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 risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale.

Il dibattito europeo in materia di intelligenza artificiale (IA) prosegue nell'ambito dei lavori del Parlamento europeo, ed è da ultimo confluito in una risoluzione adottata dall'organo democratico rappresentativo dell'Unione lo scorso 20 ottobre 2020.

In attesa di una proposta legislativa da parte della Commissione europea che regolamenti il settore in maniera uniforme per tutti gli Stati membri (prevista per l'anno venturo), il Parlamento europeo ha pubblicato una risoluzione (la Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), qui di seguito la "**Risoluzione**"), contenente una serie di raccomandazioni e indicazioni finalizzate ad indirizzare la futura disciplina della responsabilità civile applicabile al funzionamento dei sistemi di intelligenza artificiale e una proposta di regolamento.

La Risoluzione ricalca letteralmente, con alcune modifiche, il *Draft Report* in argomento discusso qualche mese fa nella Commissione JURI, ossia il Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)) del 27 aprile 2020, discusso dalla Commissione giuridica (JURI) del Parlamento europeo nella riunione del 12 maggio 2020 (il "***Draft Report***"), già illustrato su questa rubrica nel secondo numero del 2020, nella notizia n. 3: http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf.

I principi e gli obiettivi che permeano la Risoluzione rispondono all'avvertita esigenza di garantire da una parte la massima certezza giuridica del sistema di responsabilità di tutti i soggetti coinvolti, e dall'altra di evitare un eccesso di regolamentazione che sfoci in oneri burocratici che possano intralciare l'innovazione e il progresso di tecnologie, prodotti e servizi sviluppati da PMI o start-up.

Il giusto equilibrio tra protezione dei cittadini e incentivi alle imprese a investire nell'innovazione è lo scopo dichiarato per le nuove norme della responsabilità civile per l'IA proposte dal Parlamento europeo in questo documento, dove viene affermata anche la necessità di una piena armonizzazione che solo una fonte legislativa direttamente applicabile come il regolamento potrà garantire.

Tutte le scelte di fondo già presenti nel *Draft Report* vengono confermate nella Risoluzione, dove tuttavia vengono offerte nuove definizioni (tra cui quelle di "sistema di IA", di "autonomo" e di "alto rischio"), si introduce una distinzione tra operatore di "front-end" e operatore di "back-end", con le relative definizioni e una diversificazione di regime di responsabilità, si prevede la risarcibilità del "*danno non patrimoniale rilevante, risultante in una perdita economica verificabile*" e si riducono sensibilmente i limiti massimi degli importi dei risarcimenti.

Di conseguenza, i punti salienti della proposta di regolamento presentata nella Risoluzione (la "**Proposta di Regolamento**"), sono i seguenti:

- La Proposta di Regolamento è limitata nel suo oggetto (art. 1) alla "responsabilità civile" dei soli operatori di sistemi di IA (offrendo nell'art. 3 una definizione sia di "operatore" che di "sistemi di IA"), e dunque non riguarda la responsabilità dei produttori o di altri soggetti, per la quale la Risoluzione suggerisce una revisione della direttiva sulla responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE), ed inoltre "fa salve le eventuali ulteriori azioni per responsabilità derivanti da rapporti contrattuali nonché da normative in materia di responsabilità per danno da prodotti difettosi, protezione del consumatore, anti-discriminazione, lavoro e tutela ambientale tra l'operatore e la persona fisica o giuridica vittima di un danno o pregiudizio a causa del sistema di IA, e per il quale può essere presentato ricorso contro l'operatore a norma del diritto dell'Unione o nazionale" (art. 2 co. 3).
- Relativamente alle tipologie di danni o pregiudizi rilevanti, la responsabilità civile degli operatori di sistemi di IA di cui si occupa la Proposta di Regolamento è definita come la responsabilità derivante da "un'attività, dispositivo o processo virtuale o fisico guidato da un sistema di IA" che abbia arrecato un "danno o un pregiudizio alla vita, alla salute, all'integrità fisica di una persona fisica, al patrimonio di una persona fisica o giuridica o […] un danno non patrimoniale rilevante risultante in una perdita economica verificabile" (art. 2 co. 1).

- La Proposta di Regolamento distingue tra "sistemi di IA ad alto rischio" (come definiti all'art. 3 ed elencati tipologicamente in via tassativa nell'allegato alla Proposta di Regolamento unitamente ai "settori fondamentali" nei quali essi vengono impiegati, e con attribuzione alla Commissione europea del potere di modificare l'elenco) ed "altri sistemi di IA", ed istituisce due regimi di responsabilità diversi nei due ambiti (artt. 4-7 e 8-9).
- In particolare, la Proposta di Regolamento prevede per gli operatori di sistemi di IA "ad alto rischio" un regime di "responsabilità oggettiva" (tale per cui la responsabilità è esclusa solo nel caso di "forza maggiore") un obbligo di copertura assicurativa (art. 4), termini di prescrizione del diritto al risarcimento dei danni tra i 10 anni e i 30 anni (art. 7), ed importi massimi per il risarcimento dei danni, in misura sensibilmente inferiore rispetto a quelli indicati nel precedente *Draft Report*, ossia due milioni di euro (in luogo dei dieci milioni di euro previsti dal *Draft Report*) per il caso di morte, o danni alla salute o all'integrità fisica, e un milione di euro (in luogo dei due milioni di euro previsti dal *Draft Report*) in caso di danni al patrimonio o "danni non patrimoniali rilevanti che risultino in una perdita economica verificabile", con la specificazione che tali limiti massimi si applicano anche nel caso di danni patiti da più persone, che non potranno in quel caso ottenere importi eccedenti in totale i predetti limiti, nel senso che si tratta di limiti massimi non già per il danneggiato bensì per il responsabile o i responsabili in solido (art. 5).
- Per gli operatori degli altri sistemi di IA (ossia per i sistemi di IA non "ad alto rischio") la Proposta di Regolamento prevede un regime di responsabilità "per colpa" comprensivo di alcune regole peculiari sulla prova a discolpa a carico dell'operatore, sul danno provocato da terzi, e sull'obbligo di "cooperazione" del produttore del sistema IA nell'accertamento delle responsabilità (art. 8), nonché un rinvio "alle leggi dello Stato membro in cui si è verificato il danno o il pregiudizio" per la disciplina delle questioni relative "ai termini di prescrizione e agli importi ed entità del risarcimento" (art. 9).
- Infine, la Proposta di Regolamento, prevede alcune regole specifiche in tema di concorso di colpa, di responsabilità solidale e di azione di regresso (artt. 10, 11 e 12) senza distinguere per queste regole tra sistemi di IA ad alto rischio ed altri sistemi di IA.
- Quanto al concorso di colpa, la Proposta di Regolamento contempla, tra l'altro, la facoltà dell'operatore e della persona interessata di utilizzare i "dati generati dal sistema di IA" per l'accertamento del concorso di colpa "in conformità del regolamento (UE) 2016/679 [GDPR] e di altre leggi pertinenti in materia di protezione dei dati" (art. 10)
- Quanto alla responsabilità solidale, la Proposta di Regolamento statuisce innanzitutto che "in presenza di più operatori di un sistema di IA, tali soggetti sono responsabili in solido". L'art. 11 aggiunge che se un operatore di front-end è anche il produttore del sistema di IA, le disposizioni del (proposto) regolamento prevalgono su quelle della direttiva sulla responsabilità per danno da prodotti difettosi, mentre se l'operatore di back-end è anche il produttore, ai sensi dell'articolo 3 della direttiva sulla responsabilità per danno da prodotti difettosi, è opportuno che detta direttiva si applichi a tale soggetto. Ed infine si prevede che se vi è un solo operatore e tale operatore è anche il produttore del sistema di IA, le disposizioni del (proposto) regolamento dovrebbero prevalere su quelle della direttiva sulla responsabilità per danno da prodotti difettosi.
- Quanto infine all'azione di regresso, l'art. 12 prevede sia un diritto di regresso tra operatori solidalmente responsabili (stabilendosi, tra l'altro, che le quota interne di responsabilità debbano asseverarsi sulla base dei "rispettivi gradi di controllo che gli operatori hanno esercitato sul rischio connesso all'operatività e al funzionamento del sistema di IA. Se non è possibile ottenere da un operatore responsabile in solido il contributo che gli è attribuibile, tale importo mancante è a carico degli altri operatori") sia un

diritto di regresso dell'operatore nei confronti del produttore di un sistema di IA difettoso (prevedendosi che tale diritto debba esercitarsi conformemente alla direttiva 85/374/CEE e alle disposizioni nazionali che disciplinano la responsabilità per danno da prodotti difettosi).

SARA GARREFFA

https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html

2. La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l'emanazione di un Regolamento Europeo sui Mercati di Cripto-attività.

Il 24 settembre 2020, la Commissione europea ha pubblicato un "pacchetto per la finanza digitale" volto ad incentivare lo sviluppo di un mercato unico digitale innovativo per i finanziamenti. *La ratio* di fondo è che la creazione di tale mercato apporterà "*benefici per i cittadini europei e sarà fondamentale per la ripresa economica dell'Europa, offrendo prodotti finanziari migliori per i consumatori e aprendo nuovi canali di finanziamento per le imprese*". Il pacchetto si presenta ampio e articolato, occupandosi di definire gli orizzonti strategici per la "finanza digitale", nonché di delineare proposte legislative in materia di "cripto-attività" e di "resilienza digitale". Si tratta di un'iniziativa che ben esemplifica l'approccio olistico della Commissione europea durante i lavori preparatori: le proposte si inquadrano nel Piano d'Azione definito nel 2018, muovono dagli studi in materia del Parlamento europeo e delle Autorità europee di vigilanza e sono state precedute da una consultazione degli *stakeholders* lanciata nella primavera del 2020.

Tra le proposte, quella avente ad oggetto l'emanazione di un regolamento europeo sui Mercati di Cripto-attività (*Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM(2020) 593 final-2020/0265(COD)* – "**Proposta MiCAR**"), mira a dotare l'Unione Europea di norme uniformi in materia di emittenti di cripto-attività, nonché di prestatori di servizi in cripto-attività (art. 2, comma 1, MiCAR), superando così l'attuale frammentazione tra regimi nazionali. L'importanza di assicurare agli operatori del settore la possibilità di avvalersi di un passaporto europeo per offrire i propri prodotti e servizi su cripto-attività nel territorio dell'Unione è ribadita a più riprese nei considerando (cfr. in particolare considerando 4 e 5) e giustifica, del resto, la stessa scelta di intervenire nella forma giuridica del regolamento. L'ampiezza delle misure elaborate dalla Commissione si lega anche alla presenza, a fianco della Proposta MiCAR, di due proposte satellite: la prima volta ad introdurre alcuni adattamenti alle disposizioni vigenti in materia di infrastrutture di mercato con particolare riferimento ad infrastrutture basate su tecnologie a registri distribuiti (*Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology - COM/2020/594 final*); la seconda volta a coordinare l'attuale disciplina finanziaria europea con le novità contenute nel "pacchetto per la finanza digitale" (*Proposal For A Directive Of The European Parliament And Of The Council Amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341- COM/2020/596 final*).

La proposta MiCAR si articola in sette titoli e può essere concettualmente suddivisa in quattro parti. La prima (coincidente con il Titolo I) è dedicata alle definizioni e alla individuazione del campo di applicazione del Regolamento. La seconda (coincidente con i Titoli II, III e IV) si occupa dell'offerta di cripto-attività, declinando la disciplina a seconda dell'oggetto di emissione. La terza (coincidente con il Titolo V) riguarda i prestatori di servizi in cripto-attività, mentre la quarta (coincidente con i Titoli VI e VII) guarda alla prevenzione e alla repressione degli abusi di mercato, nonché ai poteri e ai rapporti tra Autorità competenti.

La lettura del Titolo I lascia trasparire la forte influenza che gli studi elaborati dalle Autorità di vigilanza – e specialmente il parere reso dall'ESMA alla Commissione nel gennaio 2019 – hanno avuto nella definizione e classificazione delle cripto-attività. La proposta offre una definizione estremamente ampia di cripto-attività che, nell'accogliere i suggerimenti elaborati dalla *Financial Action Task Force*, ricomprende ogni "*rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*". Tuttavia, il fatto che una certa attività sia attratta in questa definizione non è di per sé sufficiente ad individuare la disciplina applicabile. Da un lato, infatti, restano al di fuori del MiCAR le cripto-

attività che già rientrano nella definizione di strumenti finanziari, moneta elettronica, depositi, depositi strutturati o cartolarizzazioni (art. 2, comma 2). Dall'altro lato, il MiCAR calibra la disciplina a seconda che la cripto-attività si qualifichi alla stregua di *utility token*, token collegato ad attività o token di moneta elettronica, offrendo una definizione (puramente descrittiva) di ciascuno di questi. Sia i token collegati ad attività che quelli di moneta elettronica sono riconducibili alla famiglia delle cc.dd. *stablecoin*, in quanto idonei a mantenere un valore stabile facendo riferimento, nel primo caso, al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività, nel secondo caso, al valore di una moneta fiduciaria avente corso legale. Infine, sotto il profilo soggettivo, il MiCAR contempla ipotesi di esenzione sia totale che parziale legate alla particolare natura dei soggetti interessati (art. 2, commi 3-6).

La seconda parte della Proposta MiCAR è dedicata, come detto, all'offerta di cripto-attività. Le previsioni in larga parte recepiscono pratiche di mercato consolidatesi nel tempo (tra tutte, quella relativa alla pubblicazione dei cc.dd. *white paper*) e riadattano al mercato delle cripto-attività norme già radicate nella disciplina europea del mercato dei capitali (in particolare, quelle contenute nel Regolamento (UE) 2017/1129 relativo al prospetto da pubblicare per l'offerta pubblica o l'ammissione alla negoziazione di titoli in un mercato regolamentato). L'offerta di cripto-attività deve, infatti, accompagnarsi alla pubblicazione di un documento informativo e al rispetto di taluni obblighi di condotta, tra i quali rientra un "obbligo di sicurezza informatica", su cui le ESAs sono chiamate ad emanare standard tecnici. A differenza di quanto previsto per le IPOs, il *white paper* è soggetto alla previa autorizzazione dell'Autorità competente soltanto nelle ipotesi in cui oggetto di offerta siano token collegati ad attività, atteso il rischio che queste attività potrebbero porre per la stessa sovranità monetaria. Quanto ai token di moneta elettronica – e stante la loro espressa equiparazione alla moneta elettronica – l'offerta può essere condotta unicamente da istituti di credito o istituti di moneta elettronica. È, peraltro, intuitivo che la necessità di individuare un soggetto emittente esclude che questa disciplina possa applicarsi a Bitcoin o alle altre cripto-valute prive di un emittente.

Spostando l'attenzione sulle norme che disciplinano i prestatori di servizi in cripto-attività, è chiara ancora una volta l'influenza esercitata della disciplina del mercato dei capitali, ed in particolare dalla disciplina MiFID. In primo luogo, la proposta MiCAR affianca ai servizi di custodia, di gestione di piattaforme di negoziazione e di scambio di cripto-attività – già ampiamente diffusi sul mercato – i tradizionali servizi finanziari elencati dalla MiFID: esecuzione di ordini, collocamento, ricezione e trasmissione di ordini, e consulenza sugli investimenti. La Proposta richiede poi che coloro che intendono operare come fornitori di servizi siano autorizzati dall'Autorità competente e rispondano a requisiti prudenziali, organizzativi e a regole di condotta che rispecchiano quelle già previste nei vari *silos* della regolamentazione dell'Unione. Spiccano, in particolare, gli obblighi di agire "*in modo onesto, corretto e professionale secondo il migliore interesse dei […] clienti effettivi e potenziali*", di fornire ai clienti "*informazioni corrette, chiare e non fuorvianti*" e di mantenere e applicare "*una politica efficace per prevenire, individuare, gestire e comunicare i conflitti di interesse*".

Infine, con riguardo ai Titoli VI e VII, la Proposta mira anzitutto a prevenire e reprimere i potenziali abusi di mercato in relazione alla negoziazione di cripto-attività. Anche in questo caso, è forte l'influenza esercitata dall'assetto normativo delineato dal Regolamento 596/2014 sugli abusi di mercato: sono, infatti, previsti l'obbligo dell'emittente di rendere pubbliche le informazioni privilegiate, il divieto di *insider trading*, il divieto di diffondere illecitamente informazioni privilegiate, nonché quello di porre in essere attività che possano tradursi in una manipolazione del mercato.

Quanto alla disciplina sulla vigilanza, ogni Stato membro è libero di designare le autorità competenti per lo svolgimento dei compiti delineati dalla Proposta. Specifiche competenze sono poi attribuite all'EBA in relazione alla vigilanza sui token collegati ad attività e quelli di moneta elettronica cc.dd. significativi.

MARTINA SCOPSI

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

3. La prima sentenza della Corte di Giustizia UE sul principio di «neutralità di Internet» ai sensi del regolamento (UE) 2015/2120.

Con sentenza del 15 settembre 2020 nelle Cause riunite C-807/18 e C-39/19 (la "**Sentenza**"), la

Corte di Giustizia UE ha per la prima volta offerto un'interpretazione sul principio di accesso a un'Internet aperta, detto anche di neutralità della rete, in particolare in relazione alle disposizioni di cui ai primi tre paragrafi dell'art. 3 del regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (il "**Regolamento**").

La Corte di Giustizia ha chiarito che le disposizioni di cui ai primi tre paragrafi dell'art. 3 del Regolamento ostano, per motivi diversi, a che un fornitore di servizi di accesso a Internet privilegi talune applicazioni e taluni servizi, mediante pacchetti facenti parte di accordi contrattuali che permettano a tali applicazioni e servizi di beneficiare di una «tariffa zero» che ne consenta una fruizione sostanzialmente illimitata, assoggettando al contempo l'utilizzo delle altre applicazioni e degli altri servizi disponibili a misure di blocco e/o di rallentamento del traffico.

La pronuncia ha preso le mosse da alcune soluzioni di abbonamento offerte della società ungherese Telenor, fornitrice di servizi di accesso a Internet, denominate 'MyChat' e 'MyMusic', consistenti in pacchetti di accesso preferenziale, contemplanti una c.d. «tariffa zero» per l'utilizzo di determinati applicazioni e servizi, in particolare consistenti in sei applicazioni specifiche di comunicazione on-line nel caso del pacchetto 'MyChat' (Facebook, Facebook Messenger, Instagram, Twitter, Wiber e Whatsapp) e in quattro applicazioni per la trasmissione di musica (Apple Music, Deezer, Spotify e Tidal) e sei servizi radiofonici nel caso del pacchetto 'MyMusic'. Le offerte in questione prevedevano che non si computasse il traffico dei dati interessati dalla «tariffa zero» nel monte dati complessivo acquistato dai clienti, consentendo inoltre ai clienti, dopo l'esaurimento del volume di dati acquistati, di continuare a utilizzare senza restrizioni tali servizi e tali applicazioni specifici, mentre alle altre applicazioni e agli altri servizi disponibili venivano applicate misure di rallentamento del traffico (nel caso di 'MyChat') e di rallentamento e blocco del traffico (nel caso di 'MyMusic').

L'Ufficio nazionale dei media e delle comunicazioni ungherese ("**UNMC**") adottava due decisioni con le quali dichiarava che tali due pacchetti attuavano misure di gestione del traffico che non rispettavano l'obbligo generale di trattamento equo e non discriminatorio del traffico Internet ai sensi dell'articolo 3, paragrafo 3 del Regolamento, ordinando alla società Telenor di porvi fine.

Dopo la conferma di tali provvedimenti da parte del Presidente dell'UNMC, Telenor faceva ricorso alla Corte di Budapest Capitale, lamentando, in sostanza, che l'UNMC aveva errato nell'applicare al caso di specie l'art. 3 paragrafo 3 del Regolamento, in quanto tale disposizione, sancendo un obbligo generale di trattamento equo e non discriminatorio del traffico nella fornitura di servizi di accesso a Internet, riguarderebbe unicamente le misure di gestione del traffico attuate unilateralmente dai fornitori di servizi di accesso ad Internet, e non si applicherebbe ai casi, come quello relativo ai pacchetti 'MyChat' e 'MyMusic', facenti parte di accordi conclusi con clienti, che, come tali, possono rientrare solo nell'ambito di applicazione del paragrafo 2 dell'art. 3 del Regolamento, che vieta ai fornitori dei servizi di accesso ad Internet di concludere accordi o adottare pratiche commerciali limitativi dell'esercizio dei diritti degli utenti finali come previsti dal paragrafo 1 dell'art. 3 del Regolamento.

La Corte di Budapest Capitale, così adita, interpellava quindi la Corte di Giustizia UE in via pregiudiziale in merito all'interpretazione dei paragrafi 1, 2 e 3 dell'articolo 3 del Regolamento in relazione ai vari profili di giudizio sottoposti alla sua cognizione.

La Corte di Giustizia UE ha innanzitutto dichiarato nella Sentenza che la disposizione di cui al paragrafo 2 dell'art. 3 del Regolamento va interpretata alla luce del Considerando 7 del Regolamento, avendo cioè riguardo alle posizioni di mercato dei fornitori dei servizi di accesso a Internet e dei fornitori dei contenuti, così che si possa stabilire la "portata" degli accordi e delle pratiche commerciali ivi menzionate, e in particolare la loro idoneità a limitare significativamente la scelta degli utenti finali e così i diritti menzionati nel paragrafo 1. Su questa base, la Corte di Giustizia ha rilevato che la conclusione di accordi mediante i quali determinati clienti sottoscrivono abbonamenti che combinano una «tariffa zero» con misure di blocco o di rallentamento del traffico connesso all'utilizzo di servizi e di applicazioni diversi da quelli che beneficiano di tale «tariffa zero» è idonea a limitare l'esercizio dei diritti degli utenti finali, ai sensi del paragrafo 2 dell'articolo 3 del Regolamento, in combinato disposto con il paragrafo 1 dello stesso articolo. Ciò in quanto, se simili accordi sono conclusi su una parte significativa del mercato, siffatti pacchetti sono tali da incrementare l'utilizzo

delle applicazioni e dei servizi privilegiati e, correlativamente, da rarefare l'utilizzo delle altre applicazioni e degli altri servizi disponibili, che è reso tecnicamente più difficoltoso, se non impossibile. Nella Sentenza viene argomentato che quanto più il numero di clienti che concludono simili accordi è rilevante, tanto più l'impatto cumulativo di tali accordi può, tenuto conto della loro portata, comportare una notevole limitazione all'esercizio dei diritti degli utenti finali, o addirittura compromettere l'essenza stessa di tali diritti.

Per quanto riguarda l'interpretazione del paragrafo 3 dell'art. 3 del Regolamento, la Corte ha rilevato, innanzitutto, che esso contiene un obbligo generale di trattamento equo, senza discriminazioni, restrizioni o interferenze del traffico al quale non si può derogare nemmeno attraverso accordi conclusi dai fornitori di servizi di accesso a Internet con gli utenti finali, o attraverso pratiche commerciali adottate da tali fornitori, con ciò implicitamente rispondendo all'obiezione di Telenor che riteneva invece non applicabile il paragrafo 3 dell'art. 3 del Regolamento ai pacchetti 'MyChat' e 'MyMusic', in quanto facenti parte di accordi conclusi con clienti (e come tali, secondo Telenor, soltanto assoggettabili al paragrafo 2 dell'art. 3 del Regolamento). In secondo luogo, la Corte ha chiarito che il sindacato di cui al paragrafo 3 dell'art. 3 del Regolamento è indipendente da quello di cui al paragrafo 2 del medesimo articolo. In terzo luogo, la Corte ha dichiarato che quando misure di rallentamento o di blocco del traffico sono basate non su requisiti di qualità tecnica del servizio, ma su considerazioni di ordine commerciale, tali misure devono ritenersi incompatibili con il paragrafo 3 dell'art. 3 del Regolamento, in quanto discriminatorie.

In conclusione, relativamente alle questioni sottoposte al controllo del giudice del rinvio, con la Sentenza la Corte di Giustizia UE ha ravvisato una violazione sia del paragrafo 2, in combinato disposto con il paragrafo 1, dell'art. 3 del Regolamento, in quanto i detti pacchetti, i detti accordi e le dette misure di blocco del traffico limitano l'esercizio dei diritti degli utenti finali come previsti dal paragrafo 1 del medesimo articolo; sia del paragrafo 3 dell'art. 3 del Regolamento, in quanto le dette misure di blocco o di rallentamento sono basate su considerazioni di ordine commerciale.

MICHELA PAGANELLI

http://curia.europa.eu/juris/document/document.jsf;jsessionid=5ED4CD6277132D7FEE048CCA296A9D92?text=&docid=231042&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=17593535

4. La lunga marcia verso il *GDPR* cinese: la prima legge sulla protezione delle informazioni personali della Repubblica popolare nella bozza per i commenti pubblici del 21 ottobre 2020.

Il 21 ottobre 2020, l'Assemblea nazionale popolare (全国人民代表大会, *Quangguo Renmin Daibiao Dahui*), principale organo legislativo cinese, ha presentato la bozza della 'Legge sulla protezione dei dati personali' (个人信息保护法, *geren xinxi baohu fa*), al fine di sottoporla alla consultazione pubblica. Essa è la prima normativa organica e sistematica in materia di protezione delle informazioni personali della repubblica popolare. Ad oggi, lo statuto delle informazioni personali, in Cina, è frammentato in una serie di leggi susseguitesi nel tempo (vedi il Capitolo IV della 'Legge sulla sicurezza informatica' del 2016, l'articolo 111 dei 'Principi generali del diritto civile' del 2017, gli articoli 5, 23, 25, 32, 79 e 87 della 'Legge sul commercio elettronico' del 2019, gli articoli 31 e 40 della 'Legge sulla crittografia' del 2019, il Capitolo VI della Parte IV del 'Codice civile' promulgato nel 2020) e in una fonte di rango secondario (mi riferisco allo *Standard GB/T 35273-2020 on Information Security Technology - Personal Information Security Specification*).

La bozza è composta da settanta articoli suddivisi a loro volta in otto capitoli: (a) disposizioni generali; (b) regole per il trattamento delle informazioni personali; (c) regole per il trasferimento transfrontaliero delle informazioni personali; (d) diritti delle persone nelle attività di trattamento delle informazioni personali; (e) doveri dei soggetti che trattano le informazioni personali; (f) dipartimenti che adempiono i doveri e le responsabilità in materia di protezione dei dati personali; (g) responsabilità legale; (h) disposizioni supplementari.

Dopo aver chiarito in premessa lo scopo della legge, se ne definisce l'ambito di applicazione, circoscritto a tutte quelle attività di trattamento delle informazioni personali compiute da organizzazioni e individui nell'esercizio della propria attività d'impresa, all'interno del territorio della Repubblica Popolare cinese, ed escludendola per tutti quei trattamenti effettuati nell'ambito di attività a carattere esclusivamente personale o domestico (similmente a quanto previsto nel *GDPR*).

Si distinguono le informazioni in *personali* (个人信息, *geren xinxi*: 'vari tipi di informazioni elettroniche o in altro modo registrate relative a un soggetto identificato o identificabile', Articolo 4) e in *personali sensibili* (敏感个人信息, *mingan geren xinxi*: 'informazioni personali la cui fuga o uso illecito comporterebbe un trattamento discriminatorio o gravi danni alla sicurezza personale o dei propri beni, inclusa la razza, l'etnia, le credenze religiose, i dati biometrici, le informazioni mediche relative alla salute, i conti finanziari e la posizione personale', Articolo 29). La prima definizione ricalca quasi interamente quella contenuta nella 'Legge sulla sicurezza informatica', all'articolo 76, e nel *GDPR* europeo, all'articolo 4, mentre la seconda costituisce una specificità del sistema cinese.

La legge sembrerebbe mutuare alcuni principi che sono già sanciti nel *GDPR*: in ossequio dei quali i dati dovranno essere trattati in modo legale e legittimo, per un chiaro e ragionevole scopo, per un tempo determinato e secondo il crisma della buona fede. Essa impone ai soggetti che trattano informazioni personali gravosi oneri al fine di perseguire un sano sviluppo della *digital economy*, pena l'imposizione di sanzioni.

È evidente l'intento del legislatore cinese di contemperare due opposti interessi: da un lato, la promozione dell'innovazione attraverso lo sfruttamento dei dati, dall'altro, l'esigenza di tutelare l'interesse personale degli individui. È necessario infine precisare che il progetto, prima di essere approvato, necessita di almeno altre tre revisioni, durante le quali potrebbe chiaramente subire delle modifiche, seppur minime.

CORRADO MORICONI 马思勇

https://www.dataguidance.com/sites/default/files/china_draft_personal_data_law.pdf
http://www.ahwx.gov.cn/zcfg/gfxwj/202007/t20200708_4629245.html
https://www.sohu.com/a/426584424_780954

5. Le FAQ del Garante per la protezione dei dati personali sulla refertazione online.

Lo scorso ottobre il Garante privacy è intervenuto pubblicando dei chiarimenti, sotto forma di FAQ, sul tema della refertazione online. Si tratta di un tema di estrema rilevanza data la natura particolarmente sensibile dei dati coinvolti quali sono, appunto, i dati sanitari. Le nuove FAQ intervengono ad aggiornare, per la prima volta dopo l'entrata in vigore del GDPR, le precedenti "Linee guida in tema di referti online" del 2009.

Innanzitutto, il Garante precisa che per "referto online" deve intendersi la possibilità di accedere ad un referto medico tramite modalità digitali quali il Fascicolo sanitario elettronico, siti web, posta elettronica anche certificata.

Relativamente alla base giuridica, il Garante, confermando quanto già dichiarato nel DPCM dell'8 agosto 2013, specifica che il trattamento deve essere fondato sul consenso esplicito, libero, specifico e informato dell'interessato, preceduto dal rilascio di un'apposita informativa ex artt. 13-14 GDPR, distinta rispetto a quella relativa al trattamento dei dati personali per finalità di cura, che indichi le caratteristiche del servizio di refertazione online. Il consenso, dunque, continua a porsi come base giuridica necessaria, diversamente da quanto accade per il trattamento dei dati necessario all'erogazione della prestazione sanitaria ex art. 9, par. 2, lett. h) GDPR, in quanto la refertazione online costituisce un servizio accessorio, ulteriore e distinto dall'attività di cura, di cui l'interessato può liberamente scegliere se avvalersi o meno, senza che questo pregiudichi il suo diritto all'erogazione della prestazione sanitaria. Il consenso, inoltre, può essere concesso con riferimento ad alcuni referti ma escluso per altri (fermo restando il divieto di refertazione online per accertamenti relativi ad indagini genetiche o all'HIV).

Al fine di assicurare un'adeguata tutela dei dati sensibili contenuti nel referto, il Garante individua una serie di misure di sicurezza di natura sia tecnica che organizzativa che la struttura sanitaria deve porre in essere. Con specifico riferimento alla comunicazione del referto al paziente, devono essere adottati protocolli di comunicazione sicuri (*https*) e sistemi di autenticazione forte dell'interessato (*strong authentication*); il referto deve essere reso disponibile sul sito web della struttura per un massimo di 45 gg. con possibilità per l'interessato di cancellare dal sistema di consultazione tutti o alcuni dei referti che lo riguardano. In caso di trasmissione tramite e-mail, il referto deve essere spedito come allegato e non deve comparire come testo nel corpo del messaggio; il file contenente il referto deve essere protetto tramite password e eventuali SMS possono essere utilizzati solo per dare notizia della disponibilità del referto senza riportare la tipologia di accertamenti effettuati, il loro esito o le credenziali di autenticazione dell'interessato. A queste si aggiungono le specifiche misure di sicurezza già

previste dalle Linee guida del 2009 e dal DPCM del 2013.

Infine, l'offerta su larga scala di nuovi servizi di refertazione con l'uso di nuove tecnologie deve essere preceduta da una valutazione d'impatto (DPIA) ai sensi dell'art. 35 GDPR e deve essere predisposta un'apposita procedura per la gestione dei *data breach*, che consenta di intervenire tempestivamente in caso di violazione del sistema di refertazione online e di monitorarne costantemente la sicurezza.

CHIARA RAUCCIO

https://www.garanteprivacy.it/faq/referti-online

6. La nuova indagine della Commissione europea per abuso di posizione dominante di Amazon

Il 10 novembre 2020 la Commissione europea ha formalizzato l'avvio di una nuova procedura antitrust a carico della piattaforma e-commerce statunitense Amazon ai sensi degli articoli 11(6) del Regolamento del Consiglio No 1/2003 e 2(1) del Regolamento della Commissione No 773/2004.

Tale procedura si basa su un'ipotesi di abuso di posizione dominante da parte di Amazon tramite condotte distorsive della concorrenza al fine di favorire le proprie attività di vendita al dettaglio e/o dei venditori terzi che si servono dei servizi di logistica prestati dalla medesima Amazon, ossia di gestione dell'inventario, del magazzino, delle spedizioni e del servizio clienti (c.d. *Fulfillment by Amazon*). Questa indagine comprende tutta l'Area Economica Europea, ad eccezione del mercato italiano.

Il medesimo giorno la Commissione Europea recapitava ad Amazon, informando i regolatori degli Stati Membri dell'UE, una comunicazione di addebito relativa alla procedura avviata in data 17 luglio 2019, avente ad oggetto l'utilizzo fatto dalla società dei dati dei venditori operanti sulla propria piattaforma digitale ("*marketplace*"). Sebbene la Francia e la Germania siano indicati come i mercati più interessati per via del volume delle transazioni, anche tale procedura si estende a tutta l'Area Economica Europea. In questo caso l'addebito configura condotte ed effetti economici vietati dagli articoli 101 e 102 del TFUE.

In maggior dettaglio, le contestazioni della Commissione europea riguardano il duplice ruolo svolto dalla piattaforma Amazon sia di canale distributivo per aziende indipendenti, che di venditore di prodotti propri tramite il medesimo canale.

Infatti, si legge nella comunicazione di addebito che Amazon farebbe uso di informazioni non pubbliche raccolte attraverso il proprio *marketplace*, sulle vendite ed i prodotti di terzi venditori (quali il numero di ordini e di spedizioni per specifici prodotti, i ricavi del venditore, il numero di click alle offerte postate, i reclami e le restituzioni, altre misure di performance) per calibrare le offerte di vendita di prodotti propri e prendere decisioni strategiche a scapito delle aziende concorrenti. Una volta che tali informazioni confluiscono direttamente nel suo sistema automatizzato di aggregazione dei dati, Amazon ha la possibilità di sfruttarle per influenzare la visibilità dei suoi prodotti o di quelli di coloro che si avvalgono della logistica Amazon tramite il canale "*Buy Box*", con l'effetto di distorcere la concorrenza, abusando del proprio posizionamento di leader europeo tra i fornitori di servizi di mercato e-commerce.

Questa ipotesi accomuna la seconda investigazione ancora in fase preliminare, riguardante le condizioni ed i criteri che governano gli algoritmi di assegnazione ai venditori della permanenza nel "*Buy Box*", oltre che i criteri di selezione dei venditori abilitati ad offrire i propri prodotti agli utenti del programma fedeltà "*Prime*". Il fatto che nella sezione "*Buy Box*" dell'interfaccia della piattaforma digitale, ovvero lo spazio online attraverso il quale avvengono la maggior parte delle vendite su Amazon, sia mostrata l'offerta di un singolo venditore per prodotto scelto dal consumatore, direttamente acquistabile con un unico click, costituisce un vantaggio cruciale, così come l'accesso privilegiato ai clienti "*Prime*", statisticamente maggiormente attivi e in costante crescita. Ne consegue che costituirebbe una distorsione della concorrenza favorire artificialmente la vendita dei prodotti Amazon o quelli dei venditori che utilizzano i suoi servizi di logistica attraverso tali canali.

In questa fase i due procedimenti avviati dalla Commissione europea non comprovano definitivamente l'esistenza di un'infrazione da parte di Amazon e non pregiudicano, dunque, la possibilità che vi sia un esito contrario alle allegazioni rese pubbliche dall'Autorità europea. Ad ogni modo, la Commissione darà priorità alla prosecuzione di tale indagine e spetterà ad Amazon iniziare a presentare le proprie difese, alla luce del fatto che, qualora fossero accertate le violazioni, la società rischia sanzioni nell'ordine dei miliardi di euro, ossia fino al 10% dei ricavi annuali in Europa. In alternativa, la società potrebbe decidere di adottare un approccio collaborativo con la

Commissione al fine di trovare un accordo sulle sanzioni e i rimedi successivi che saranno imposti alla società.

DOMENICO PIERS DE MARTINO

https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077

7. *Droits voisins e snippets*: la Corte d'appello di Parigi conferma la decisione dell'Autorità garante della concorrenza francese nei confronti di Google.

La Corte d'appello di Parigi, con l'*arrêt* dell'8 ottobre 2020, ha respinto il ricorso presentato da Google avverso la decisione n. 20-MC-01 della *Autorité de la Concurrence* del 9 aprile 2020 l'"**Autorità**"), con la quale, constatato un pregiudizio grave ed immediato al settore della stampa per abuso di posizione dominante, l'Autorità ha ingiunto alla piattaforma di Mountain View di avviare e concludere entro tre mesi le negoziazioni con agenzie di stampa, organismi di gestione collettiva ed i maggiori editori francesi (ovvero i cd. titolari dei diritti sui contenuti) al fine di raggiungere un accordo sull'equa remunerazione per l'utilizzo dei contenuti di questi ultimi attraverso i cd. *snippets*. Trattasi di anteprime o estratti di notizie (letteralmente *frammenti*), rinvenibili online gratuitamente sulle pagine dei collettori di news (nel caso di specie, Google News) che, di tal guisa, veicolano e utilizzano contenuti protetti dai diritti connessi al diritto d'autore (cd. *droits voisins*).

Segnatamente, l'Autorità ha accolto il ricorso presentato dall'*AFP* (*Alliance de la presse d'information générale*) e dagli organi di rappresentanza degli editori di giornali (*Syndicat des éditeurs de la presse magazine*), che chiedevano un'equa retribuzione per l'utilizzo dei loro contenuti, stabilendo, *inter alia*, che «*(i)lest enjoint aux sociétés Google LLC, Google Ireland Ltd et Google France, à titre conservatoire et dans l'attente d'une décision au fond, de négocier de bonne foi avec les éditeurs et agences de presse ou les organismes de gestion collective qui en feraient la demande, la rémunération due par Google à ces derniers pour toute reprise des contenus protégés sur ses services, conformément aux modalités prévues à l'article L. 218-4 du code de la propriété intellectuelle et selon des critères transparents, objectifs et non discriminatoires»;* ed aggiunge che *«(c)ette négociation devra couvrir la période de reprise des contenus depuis le 24 octobre 2019»*, sancendone l'efficacia retroattiva.

La vicenda s'inscrive nel più ampio quadro normativo recentemente riformato a livello europeo dalla direttiva 790/2019/UE del Parlamento europeo e del Consiglio del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale. Quest'intervento di armonizzazione della disciplina sul *copyright* si pone all'esito di un acceso dibattito, sia fuori che dentro le sedi istituzionali, che non può ancora dirsi del tutto sopito. In particolare, un *punctum dolens* della direttiva è ravvisabile, secondo le più note piattaforme digitali, nell'art. 15 che disciplina la "protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online", invocato nel caso di specie.

Ciononostante, con quest'intervento, il legislatore europeo ha inteso armonizzare la disciplina *in subjecta materia* all'interno dei singoli Stati membri. Tra questi, la Francia è stato il primo Paese a recepire il 24 luglio 2019 la direttiva *copyright*, con la quasi unanimità dei voti in Parlamento (solo un voto contrario).

Il termine per il recepimento per gli altri Stati membri è fissato per il 7 giugno 2021, sebbene si registri un forte pressing da parte di autori ed editori – anche in Italia – affinché venga recepita in tempi brevi.

Con questa fondamentale decisione, inoltre, la Francia si candida come apripista anche sul terreno giurisprudenziale, offrendo un 'formante' con effetti che certamente travalicheranno i confini nazionali, riversandosi in tutti gli altri ordinamenti ed aprendo, *de facto*, un varco per l'avvio di negoziati nel settore di riferimento. In altri termini, la decisione appare destinata a riscrivere i rapporti tra le piattaforme digitali e i titolari dei diritti d'autore nel mercato unico digitale europeo.

LUCIO CASALINI

https://www.autoritedelaconcurrence.fr/sites/default/files/appealsd/2020-10/ca_20mc01_oct20.pdf
https://www.autoritedelaconcurrence.fr/sites/default/files/integral_texts/2020-04/20mc01.pdf

8. La Sapienza aderisce alla "Rome Call for AI Ethics".

Il 30 ottobre 2020 l'Università Sapienza di Roma ha formalizzato la sua adesione alla "Rome Call for AI Ethics", con la firma del documento da parte del Rettore Eugenio Gaudio, alla presenza di Mons. Vincenzo

Paglia, Presidente della Pontificia Accademia per la Vita.

"Rome Call for AI Ethics", promossa dalla Pontificia Accademia per la Vita, è stata presentata il 28 febbraio 2020 e ha avuto come primi firmatari rappresentanti della FAO, del Governo italiano, di Microsoft ed IBM, come riportato nella notizia n. 7 del primo numero di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf.

Il documento, inteso a promuovere un'opera di sensibilizzazione intorno ai temi dell' "etica" della intelligenza artificiale, in particolare con riferimento alle sue possibilità di perpetuare ed amplificare discriminazioni e pratiche lesive della libertà degli esseri umani e della dignità dei soggetti più vulnerabili, individua sette principi, da sviluppare in ambito educativo e giuridico, per una c.d. "*algorethical vision*": trasparenza, inclusione, responsabilità, imparzialità, affidabilità, sicurezza e privacy.

https://www.uniroma1.it/it/notizia/sapienza-ha-aderito-alla-rome-call-ai-ethics-un-approccio-etico-allintelligenza-artificiale#:~:text=per%20la%20Vita-,Venerdì%2030%20ottobre%202020%20è%20stata%20formalizzata%20l'adesione%20della,Gaudio%2C%20alla%20presenza%20di%20Mons.&text=Fare%20scelte%20etiche%20oggi%20significa%20cercare%20di%20trasformare%20il%20progresso%20in%20sviluppo