiva sul commercio elettronico e affrontati in numerosi casi dalla Corte di Giustizia. Obblighi specifici di motivazione (*statement of reasons*), sono previsti dall'art. 15 per il prestatore di servizi di *hosting* che decida di rimuovere specifiche informazioni fornite dai destinatari del servizio o disabilitare l'accesso alle stesse. In particolare, il fornitore del servizio deve informare il destinatario della sua decisione, delle ragioni della stessa (ragioni che devono consistere nell'indicazione di alcune informazioni minime, elencate nel medesimo art. 15) e dei mezzi disponibili per impugnarla. Emerge la consapevolezza delle possibili conseguenze negative che tali decisioni possano avere per il destinatario, anche per quanto riguarda l'esercizio del suo diritto fondamentale alla libertà di espressione.

Da questo punto di vista, il DSA mira a rappresentare, insieme allo *European Democracy Action Plan* (su cui v. *supra* in questo numero di questa Rubrica sub **1.**), un elemento di svolta nella lotta all'*hate speech* digitale, puntando su obblighi di trasparenza da parte dei *provider* e sulla predisposizione di opportune garanzie procedurali a favore degli utenti.

Nelle sezioni del DSA che seguono si entra nello specifico del differente apparato di obblighi a seconda delle dimensioni delle piattaforme e dell'influenza che possono avere sulle scelte, di mercato e di vita, degli *user*.

Un ulteriore gruppo di disposizioni aggiuntive riguarda le piattaforme *online*, ad esclusione di quelle che sono *micro* o piccole imprese ai sensi dell'Allegato alla Raccomandazione 2003/361/CE. Si tratta di dettagliati obblighi relativi al sistema interno di gestione dei reclami (art. 17), che deve avvenire in modo tempestivo, diligente e obiettivo, assicurando una continua interazione con i reclamanti.

Il sistema previsto mira ad evitare che si abusi della possibilità delle notifiche, nell'ottica di un equilibrio tra i diversi interessi coinvolti. A tal fine, l'attendibilità delle segnalazioni è calibrata sulla provenienza delle stesse, ma anche su eventuali precedenti segnalazioni risultate manifestamente infondate. In tale logica si giustifica che le piattaforme *online* debbano garantire che le notifiche presentate dai c.d. *trusted flaggers*, ossia dai segnalatori attendibili, identificati come tali dal competente "Coordinatore dei servizi digitali" (organo previsto dai considerando n. 73 e ss. e dall'art. 38), siano trattate con priorità.

Al fine di contrastare la vendita di prodotti contraffatti *online* è prevista la cd. Tracciabilità degli operatori commerciali (art. 22). Le 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*" (KYC). Rispetto a tali informazioni, il ruolo delle piattaforme *online* non può essere meramente passivo, in quanto sono tenute a compiere sforzi ragionevoli, ai sensi dell'art. 22, per stabilire se le stesse siano attendibili.

È, altresì, obbligatorio redigere un *transparency reporting* con informazioni aggiuntive rispetto a quelle previsti dall'art. 13 per tutti gli intermediari.

La trasparenza riguarda anche la pubblicità *online* e, pure in questo caso, si applica una logica di imposizione di obblighi crescenti, in proporzione alle dimensioni della piattaforma.

L'*online advertising transparency* è affidata, in prima battuta, ad alcuni obblighi che riguardano tutte le piattaforme e che sono delineati dall'art. 24. Ogni singolo destinatario del messaggio pubblicitario, infatti, deve essere in grado di identificare, in modo chiaro e non ambiguo, e in tempo reale, la natura pubblicitaria delle informazioni visualizzate, la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità, nonché le informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità.

Obblighi supplementari di trasparenza riguardano le piattaforme *online* di dimensioni molto grandi, che, infatti, sono tenute a compilare e rendere disponibile al pubblico, attraverso le interfacce di programmazione delle applicazioni, un registro contenente, come minimo, le informazioni previste dall'art. 30 e poste anche a garanzia di pubblicità destinate ad uno o più gruppi specifici di soggetti.

Gli obblighi aggiuntivi per le piattaforme *online* di dimensioni molto grandi non si limitato a quelli evidenziati con riferimento alla pubblicità, ma ad essi è dedicata tutta la Sezione IV del Capo III del DSA che riguarda i rischi sistemici. In particolare, le piattaforme *online* di dimensioni molto grandi sono tenute, almeno una volta all'anno, ad individuare, analizzare e valutare, *ex* art. 26, eventuali rischi sistemici significativi derivanti dal

funzionamento e dall'uso dei loro servizi nell'Unione, anche sulla base dei valori espressi dalla Carta dei diritti fondamentali dell'Unione europea (la "**Carta**").

Ai sensi dell'art. 26, tali rischi sono riconducibili a tre categorie: "a) la diffusione di contenuti illegali tramite i loro servizi; b)eventuali effetti negativi per l'esercizio dei diritti fondamentali al rispetto della vita privata e familiare e alla libertà di espressione e di informazione, del diritto alla non discriminazione e dei diritti del minore, sanciti rispettivamente dagli articoli 7, 11, 21 e 24 della Carta; c) la manipolazione intenzionale del servizio, anche mediante un uso non autentico o uno sfruttamento automatizzato del servizio, con ripercussioni negative, effettive o prevedibili, sulla tutela della salute pubblica, dei minori, del dibattito civico, o con effetti reali o prevedibili sui processi elettorali e sulla sicurezza pubblica".

L'attività di *risk assessment* è propedeutica all'adozione di misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate agli specifici rischi sistemici individuati. I risultati della valutazione di tali rischi e delle relative misure di mitigazione formano oggetto di una relazione che le *very large online platforms* devono trasmettere al Coordinatore dei servizi digitali del luogo di stabilimento e alla Commissione, in adempimento alle obbligazioni di comunicazione trasparente di cui all'art. 33.

Le piattaforme *online* di dimensioni molto grandi, inoltre, hanno l'obbligo di sottoporsi, a proprie spese e almeno una volta all'anno, ad *audit*, esterni e indipendenti, volti a verificare la conformità della loro condotta agli obblighi previsti.

Ulteriori obblighi sono previsti dall'art. 29 con riferimento ai "sistemi di raccomandazione" (*recommender systems*, definiti nell'art. 2 lett. o), in particolare, l'obbligo di specificare nelle condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati, nonché qualunque opzione messa a disposizione dei destinatari del servizio per consentire loro di modificare o influenzare i parametri principali.

Le piattaforme *online* di dimensioni molto grandi hanno, nei confronti del Coordinatore dei servizi digitali del luogo di stabilimento o della Commissione, obblighi di *disclosure* dei dati necessari per monitorare e valutare la conformità della loro condotta al DSA.

Tra le figure preposte al controllo e al monitoraggio del rispetto del DSA, da parte dell'organizzazione delle piattaforme *online* di grandi dimensioni, i "responsabili di conformità" (*compliance officers*) (art. 32), che possono essere dipendenti delle piattaforme oppure svolgere le loro funzioni sulla base di un contratto con le stesse. In entrambi i casi, però, devono essere adottate le misure necessarie per far sì che i responsabili della conformità possano svolgere i loro compiti in modo indipendente.

La proposta di regolamento in oggetto si pone nel solco dell'orientamento dell'Unione Europea particolarmente fiducioso negli strumenti di autoregolazione. Lo si evince dagli ulteriori obblighi di diligenza previsti dal DSA e relativi all'elaborazione ed allo sviluppo di codici di condotta specifici per la pubblicità *online*. Disposizioni alle quali si aggiungono quelle sui protocolli di crisi per affrontare circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica (art. 34-37).

Le novità in punto di *governance* chiudono il DSA che prevede una o più Autorità competenti designate a garantire l'applicazione del regolamento. Tra queste autorità competenti c'è quella, sopra già menzionata, dei 'Coordinatori dei servizi digitali' (*Digital Services Coordinators*) (considerando 73 ss., art. 38).

Ad arricchire ulteriormente l'apparato burocratico c'è il già menzionato Comitato (lo *European Board for Digital Services*), definito come "gruppo consultivo indipendente di Coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari" (art. 47). Il Comitato fornisce consulenza ai Coordinatori dei servizi digitali e alla Commissione sull'applicazione del Regolamento, assistendoli anche nell'attività di vigilanza sulle piattaforme di grandi dimensioni. Oltre a poteri consultivi, di coordinamento e di assistenza, il Comitato ha il compito di promuovere l'elaborazione e l'attuazione di norme, orientamenti, relazioni, modelli e codici di condotta europei.

Parallelamente ad obblighi più stringenti, è prevista per le piattaforme *online* di dimensioni molto grandi una vigilanza rafforzata che si articola in un procedimento le cui fasi sono dettagliatamente disciplinate, anche al fine di garantire il contraddittorio e l'accesso agli atti. Su raccomandazione del Comitato o di propria iniziativa previa consultazione del Comitato, nel procedimento può intervenire la Commissione che può richiedere informazioni ed ha, altresì, poteri di audizione e di raccogliere dichiarazioni (art. 53) e di effettuare ispezioni *in loco* (art. 54).

Ancora, è previsto che qualora la Commissione accerti che la *very large online platform* non rispetti le disposizioni del Regolamento, o le misure provvisorie ordinate o gli impegni resi vincolanti, adotti la cd. decisione di non conformità (*non-*

compliance decision) (art. 58), sia pure a seguito di contestazioni preliminari motivate e che contengono una spiegazione delle misure che la Commissione intende adottare, o che ritiene che la piattaforma *online* di dimensioni molto grandi dovrebbe adottare. Qualora la Commissione constati che le condizioni da essa richiesta non siano state soddisfatte, l'indagine potrà essere chiusa con una decisione che può prevedere sanzioni pecuniarie non superiori al 6% del fatturato totale realizzato dalla piattaforma nell'esercizio precedente (art. 59).

L'intento è quello di un apparato sanzionatorio effettivo, proporzionato e dissuasivo, che tenga conto della natura, della gravità, della reiterazione e della durata della violazione, secondo una politica ormai costante dell'Unione e affidata prevalentemente ad una sanzione pecuniaria in percentuale del fatturato.

Il percorso verso a *human-centric technological model*, che prescinda anche dai limiti europei e si basi su un approccio globale, è ancora in salita, ma il DSA sarà una tappa importante, quantomeno per l'attenzione ai rischi dei servizi digitali e alla vulnerabilità dei diritti fondamentali degli utenti, che non possono avere un ruolo di secondo piano rispetto alle potenzialità del commercio elettronico ed alla sua portata trainante per il rilancio dell'economia europea.

SARA TOMMASI

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0825&from=en

4. Verso il *Digital Markets Act*: la Proposta di Regolamento su "mercati equi e contendibili nel settore digitale" del 15.12.2020

Il 15 dicembre 2020 la Commissione europea ha pubblicato la *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale* (c.d. *Digital Markets Act* o, nella versione italiana della proposta, "legge sui mercati digitali"), COM(2020) 842 final. La proposta si inserisce nella più ampia strategia digitale dell'Unione Europea (*Shaping Europe's Digital Future)* ed insieme alla proposta sul c.d. *Digital Services Act* (su cui v. *supra* in questa Rubrica sub **3.**) mira a garantire uno spazio virtuale sicuro e a costituire un *level playing field* che favorisca l'innovazione e la competitività nel mercato europeo.

La proposta prevede che il *Digital Markets Act* ("**DMA**") si applichi alle piattaforme digitali che hanno assunto una rilevanza sistemica all'interno del mercato unico digitale ed alle loro attività qualificate come "servizi di piattaforma di base", definiti dall'art. 2, come uno qualunque dei seguenti servizi: "a) servizi di intermediazione *online*; b) motori di ricerca *online*; c) servizi di *social network online*; d) servizi di piattaforma per la condivisione di video; e) servizi di comunicazione interpersonale indipendenti dal numero; f) sistemi operativi; g) servizi di *cloud computing*; h) servizi pubblicitari, compresi reti pubblicitarie, scambi di inserzioni pubblicitarie e qualsiasi altro servizio di intermediazione pubblicitaria, erogati da un fornitore di uno dei servizi di piattaforma di base elencati alle lettere da a) a g)".

La proposta si rivolge, in particolare, ai c.d. *gatekeeper* che offrono servizi di piattaforma di base, ovvero gli operatori che detengono il controllo dell'accesso in specifici settori e si connota per adottare un approccio regolatorio *ex ante*, diverso dal tradizionale controllo *ex post* della disciplina antitrust europea.

Ai sensi dell'art. 3, le piattaforme si qualificano come *gatekeeper* se: *(i)* hanno un impatto significativo sul mercato interno, *(ii)* gestiscono un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) tra gli utenti commerciali e gli utenti finali, e *(iii)* detengono una posizione consolidata e duratura nel proprio settore di mercato (o si prevede che la acquisiranno).

Il primo requisito si presume soddisfatto se l'impresa del fornitore dei servizi di piattaforma di base raggiunge un fatturato annuo nello Spazio Economico Europeo pari o superiore a 6,5 miliardi di euro negli ultimi tre esercizi finanziari, o se la capitalizzazione di mercato media o il valore equo di mercato equivalente dell'impresa cui appartiene era quanto meno pari a 65 miliardi di euro nell'ultimo esercizio finanziario, e se esso fornisce un servizio di piattaforma di base in almeno tre Stati membri.

Il secondo requisito si presume soddisfatto se viene fornito un servizio di piattaforma di base che annovera nell'ultimo esercizio finanziario più di 45 milioni di utenti finali attivi mensilmente, stabiliti o situati nell'Unione, e oltre 10.000 utenti commerciali attivi annualmente stabiliti nell'Unione.

Il terzo requisito consiste nel possedere i primi due requisiti in ciascuno degli ultimi tre esercizi finanziari.

Importante sottolineare che, nella proposta in commento, la competenza a stabilire se nel caso concreto un fornitore dei servizi di piattaforma di base sia qualificabile come *gatekeeper* spetta alla Commissione e che l'art. 3 del DMA fornisce non solo le suddette soglie che valgono come presunzioni di ricorrenza dei predetti requisiti, ma anche criteri qualitativi, nonché altri numerosi criteri di giudizio relativi alla struttura, la composizione e le caratteristiche dei mercati, al fine di guidare la decisione della Commissione. Gli artt. 3 e 4 stabiliscono i doveri di comunicazione alla Commissione cui sono tenuti i fornitori di servizi di piattaforma di base per consentire alla Commissione la sua valutazione, nonché alcune regole per la decisione e il riesame dello *status* di *gatekeeper*.

Il Capo III del DMA (artt. 5 ss.) prevede specifici obblighi, divieti e restrizioni posti in capo ai *gatekeeper* per impedire "pratiche sleali" o "pratiche che limitano la contendibilità", attraverso un quadro normativo parzialmente flessibile: è prevista, infatti, la possibilità per la Commissione di aggiornare la struttura regolatoria a seguito di indagini di mercato.

Più nello specifico, il DMA di cui alla proposta in commento prevede divieti o restrizioni nell'esecuzione di determinate pratiche commerciali e prevede nuovi obblighi per favorire la concorrenza (artt. 6 e 7), oltre all'inserimento di rimedi *ad hoc* che si applicano sulla base di una analisi caso per caso. Tra i limiti imposti, bisogna evidenziare che si fa esplicito divieto di: a) usare i dati degli utenti commerciali al fine di competere con gli stessi; b) impedire agli utenti di accedere a servizi esterni alla piattaforma; c) impedire agli utenti di disinstallare qualsiasi *app* o *software* preinstallato sui propri dispositivi; d) garantire un trattamento più favorevole in termini di posizionamento ai servizi e prodotti offerti dalla piattaforma stessa (c.d. *self preferencing*) o da soggetti terzi appartenenti sempre al *gatekeeper*.

Il processo di verifica ed accertamento della qualifica di *gatekeeper* è seguito da un periodo di sei mesi in cui la piattaforma deve adeguarsi agli obblighi ed ai divieti imposti dal DMA. In caso di mancato adempimento degli obblighi imposti, sono previste sanzioni ed ammende per un importo fino al 10% del fatturato totale della piattaforma digitale (artt. 26 e ss.).

Come si legge nella proposta, l'obiettivo del DMA e dell'intera strategia digitale europea è quello di aumentare la coerenza e la certezza giuridica nell'ambiente delle piattaforme *online*, offrendo un quadro giuridico uniforme che superi i nazionalismi legislativi e che sappia prevenire i comportamenti sleali dei c.d. *gatekeeper*.

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0842&from=en

5. Il parere del 10.02.2021 dello *European Data Protection Advisor* sulla proposta del *Digital Services Act* in particolare sulla pubblicità mirata e i *recommender systems*

Il 10 febbraio 2021 lo *European Data Protection Supervisor* ("**EDPS**") ha espresso il proprio parere in merito alla proposta di Regolamento della Commissione europea relativa al *Digital Services Act* (la "**Proposta**") su cui v. la notizia in questa rubrica *supra* al numero **3.**

L'EDPS constata innanzitutto la necessità di adottare adeguate misure di mitigazione dei rischi presenti nel contesto delle piattaforme *online*, segnalando in particolare i rischi connessi alla pubblicità mirata *online* ed all'impiego dei *recommender systems*.

Sul primo aspetto, l'Autorità giudica la Proposta idonea a garantire trasparenza ed *accountability* degli operatori di tali piattaforme. Ed infatti, l'EDPS osserva che la Proposta prevede (Articoli 24 e 30) che siano fornite al destinatario della pubblicità mirata informazioni circa i "*principali parametri"* usati per individuare i destinatari del messaggio pubblicitario e prescrive altresì che le piattaforme di notevoli dimensioni rendano accessibile al pubblico un repositorio contenente le suddette informazioni. L'EDPS, tuttavia, ritiene opportuno che si renda obbligatorio comunicare *ogni* parametro utilizzato, anziché i soli parametri principali, e che, comunque, la Proposta chiarisca le condizioni minime necessarie affinché l'informazione da fornire sia "*meaningful*", vale a dire idonea a trasmettere conoscenza. Preoccupazione evidente dell'EDPS è garantire che le nuove norme riescano a promuovere la consapevolezza del destinatario dell'informazione circa i rischi della pubblicità mirata (cfr. *EDPS's Guidelines 8/2020 on the targeting of social media users*, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf, 5, 25).

Invece, con il fine di far sì che la pubblicità mirata non dia luogo a forme di discriminazione, l'Autorità suggerisce che l'articolo 30(2)(d) della Proposta, oltre a prescrivere che sia indicato se il

messaggio pubblicitario è indirizzato ad uno o più gruppi *target*, chiarisca altresì quali gruppi sono esclusi e su quali criteri l'esclusione si basa.

Inoltre, secondo l'Autorità, andrebbero considerate salvaguardie ulteriori rispetto alla trasmissione di informazioni agli utenti. Tali misure dovrebbero includere restrizioni circa le categorie di dati che è consentito trattare a fini di pubblicità mirata e spingersi sino a prevedere la graduale messa al bando di quelle forme di pubblicità mirata, che abbiano luogo sulla base del tracciamento delle attività *online* dell'utente.

L'EDPS dedica, inoltre, particolare attenzione alla regolamentazione dei *recommender systems*, trattandosi di una tecnologia responsabile del preoccupante fenomeno noto come '*filter bubble*'. L'Autorità sottolinea che tali sistemi non si limitano a raccomandare contenuti (commerciali e non), ma più esattamente 'curano' i contenuti forniti agli utenti e dunque sono in grado di limitare la capacità di questi ultimi di ricercare ed interagire con le informazioni nell'ambiente *online*. Inoltre, tale attività è spesso svolta sulla base della profilazione degli utenti, con tutti i conseguenti rischi (segnalati dalla stessa *EDPS*, "Opinion 3/2018 *EDPS Opinion on online manipulation and personal data*", 19 March 2018, p. 9, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf).

Pertanto, in ossequio ai principi di protezione dei dati personali *by design* e *by default*, nonché del principio di minimizzazione, l'EDPS auspica che sia prescritta come impostazione *by default* che l'algoritmo di raccomandazione non si basi su dati di profilazione e che sia richiesto un esplicito *opting in* (anziché un *opting out*) dell'utente, al fine di rendere lecito un simile tipo di trattamento.

Inoltre, si raccomandano misure aggiuntive rispetto a quanto previsto dall'art. 29 della Proposta, atte a promuovere la trasparenza ed il controllo degli utenti in relazione ai sistemi di raccomandazione, tra cui: *i)* indicare chiaramente che la piattaforma utilizza un sistema di raccomandazione; *ii)* informare l'utente della piattaforma se il sistema di raccomandazione è un sistema decisionale automatizzato e, in tal caso, l'identità della persona fisica o giuridica responsabile della decisione; *iii)* consentire agli interessati di visualizzare il profilo od i profili relativi, utilizzati per curare il contenuto della piattaforma per il destinatario del servizio, nonché consentire a questi la cancellazione del o dei profili; *iv)* permettere ai destinatari del servizio di personalizzare i sistemi di raccomandazione sulla base di una serie di criteri (tempo, argomenti di interesse, etc.).

L'effettività di simili misure dipende dall'acquisita capacità dell'utente di conoscere la logica applicata da tali sistemi, nonché di comprenderne le implicazioni. In tale ottica, secondo l'EDPS, non può dirsi adeguata la diposizione, contenuta nell'Articolo 29 (1) della Proposta, con cui è resa obbligatoria la descrizione dei principali parametri impiegati dai *recommender systems*, da rendersi inserendo tale informazione all'interno dei termini e condizioni di servizio della piattaforma *online*.

L'EDPS accoglie con favore il fatto che la proposta si muova nel segno della integrazione della adottanda disciplina con le tutele di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE. In considerazione della incidenza degli aspetti da regolare sul trattamento dei dati personali, l'EDPS reputa necessario garantire la complementarità nella vigilanza e nel controllo delle piattaforme *online*, dando seguito all'esperienza e sviluppi relativi alla c.d. *Digital Clearinghouse* (cfr. *Opinion on coherent enforcement of fundamental rights in the age of Big Data*, 23 September 2016, https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en). A tal fine, tuttavia, l'EDPS stima opportuno che la Proposta preveda una base giuridica esplicita e completa per la cooperazione e lo scambio di informazioni pertinenti tra le diverse autorità di vigilanza.

ROBERTA MONTINARO

https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

6. La Risoluzione del 21.01.2021 del Parlamento europeo sul diritto dei lavoratori alla disconnessione

Il 21 gennaio 2021 è stata approvata la Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione sul diritto alla disconnessione (2019/2181(INL)), formalizzate in una proposta di direttiva (la "**Risoluzione**"). L'approvazione rappresenta il primo tentativo di definire a livello eurounitario il diritto alla disconnessione, inteso come diritto fondamentale dei lavoratori, da esercitare al di fuori dell'orario di lavoro senza incorrere in misure sfavorevoli da parte dei datori di lavoro.

La Risoluzione rientra nel quadro normativo già delineato da numerosi interventi europei in tema di salute e sicurezza sul lavoro. Ma il tema della

disconnessione rappresenta una novità ed è strettamente connesso al fenomeno della digitalizzazione. Nella Risoluzione è espressa la consapevolezza che l'utilizzo sempre maggiore degli strumenti digitali a scopi lavorativi ha comportato la nascita di una cultura del "sempre connessi" che influisce negativamente sull'equilibrio tra vita professionale e vita privata dei lavoratori. Così, se da una parte l'utilizzo di strumenti digitali è stato determinante per tutelare posti di lavoro durante il confinamento per ragioni sanitarie, dall'altra gli orari di lavoro prolungati e le maggiori sollecitazioni sui lavoratori "da remoto" hanno fatto crescere i casi di ansia, *burnout* e altri disturbi psicofisici.

È quanto emerso dalle ricerche condotte da Eurofound (*European Foundation for the Improvement of Living and Working Conditions*), da cui prende le mosse la Risoluzione, secondo cui chi lavora da casa ha più del doppio delle probabilità di lavorare oltre le 48 ore settimanali massime previste rispetto a chi lavora in ufficio e quasi il 30% dei telelavoratori dichiara di lavorare nel proprio tempo libero, a fronte del 5% di coloro che lavorano in ufficio.

Analizzando più da vicino alcuni punti fondanti della Risoluzione, si segnala, ai sensi dell'art. 2, la definizione di "disconnessione" come "il mancato esercizio di attività o comunicazioni lavorative per mezzo di strumenti digitali, direttamente o indirettamente, al di fuori dell'orario di lavoro" e, come meglio specificato dal considerando 10, come "il diritto dei lavoratori di non svolgere mansioni o comunicazioni lavorative al di fuori dell'orario di lavoro per mezzo di strumenti digitali, come telefonate, email o altri messaggi". Al fine di darne effettiva attuazione, la Risoluzione pone in capo agli Stati membri l'obbligo di stabilire, previa consultazione delle parti sociali, modalità dettagliate per consentire l'esercizio del diritto alla disconnessione, tra cui modalità pratiche per scollegarsi dagli strumenti digitali a scopi lavorativi, compreso qualsiasi strumento di monitoraggio legato al lavoro (art. 4, co. 1, lett. a). Tra queste modalità di attuazione assume un rilievo centrale il sistema di misurazione dell'orario di lavoro (art. 4, co. 1, lett. b). Gli Stati membri dovranno, inoltre, assicurare che tale diritto sia effettivo, nel senso di garantire la tutela del lavoratore da qualsiasi tipo di trattamento sfavorevole da parte del datore di lavoro per non aver risposto a richieste lavorative al di fuori dell'orario lavorativo (art. 5), prevedendo un apposito regime sanzionatorio in caso di violazione delle disposizioni in materia (art. 8).

https://www.europarl.europa.eu/doceo/document/TA-9-2021-0021_IT.pdf

7. Regolamento P2B e nuove funzioni delle Autorità indipendenti alla luce della Legge di Bilancio 2021

La Legge di Bilancio 2021 (l. 30 dicembre 2020, n. 178, in vigore dal 1° gennaio 2021) contiene all'art. 1, commi 515-517, alcuni specifici riferimenti al "Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione *online*" (il "**Regolamento**").

Il Regolamento, che dal 12 luglio 2020 trova applicazione in tutta l'Unione europea, è diretto a disciplinare i rapporti *Platform-to-Business* ("**P2B**"), ovvero tra le imprese e, in senso ampio, le piattaforme digitali, in ciò rappresentando una significativa novità nel panorama normativo europeo in quanto, per la prima volta, si rivolge non ai consumatori, ma alle imprese quali nuovi soggetti deboli del mercato nel contesto della *platform economy*.

In primo luogo, il comma 515 modifica la l. 31 luglio 1997, n. 249, istitutiva dell'Autorità per le garanzie nelle comunicazioni ("**AGCOM**"), intervenendo sulle funzioni da essa attribuite a due degli organi collegiali dell'AGCOM: la Commissione per le infrastrutture e le reti, costituita dal Presidente e da due commissari; e il Consiglio, di cui fanno parte il Presidente e tutti i commissari. Rispetto alla Commissione, il riferimento è alla tenuta del Registro degli operatori di comunicazione (ROC), al cui interno è adesso altresì previsto che si iscrivano «i fornitori di servizi di intermediazione *on line* e i motori di ricerca *on line*, anche se non stabiliti, che offrono servizi in Italia» (art. 1, comma 6, lett. a), n. 5). Al Consiglio si attribuisce invece *ex novo* il compito di garantire l'adeguata ed efficace applicazione del Regolamento, «anche mediante l'adozione di linee guida, la promozione di codici di condotta e la raccolta di informazioni pertinenti» (art. 1, comma 6, lett. c), n. 14-bis). Peraltro, proprio l'adozione di codici di condotta è fortemente incoraggiata già dal legislatore europeo, soprattutto in relazione alla corretta applicazione dell'art. 5 del Regolamento in materia di *ranking*. La medesima disposizione estende inoltre la portata del successivo comma 31 dell'art. 1 della l. 249/1997, ove, anche per l'inottemperanza a quei provvedimenti che l'AGCOM abbia adottato a

fronte della violazione delle norme del Regolamento, si prevede una sanzione amministrativa pecuniaria compresa tra il 2 e il 5 per cento del fatturato realizzato dal soggetto destinatario della contestazione nell'ultimo esercizio chiuso prima della sua notificazione.

A norma del comma 516, ai sensi del quale «[r]esta fermo quanto previsto dall'art. 27, comma 1-bis, del codice del consumo» (d. lgs. 6 settembre 2005, n. 206), appare poi volersi riconoscere all'Autorità garante della concorrenza e del mercato ("**AGCM**") la competenza a procedere, anche nell'ambito dei rapporti disciplinati dal Regolamento, nei confronti di condotte integranti pratiche commerciali scorrette.

Il comma 517 si riferisce infine alla copertura dei costi amministrativi sostenuti dall'AGCOM per l'esercizio delle sue funzioni e rinvia pertanto alla l. 23 dicembre 2005, n. 266, al cui art. 1 viene aggiunto il nuovo comma 66-bis. La nuova disposizione impone a carico dei fornitori di servizi di intermediazione e di motori di ricerca *online*, per l'anno 2021, una contribuzione pari all'1,5 per mille dei ricavi relativi al valore della produzione e realizzati nel territorio nazionale, a prescindere da dove vengano concretamente contabilizzati. Per gli anni successivi, competerà invece direttamente all'AGCOM l'individuazione di eventuali variazioni di tale rapporto, per quanto entro il valore massimo del 2 per mille di tali ricavi.

FEDERICO RUGGERI

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-12-30&atto.codiceRedazionale=20G00202&elenco30giorni=false

8. Clearview AI condannata in Germania per violazione del GDPR: il caso Marx

Il 27 gennaio 2021 l'autorità per la protezione dei dati personali della città di Amburgo (l'"**Autorità**") ha ordinato alla società statunitense Clearview AI di cancellare i dati biometrici relativi ad un cittadino tedesco, Matthias Marx, acquisiti senza il consenso di quest'ultimo. La pronuncia è intervenuta in seguito al reclamo presentato dal Sig. Marx dopo che quest'ultimo aveva scoperto, esercitando il proprio diritto di accesso ex art. 13 GDPR, che Clearview AI deteneva a sua insaputa dati personali a lui relativi. Clearview AI è una società statunitense che acquisisce foto e video liberamente disponibili sul web (ad esempio da social *network* e *blog*) all'insaputa dei soggetti interessati e, attraverso un sistema di intelligenza artificiale, estrae i profili biometrici delle persone raffigurate che vengono poi conservati all'interno di un database. Tale tecnologia permette di associare rapidamente il volto di qualunque persona a milioni di immagini, riuscendo così a ricostruirne l'identità. In particolare, le forze dell'ordine statunitensi si avvolgono di tale sistema per poter identificare persone di interesse di cui non si hanno sufficienti informazioni.

Clearview AI si è difesa sostenendo di non essere soggetta agli obblighi imposti dal GDPR essendo una società con sede negli Stati Uniti e priva di uno stabilimento all'interno dell'UE. L'Autorità, tuttavia, ha rigettato tale opposizione sulla base del fatto che il Regolamento, ai sensi dell'art. 3(2)(b), si applica a tutti i trattamenti di dati personali relativi a soggetti che si trovano nell'Unione, indipendentemente dal luogo della sede del titolare del trattamento, quando il trattamento consiste nel monitoraggio del comportamento degli interessati. Nel caso in esame, l'Autorità ha precisato che il trattamento svolto da Clearview AI costituisce un monitoraggio in quanto è finalizzato ad identificare le persone attraverso la loro profilazione.

Alla luce di ciò, l'Autorità ha riconosciuto che Clearview AI è soggetta all'obbligo di individuare una valida base giuridica per il trattamento dei dati personali tra quelle di cui agli art. 6 o 9 GDPR. Nello specifico, essendo i dati biometrici inclusi tra le categorie particolari di dati personali, il trattamento deve essere fondato su una delle basi individuate dall'art. 9 GDPR. Nel caso concreto, la base giuridica più idonea è stata individuata dall'Autorità nel consenso dell'interessato che, tuttavia, non è stato acquisito da Clearview AI. Pertanto, il trattamento risulta invalido e, sulla base dell'art. 17 GDPR che riconosce il diritto alla cancellazione, l'Autorità ha ordinato al titolare di cancellare i dati biometrici relativi al Sig. Marx.

Tale decisone risulta tuttavia limitata sotto due profili. In primo luogo, l'Autorità ha disposto la cancellazione solo per i dati relativi al Sig. Marx, con la conseguenza che altri cittadini europei le cui foto siano state inserite (senza il loro consenso) nel database di Clearview AI, dovranno personalmente presentare una apposita richiesta di cancellazione al titolare del trattamento e, eventualmente, un reclamo all'autorità per la protezione dei dati personali del loro Stato di residenza. In secondo luogo, l'Autorità ha ordinato solamente la cancellazione degli *hash*, ovvero i codici numerici che permettono di estrarre da una fotografia i dati biometrici delle persone raffigurate e di creare un

profilo biometrico. Al contrario, non è stata disposta l'eliminazione delle singole foto.

CHIARA RAUCCIO

https://noyb.eu/sites/default/files/2021-01/545_2020_Anhörung_CVAI_ENG_Redacted.PDF

9. Apple condannata dal Tribunale di Milano a fornire accesso al patrimonio digitale di un defunto (ordinanza del 09.02.2021)

Con un provvedimento emesso in data 9 febbraio 2021, il Tribunale di Milano, Prima Sezione Civile, si è pronunciato in materia di accesso al patrimonio digitale di un defunto.

Per la prima volta in Italia, a quanto consta, un giudice ha ordinato in via cautelare d'urgenza ad una società del gruppo Apple (la Apple S.r.l., di seguito "**Apple**") di fornire la propria assistenza ai genitori di un ragazzo deceduto al fine di consentire il recupero dei dati dell'*account i-cloud* del figlio. Nel caso di specie, il ragazzo era deceduto in un incidente stradale e l'assistenza di Apple risultava necessaria in quanto il suo *smartphone* era andato distrutto nell'incidente.

Leggendo la motivazione del provvedimento (l'"**Ordinanza**") si apprende che, alla richiesta dei genitori di accedere alle credenziali dell'*account* del figlio, Apple aveva risposto affermando che avrebbe consentito loro l'accesso ai dati contenuti dell'ID Apple solo a fronte di un ordine di un Tribunale avente determinati contenuti, alcuni dei quali peraltro anche estranei all'ordinamento giuridico italiano (poiché facenti riferimento a quello americano).

Il 14.12.2020 i genitori proponevano pertanto ricorso *ex* artt. 669-*bis* e 700 c.p.c. al Tribunale di Milano chiedendo, in via cautelare, di emettere, con decreto *inaudita altera parte*, o con ordinanza, previa audizione delle parti, i provvedimenti necessari ed idonei a tutelare i diritti dei ricorrenti e, segnatamente, chiedendo di ordinare alla Apple di fornire assistenza nel recupero dei dati personali dagli *account* del figlio defunto.

Apple non si costituiva in giudizio e rimaneva pertanto contumace.

A fondamento della domanda cautelare, i genitori affermavano, da una parte, il *fumus*, ravvisabile nella ricorrenza *prima facie* dei requisiti di applicabilità della norma di cui all'articolo 2-*terdecies* del nuovo Codice in materia di dati personali (il "**Codice privacy**"), dall'altra, il *periculum*, consistente nel fatto che la società di Cupertino aveva comunicato ai genitori che i propri sistemi, dopo un periodo di inattività dell'*account i-cloud*, avrebbero automaticamente distrutto i dati dello stesso *account*.

La norma di cui all'articolo 2-*terdecies* co. 1 del Codice Privacy dispone che i diritti relativi ai dati personali delle persone decedute possono essere esercitati "da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione". Pertanto, volendo i genitori accedere ai dati del figlio contenuti nel *cloud* al fine di "poter cercare di colmare – almeno in parte – quel senso di vuoto e l'immenso dolore che si accompagna alla prematura perdita di un proprio caro", il Tribunale riteneva che questo caso integrasse pienamente l'ipotesi delle "ragioni familiari meritevoli di protezione" richieste dalla norma e, ricorrendo inoltre il requisito del *periculum* per la ragione rappresentata dai ricorrenti, giudicava fondato il ricorso ed emetteva l'ordine richiesto dai ricorrenti.

La pronuncia risulta particolarmente interessante posto che il GDPR (reg. UE n. 2016/679) non contiene disposizioni in materia, ed anzi il Considerando 27 del GDPR dispone espressamente che il medesimo regolamento "non si applica ai dati personali delle persone decedute", aggiungendo subito dopo che "[g]li Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute".

Viceversa, l'art. 2-*terdecies* del Codice privacy, introdotto con il decreto legislativo 10 agosto 2018, n. 101 e rubricato "Diritti riguardanti le persone decedute", contiene, come sopra ricordato, una nuova disposizione specificamente dedicata al tema della tutela *post-mortem* e dell'accesso ai dati personali del defunto, che, al comma 1, così reca: "I diritti di cui agli articoli da 15 a 22 del Regolamento [GDPR] riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione".

Nell'Ordinanza, il Tribunale di Milano osserva che, come già per la previgente disciplina, il legislatore italiano non chiarisce qui se si tratti di un acquisto *mortis causa* o di una legittimazione *iure proprio*, "limitandosi a prevedere quello che la più attenta dottrina ha qualificato in termini di 'persistenza' dei diritti oltre la vita della persona fisica (diritti che prevedono il diritto di accesso, di rettifica, di limitazione di trattamento, di opposizione, ma anche il diritto alla cancellazione ed alla portabilità dei dati), persistenza che assume rilievo preminente a livello dei rimedi esperibili".

Da qui la ricostruzione per la quale i diritti dell'interessato "sopravvivono" alla sua morte ed essi possono essere esercitati da determinati soggetti "legittimati". Dopo una digressione sul contenuto dei successivi commi del medesimo art. 2-*terdecies* del Codice privacy (non rilevanti per la decisione del caso), il Tribunale ha affrontato la questione dei "requisiti" di contenuto, che, ai termini delle condizioni generali del contratto di servizio predisposte da Apple, un ipotetico ordine del tribunale dovrebbe presentare per consentire ad Apple di fornire l'assistenza e l'accesso ai dati. In particolare, nelle comunicazioni inviate da Apple ai genitori del ragazzo defunto si richiedeva: "un ordine del tribunale che specifichi: 1) che il defunto era il proprietario di tutti gli *account* associati all'ID Apple; 2) che il richiedente è l'amministratore o il rappresentante legale del patrimonio del defunto; 3) che, in qualità di amministratore o rappresentante legale, il richiedente agisce come 'agente' del defunto e la sua autorizzazione costituisce un 'consenso legittimo', secondo le definizioni date nell'Electronic Communications Privacy Act; 4) che il tribunale ordina a Apple di fornire assistenza nel recupero dei dati personali dagli *account* del defunto, che potrebbero contenere anche informazioni o dati personali identificabili di terzi". Con riferimento a tali richieste il Tribunale di Milano, nell'Ordinanza osservava quanto segue: "solo Apple è a conoscenza delle informazioni relative al punto 1); nell'ordinamento italiano non esiste la figura dell' 'amministratore o rappresentante legale del patrimonio del defunto' né, tantomeno, quello di 'agente' del *de cuius*; la disciplina legislativa italiana non richiede, in alcun modo, né l'autorizzazione di un 'agente' del defunto all'accesso né la presenza di un 'consenso legittimo' secondo un atto normativo di un ordinamento giuridico diverso".

Sulla base di queste osservazioni, il Tribunale di Milano ha definito "del tutto illegittima la pretesa avanzata dalla società resistente di subordinare l'esercizio di un diritto, riconosciuto dall'ordinamento giuridico italiano, alla previsione di requisiti del tutto estranei alle norme di legge che disciplinano la fattispecie in esame".

Infine, e "solo per completezza", il Tribunale di Milano ha osservato che, relativamente alla questione dell'applicabilità del GDPR a tutela della posizione di Apple che aveva motivato la sua resistenza invocando la "sicurezza dei clienti", viene in evidenza l'art. 6, par. 1, lettera f) del medesimo regolamento, che autorizza il trattamento dei dati personali necessario per il "perseguimento del legittimo interesse" del titolare o di terzi. Pertanto, avendo preso atto che i ricorrenti avevano chiesto di accedere agli *account* personali del defunto figlio per "ragioni familiari meritevoli di protezione", il Tribunale ha stabilito che dovesse ritenersi sussistente il predetto legittimo interesse anche ai fini dell'applicazione dell'art. 6, par. 1, lettera f) del GDPR.

CORRADO MORICONI

https://web.uniroma1.it/deap/sites/default/files/allegati/Trib_Milano_Apple_eredita_digitale_9_feb_2021.pdf