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. Verso l'*Artificial Intelligence Act*: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale.

Con il documento COM(2021) 206 final del 21 aprile 2021, recante "Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione", la Commissione europea ha pubblicato una proposta normativa volta a fissare un quadro di divieti e di requisiti per i sistemi di IA, comprensivo di un apparato sanzionatorio e istituzionale (la "**Proposta di *AI Act***").

La Proposta di *AI Act* comprende una bozza di regolamento (la "**Bozza di Regolamento**") con i relativi allegati (gli "**Allegati**") ed una relazione esplicativa (la "**Relazione**").

Nella Relazione si ricordano innanzitutto i principali documenti e le principali azioni adottate negli ultimi anni dalle istituzioni dell'Unione europea in materia di intelligenza artificiale ("**IA**"). In particolare, per quanto riguarda il Consiglio europeo, la Relazione ricorda: lo *European Council meeting (19 October 2017) – Conclusion* EUCO 14/17, 2017, p. 8; l' *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption* 6177/19, 2019; lo *Special meeting of the European Council (1 and 2 October 2020) – Conclusions*, EUCO 13/20, 2020, p. 6; le *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020.

Quanto al Parlamento europeo, la Relazione ricorda le risoluzioni adottate nell'ottobre 2020 sull'etica, la responsabilità civile e il *copyright* (preceduti dalla pubblicazione di tre *draft reports* della commissione JURI dell'aprile 2020, sui quali v. le notizie n. 2, 3 e 4 del numero 2/2020 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf): la *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*, 2020/2012(INL); la *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence*, 2020/2014(INL) (su cui la notizia n. 1 del numero 4/2020 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf), la *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies*, 2020/2015(INI); nonché i documenti del 2021 in materia di diritto penale e in materia di educazione, cultura e settore audiovisivo: lo *European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2020/2016(INI) e lo *European Parliament Draft Report, Artificial intelligence in education, culture and the audiovisual sector*, 2020/2017(INI).

Quanto alla Commissione europea, la Relazione ricorda il libro bianco sulla IA del febbraio 2020, ossia lo *European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final, 2020 (su cui v. la notizia n. 5 nel numero 1/2020 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf), nonché il *Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education* – Commission Communication COM(2020) 624 final.

La Relazione spiega che la Bozza di Regolamento è stata concepita con l'intenzione di limitare i requisiti legali per le imprese che immettono soluzioni di IA nel mercato nella misura minima necessaria per affrontare i "rischi" e i "problemi" legati all'IA. Nella Relazione si dà atto che, in esito ad una consultazione pubblica, l'opzione scelta per la Bozza di Regolamento riflette il modello di uno strumento legislativo "orizzontale" che segue un approccio proporzionato basato sul rischio, e che contempla codici di condotta per i sistemi di IA "non ad alto rischio". In conseguenza della scelta di modello legislativo "orizzontale", la Proposta di *AI Act* è intesa ad inserirsi in un quadro normativo coerente avuto riguardo alle altre normative e politiche legislative dell'Unione e viene specificato che la Proposta di *AI Act* non pregiudica l'applicazione del diritto della concorrenza dell'Unione. La Bozza di Regolamento è dichiaratamente coerente con la Carta dei diritti fondamentali della UE e l'esistente legislazione "secondaria" dell'Unione sulla protezione dei dati personali, sulla tutela dei consumatori, sulla non discriminazione e sull' uguaglianza di genere. In particolare, la Relazione specifica che la Proposta di *AI Act* non pregiudica bensì integra le disposizioni del GDPR (Regolamento (UE) 2016/679) e della direttiva *Law Enforcement* (Direttiva (UE) 2016/680) prevedendo regole armonizzate sulla progettazione, sviluppo e

uso di certi sistemi di IA ad alto rischio e alcuni limiti per alcune utilizzazioni di sistemi di identificazione biometrica a distanza. La Relazione dichiara che la Bozza di Regolamento si propone di integrare la legislazione esistente dell'Unione sulla non-discriminazione al fine di minimizzare il rischio di "discriminazione algoritmica". Con riferimento ai sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del c.d. "Nuovo Quadro Normativo" (*New Legislative Framework*, "**NLF**"), ad es. macchinari, dispositivi medici, giocattoli, etc., la Relazione specifica che i requisiti per i sistemi di IA previsti nella Bozza di Regolamento dovranno essere controllati nel contesto delle procedure di controllo di conformità previsti dalla legislazione NLF di volta in volta applicabile. Per quanto riguarda la questione del coordinamento tra i varî e diversi requisiti, la Relazione precisa che mentre la Bozza di Regolamento intende occuparsi dei rischi di sicurezza tipici dei sistemi di IA attraverso la predisposizione di specifici requisiti, la legislazione NLF è intesa ad assicurare la sicurezza complessiva del prodotto finale e può, di conseguenza, contenere la previsione di specifici requisiti che riguardano condizioni per integrare in modo sicuro un sistema di IA in un prodotto finale. A questo riguardo, la Relazione aggiunge che tale approccio è seguito dalla **proposta di *Machinery Regulation*** adottata il 21 aprile 2021, ossia nello stesso giorno della Proposta di *IA Act*: *Proposal for a Regulation of the European Parliament and of the Council on machinery products* COM(2021) 202 (https://ec.europa.eu/docsroom/documents/45508).

Nell'Allegato II, sezione A della Bozza di Regolamento, sono elencati i seguenti atti della legislazione NLF: Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE [che si prevede sarà abrogata dal nuovo regolamento sui prodotti macchina]; Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli; Direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE; Direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori; Direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva; Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE; Direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione; Regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la direttiva 2000/9/CE; Regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio; Regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE; Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio; Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione.

Invece, per quanto riguarda i sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla legislazione del c.d. vecchio approccio ("***Old Approach legislation***"), ad es. aeromobili, autoveicoli, la Relazione aggiunge che la Proposta di *AI Act* non si applica direttamente, e che, tuttavia, gli essenziali requisiti *ex-ante* per i sistemi di IA di alto rischio dovranno essere presi in considerazione quando si adotteranno normative attuative o delegate della medesima legislazione. Ciò è ribadito nel Considerando 29 e nell'art. 2, para. 2 della Bozza di Regolamento, relativamente ai seguenti atti della c.d. *Old Approach legislation*: Regolamento (CE) 300/2008 che istituisce norme comuni per la sicurezza dell'aviazione civile; Regolamento (UE) No 167/2013 sull'omologazione e la vigilanza del mercato dei veicoli agricoli e forestali; Regolamento (UE) No 168/2013 sull'omologazione e la vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli; Direttiva 2014/90/UE sull'equipaggiamento marittimo; Direttiva (UE) 2016/797 sull'interoperabilità del sistema ferroviario

dell'Unione europea; Regolamento (UE) 2018/858 sull'omologazione e la vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli; Regolamento (UE) 2018/1139 recante norme comuni nel settore dell'aviazione civile e che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea; Regolamento (UE) 2019/2144 sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada. Riferendosi a tali atti, il Considerando 29 della Bozza di Regolamento statuisce che è opportuno modificarli per far sì che la Commissione, nell'adottare qualsiasi futuro provvedimento attuativo o delegato sulla base dei medesimi atti, possa tener conto dei requisiti obbligatori *ex-ante* stabiliti nella Bozza di Regolamento per i sistemi di IA ad alto rischio, sulla base delle specificità tecniche e regolamentari di ciascun settore; e l'art. 2 para 2 della Bozza di Regolamento prevede che ai sistemi di IA ad alto rischio che costituiscono componenti di sicurezza di prodotti o sistemi, o che sono essi stessi prodotti o sistemi disciplinati dagli atti di cui sopra, si applica soltanto l'art. 84 della Bozza di Regolamento, il quale ultimo prevede alcuni compiti della Commissione in materia di revisione della normativa.

La Relazione aggiunge che per quanto concerne i sistemi di IA forniti o utilizzati da enti creditizi regolamentati, le autorità competenti per il controllo sulla legislazione dell'Unione in materia di servizi finanziari dovrebbero essere designate come autorità competenti per il controllo dell'osservanza dei requisiti previsti dalla Proposta di *AI Act* al fine di assicurare un'applicazione coerente della normativa dell'Unione in materia di servizi finanziari laddove i sistemi di IA siano in una certa misura implicitamente regolamentati in relazione al sistema di *governance* interna degli enti creditizi. A tal proposito, l'art. 9, ultimo paragrafo della Bozza di Regolamento prevede che per gli enti creditizi disciplinati dalla direttiva 2013/36/UE (la direttiva sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale) le previsioni dettate dal medesimo art. 9 della Bozza di Regolamento in materia di gestione dei rischi si debbano osservare includendole nelle procedure di gestione dei rischi previste dalla medesima direttiva. Infine, la Relazione dichiara che la Proposta di *AI Act* è coerente con la legislazione dell'Unione applicabile ai servizi, compresi i servizi di intermediazione regolati dalla direttiva sul commercio elettronico (direttiva 2000/31/CE) e la recente proposta della Commissione per la legge sui servizi digitali, c.d. *Digital Services Act* (su cui v. notizia n. 3 sul numero 1/2021 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf). Per quanto riguarda le altre linee di politica legislativa dell'Unione, la Relazione sottolinea la coerenza della Proposta di *AI Act* con i documenti in materia di innovazione digitale (Comunicazione della Commissione, "Plasmare il futuro digitale dell'Europa" (COM(2020) 67 final; "Bussola per il digitale 2030: il modello europeo per il decennio digitale") e in materia di *governance* e mercato dei dati (Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati (c.d. *Data Governance Act*) (COM/2020/767); Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico; Comunicazione della Commissione, "Una strategia europea per i dati" (COM/2020/66 final)).

La Relazione specifica che la base dell'intervento è ravvisata nell'art. 114 TFUE, e richiama i principi di sussidiarietà e di proporzionalità. Sempre secondo la Relazione, la Bozza di Regolamento persegue i seguenti obiettivi:

- assicurare che i sistemi di IA immessi e utilizzati nel mercato dell'Unione siano sicuri e rispettino la normativa esistente sui diritti fondamentali e i valori dell'Unione;
- assicurare certezza del diritto al fine di facilitare l'investimento e l'innovazione in IA;
- rafforzare l'effettiva applicazione della normativa esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA legittime, sicure e meritevoli di fiducia ed evitare la frammentazione di mercato.

Venendo ai contenuti della Bozza di Regolamento, il titolo I (artt. 1-4) definisce l'oggetto del regolamento e l'ambito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. L'art. 2 para. 1 stabilisce che la Bozza di Regolamento si applica: a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo; b) agli utenti dei sistemi di IA situati nell'Unione; c) ai fornitori e agli utenti di sistemi di IA situati in un paese terzo, laddove l'*output* prodotto dal sistema sia utilizzato nell'Unione. L'art. 2 para. 3 prevede che la Bozza di

Regolamento non si applica ai sistemi di IA sviluppati o usati per scopi esclusivamente militari. L'art. 2 para. 4 esclude l'applicazione del regolamento alle "*autorità pubbliche di un paese terzo [e] alle organizzazioni internazionali […], laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri*". L'art. 3 della Bozza di Regolamento stabilisce le definizioni utilizzate in tutto l'atto. Come si ricava anche dalla Relazione, la definizione di sistema di IA intende essere "*future proof*" ossia mira ad essere il più possibile neutrale dal punto di vista tecnologico e in questo senso adeguata alle esigenze future. Il sistema di IA è definito come "*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*". L'Allegato I della Bozza di Regolamento prevede le seguenti tre tipologie di "approcci" e "tecniche" in funzione della predetta definizione: "*a) Approcci di apprendimento automatico [*machine learning*], compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (*deep learning*); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione*.". È previsto che tale allegato debba essere adattato dalla Commissione in linea con i nuovi sviluppi tecnologici. L'art. 3 definisce anche gli "*operatori*" lungo l'intera catena del valore dell'IA, ossia il "*fornitore*" (e anche il "*fornitore di piccole dimensioni*"), l'"*utente*", il "*rappresentante autorizzato*", l'"*importatore*" e il "*distributore*", considerando tanto gli operatori pubblici quanto quelli privati.

Il titolo II della Bozza di Regolamento – che consiste del solo articolo 5 – prevede quattro fattispecie di "*pratiche*" di IA vietate. In modo conforme a molti atti e documenti in materia, la Bozza di Regolamento segue un approccio basato sul rischio, differenziando tra gli usi dell'IA che creano: i) un rischio inaccettabile; ii) un rischio alto; iii) un rischio basso o minimo. Le "*pratiche*" vietate di cui all'art. 5 sono quelle che secondo la Bozza di Regolamento creano un rischio inaccettabile. Relativamente alle prime tre fattispecie di cui all'art. 5 per "*pratiche*" si intendono "*l'immissione sul mercato, la messa in servizio o l'uso*" di un sistema di IA, mentre per la quarta fattispecie, la pratica vietata è il solo "*uso*". Le prime due fattispecie di pratiche riguardano sistemi di IA idonei a falsare il comportamento delle persone in modo tale da procurare un "*danno fisico o psicologico*". La terza fattispecie riguarda sistemi di IA di c.d. *social scoring* e il divieto si applica solo se le pratiche sono poste in essere da autorità pubbliche o per loro conto e se tali sistemi di AI sono idonei a produrre determinati "*trattamenti pregiudizievoli o sfavorevoli*" per determinate persone o gruppi di persone. La quarta fattispecie di pratica vietata consiste nell'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto svolte dalle autorità per la prevenzione, indagine, accertamento o perseguimento di reati o per esecuzione di sanzioni penali, fatta salva l'applicazione di talune eccezioni limitate.

Il titolo III della Bozza di Regolamento (artt. 6-51) contiene regole specifiche per i sistemi di IA che creano un "rischio alto" per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche. In linea con un approccio basato sul rischio, tali sistemi di IA ad alto rischio sono consentiti sul mercato europeo subordinatamente al rispetto di determinati requisiti obbligatori e ad una valutazione della conformità *ex ante*. La classificazione di un sistema di IA come ad alto rischio si basa sulla sua finalità prevista, in linea con la normativa vigente dell'UE in materia di sicurezza dei prodotti. Di conseguenza la classificazione come ad alto rischio non dipende solo dalla funzione svolta dal sistema di IA, ma anche dalle finalità e modalità specifiche di utilizzo di tale sistema.

Il capo 1 del titolo III fissa le regole di classificazione e individua nell'art. 6 due categorie principali di sistemi di IA ad alto rischio:

- i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti, o che sono essi stessi prodotti, soggetti a valutazione di conformità *ex ante* da parte di terzi, ai sensi della normativa di armonizzazione dell'Unione di cui all'Allegato II;
- altri sistemi di IA c.d. "indipendenti" che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'Allegato III.

Tale elenco di sistemi di IA ad alto rischio di cui all'Allegato III contiene una descrizione tipologica di 21 sistemi di IA afferenti ai seguenti 8

settori, dichiaratamente scelti dalla Commissione ed inseriti nel medesimo Allegato III per la circostanza che i relativi "rischi" si sono già "concretizzati" o "potrebbero concretizzarsi nel prossimo futuro": (i) Identificazione e categorizzazione biometrica delle persone fisiche; (ii) Gestione e funzionamento delle infrastrutture critiche; (iii) Istruzione e formazione professionale; (iv) Occupazione, gestione dei lavoratori e accesso al lavoro autonomo; (v) Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi; (vi) Attività di contrasto di reati; (vii) Gestione della migrazione, dell'asilo e del controllo delle frontiere; (viii) Amministrazione della giustizia e processi democratici. Al fine di assicurare che il regolamento possa essere adattato in futuro agli usi e alle applicazioni emergenti dell'intelligenza artificiale, è previsto che la Commissione possa ampliare l'elenco dei sistemi di IA ad alto rischio utilizzati all'interno di alcuni settori predefiniti, applicando una serie di criteri e una metodologia di valutazione dei rischi.

Il capo 2 del titolo III definisce i requisiti giuridici per i sistemi di IA ad alto rischio in relazione a dati e *governance* dei dati (art. 10), documentazione (art. 11 e Allegato IV) e conservazione delle registrazioni, trasparenza e fornitura di informazioni agli utenti, sorveglianza umana, robustezza, accuratezza e sicurezza.

Il capo 3 del titolo III definisce una serie di obblighi orizzontali per i fornitori di sistemi di IA ad alto rischio. Obblighi proporzionati sono imposti anche a utenti e altri operatori.

Il capo 4 del titolo III definisce il quadro per gli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità, mentre il capo 5 del titolo III prevede le procedure di valutazione della conformità da seguire per ciascun tipo di sistema di IA ad alto rischio. A tali procedure si riferiscono gli Allegati V, VI, VII e VIII.

Il titolo IV della Bozza di Regolamento, che consiste del solo art. 52, prevede "obblighi di trasparenza" per i sistemi di IA che: i) interagiscono con gli esseri umani; ii) sono utilizzati per rilevare emozioni o stabilire un'associazione con categorie (sociali) sulla base di dati biometrici; oppure iii) generano o manipolano contenuti ("*deep fake*"). È previsto che le persone debbano essere informate quando interagiscono con un sistema di IA o le loro emozioni o caratteristiche vengono riconosciute attraverso mezzi automatizzati. Se un sistema di IA viene utilizzato per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a contenuti autentici, è previsto in linea generale, e salve alcune eccezioni per finalità legittime (come la finalità di contrasto di reati e la libertà di espressione), l'obbligo di rivelare che tali contenuti sono generati ricorrendo a mezzi automatizzati.

Il titolo V della Bozza di Regolamento (artt. 53-55) dedicato alle "misure di sostegno all'innovazione" prevede alcune disposizioni in materia di spazi di sperimentazione normativa, le c.d. *sand-boxes*.

Il titolo VI della Bozza di Regolamento (artt. 56-59) dedicato alla "*governance*" prevede il quadro istituzionale per i sistemi di IA, ed in particolare l'istituzione di un Comitato europeo per l'IA (lo '*European Artificial Intelligence Board*'), costituito da rappresentanti degli Stati membri e della Commissione europea. A livello nazionale, è previsto che gli Stati membri dovranno designare una o più autorità nazionali competenti e, tra queste, l'autorità nazionale di controllo, al fine di controllare l'applicazione e l'attuazione del regolamento.

Il titolo VII della Bozza di Regolamento, che consiste del solo art. 60, intitolato "Banca dati dell'UE per i sistemi di IA indipendenti ad alto rischio" prevede la creazione di una banca dati a livello dell'UE per sistemi di IA ad alto rischio "indipendenti" che presentano principalmente implicazioni in relazione ai diritti fondamentali. È previsto che la banca dati sia gestita dalla Commissione e alimentata con i dati messi a disposizione dai fornitori dei sistemi di IA, che saranno tenuti a registrare i propri sistemi prima di immetterli sul mercato o altrimenti metterli in servizio.

Il titolo VIII della Bozza di Regolamento (artt. 61-68) intitolato "Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato" stabilisce gli obblighi in materia di monitoraggio e segnalazione per i fornitori di sistemi di IA per quanto riguarda il monitoraggio successivo all'immissione sul mercato e la segnalazione di incidenti e malfunzionamenti correlati all'IA nonché le indagini in merito. È previsto che il regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti si applichi ai sistemi di IA disciplinati dalla Bozza di Regolamento.

Il titolo IX della Bozza di Regolamento, che consiste del solo art. 69, intitolato "Codici di condotta" mira a incoraggiare i fornitori di sistemi di IA non ad alto rischio ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio

Il titolo X della Bozza di Regolamento (artt. 70-73) intitolato "Riservatezza e sanzioni" contiene alcune importanti disposizioni, in particolare l'art.

71 che prevede sanzioni amministrative pecuniarie per la violazione del divieto di cui all'art. 5 (pratiche vietate) e la mancata osservanza dei requisiti di conformità di cui all'art. 10 (dati e *governance* dei dati) nella misura di un importo fino a 30 milioni di euro o, in caso di società, di un importo fino al 6 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Sanzioni amministrative pecuniarie con tetti massimi inferiori sono previste per l'inosservanza di altre disposizioni della Bozza di regolamento, diverse da quelle contenute negli artt. 5 e 10. L'art. 72 prevede sanzioni amministrative pecuniarie a carico di istituzioni, agenzie e organismi dell'Unione. L'art. 70 prevede che le autorità nazionali competenti e gli organismi notificati che partecipano all'applicazione del regolamento debbano rispettare la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, *inter alia*, i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, salva l'applicazione dell'art. 5 della direttiva 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali). L'art. 70 contiene altre previsioni in materia di scambio di informazioni tra le autorità competenti.

I restanti titoli XI e XII contengono le regole per l'esercizio della delega e delle competenze di esecuzione e alcune disposizioni finali, tra cui la previsione dell'esclusione di applicazione del regolamento ai sistemi di IA che sono componenti di "sistemi IT su larga scala" come istituiti dagli atti giuridici elencati nell'Allegato IX, che siano stati immessi sul mercato o messi in servizio in un periodo antecedente alla futura entrata in vigore del regolamento. L'Allegato IX elenca la legislazione dell'Unione nei seguenti 7 settori: Sistema di informazione Schengen; Sistema di informazione visti; Eurodac; Sistema di ingressi/uscite; Sistema europeo di informazione e autorizzazione ai viaggi; Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi; Interoperabilità.

Complessivamente, la Bozza di Regolamento sembra andare nella direzione di una strumentazione di c.d. *public enforcement* complementare a (e separata da) quella di c.d. *private enforcement* attinente al diverso tema della responsabilità civile per i danni causati da sistemi di IA. Quest'ultimo tema ha formato oggetto di specifica e separata considerazione da parte del Parlamento europeo in studi e progetti normativi (v. in particolare il già richiamato *Draft report* del 27 aprile 2020 della commissione giuridica del Parlamento europeo "JURI" sulla responsabilità civile, su cui la notizia n.3 del numero 2/2020 in questa Rubrica http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf; lo studio pubblicato dal Parlamento europeo nel luglio 2020 dal titolo "Intelligenza artificiale e responsabilità civile", su cui la notizia n.5 del numero 3/2020 in questa Rubrica http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf) culminati nella ricordata 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)), 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 (su cui la notizia n. 1 del numero 4/2020 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf).

SALVATORE ORLANDO

https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

2. *Il comunicato del 23.04.2021 dello* European Data Protection Supervisor *sulla proposta dell'*Artificial Intelligence Act *in particolare sul riconoscimento facciale.*

Il 23 aprile 2021 il Garante europeo della protezione dei dati ("*European Data Protection Supervisor*" o "**EDPS**") ha rilasciato un comunicato stampa con cui ha commentato la proposta di regolamento europeo per l'Intelligenza Artificiale ("*Artificial Intelligence Act*") presentata dalla Commissione europea il 21 aprile 2021, su cui v. la notizia *sub* n. 1 *supra* in questa Rubrica.

Wojciech Wiewiórowski, presidente dell'EDPS, si è dichiarato orgoglioso dell'iniziativa e particolarmente favorevole all'approccio "*risk-based*" su cui si fonda la proposta, in quanto questo permetterebbe di sfruttare i benefici derivanti da numerosi sistemi di intelligenza artificiale che presentano un rischio minimo per il diritto alla privacy e alla protezione dei dati personali dei cittadini.

Tuttavia, il Garante europeo ha criticato l'approccio adottato dalla Commissione con

riferimento all'utilizzo dei sistemi di identificazione biometrica a distanza – compreso il riconoscimento facciale – in spazi accessibili al pubblico, considerato dall'EDPS non sufficientemente rigoroso.

La proposta di regolamento, infatti, pur ponendo in via generale un divieto di utilizzare tali sistemi, ammette alcune eccezioni quando l'utilizzo risulti strettamente necessario per il perseguimento di determinate finalità di ordine pubblico - quali la ricerca di potenziali vittime di reati (es. minori scomparsi), la prevenzione di una minaccia specifica, sostanziale e imminente alla vita di una persona o di un attentato terroristico, l'individuazione, localizzazione, identificazione o perseguimento di una persona sospettata di aver commesso alcuni reati di particolare gravità (es. terrorismo, tratta di esseri umani, pedopornografia, truffa, falsificazione di monete, corruzione). In questi casi – sulla base della proposta di regolamento - il riconoscimento biometrico a distanza potrà essere ammesso all'esito di una specifica valutazione della gravità della situazione e delle conseguenze per i diritti e le libertà dei soggetti coinvolti, in modo proporzionato, temporalmente e geograficamente limitato, e sulla base di una preventiva autorizzazione del giudice (salvo casi di emergenza in cui l'autorizzazione potrà essere successiva). In ogni caso viene rimesso ai singoli Stati decidere se autorizzare queste forme di riconoscimento biometrico, con quali modalità e per quali reati.

Il Garante europeo già in passato aveva manifestato alla Commissione l'esigenza di assumere un atteggiamento restrittivo nei confronti dei sistemi di riconoscimento automatico in spazi accessibili al pubblico delle caratteristiche umane come i volti, l'andatura, le impronte digitali, il DNA, la voce, la digitazione e altri segnali biometrici o comportamentali. Pertanto, nel comunicato stampa in esame il presidente Wiewiórowski si è dichiarato dispiaciuto del fatto che la Commissione si sia discostata dall'indicazione del Garante di introdurre un divieto assoluto all'uso di sistemi identificazione biometrica a distanza e ha ribadito la necessità di adottare un approccio più rigoroso. Tali sistemi, infatti, con lo sviluppo dell'intelligenza artificiale potranno presentare rischi particolarmente elevati di intrusione nella vita privata dei cittadini, in violazione dei principi democratici su cui si fonda l'Unione.

Alla luce di quanto sopra, l'EDPS si è impegnato ad analizzare in maniera approfondita la proposta della Commissione al fine di rafforzare la protezione degli individui e della società nel suo complesso. In particolare, il *Supervisor*, conformemente al suo ruolo istituzionale, provvederà ad individuare i limiti per quegli strumenti che possono rappresentare un rischio per i diritti fondamentali alla privacy e alla protezione dei dati.

CHIARA RAUCCIO

https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

3. Il parere del Garante Privacy del 25.03.2021 sul sistema di riconoscimento facciale SARI Real Time da parte del Ministero dell'Interno

Il 25 marzo 2021 il Garante per la protezione dei dati personali (di seguito anche "Garante privacy" o "Garante") ha espresso il proprio parere in merito all'utilizzo del sistema Sari Real Time da parte del Ministero dell'Interno. Il sistema in esame - ad oggi non in uso – consentirebbe attraverso una serie di telecamere installate in una determinata area geografica di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (c.d. "*watch-list*"), che può contenere fino a 10.000 volti. Qualora, attraverso un algoritmo di riconoscimento facciale, venisse riscontrata una corrispondenza tra un volto presente nella *watch-list* ed un volto ripreso da una delle telecamere, il sistema invierebbe un *alert* agli operatori delle Forze di Polizia. Il sistema è stato progettato e sviluppato come soluzione mobile installabile direttamente presso il luogo dove si rendesse necessario al fine di supportare – e non sostituire – le Forze di Polizia nella gestione dell'ordine e della sicurezza pubblica.

Il Garante ha espresso un parere negativo sull'utilizzo di tale sistema in quanto mancherebbe un'adeguata base giuridica su cui fondare il trattamento di dati personali (come richiesto dagli Artt. 6 e 9 del GDPR). Il sistema, infatti, comporterebbe il trattamento di enormi quantità di dati biometrici che, a seconda dei casi, potrebbero rientrare anche tra le categorie particolari di dati personali (ad esempio, dati idonei a rivelare opinioni politiche, sindacali o religiose nel caso in cui le telecamere venissero installate in occasione di manifestazioni pubbliche). Inoltre, esso non si limiterebbe ad acquisire i dati di soggetti predeterminati come i sospettati di reati, ma finirebbe per raccogliere indiscriminatamente i dati biometrici di tutte le persone presenti nello spazio

monitorato. Si passerebbe così, a giudizio del Garante, da una sorveglianza mirata di alcuni individui alla possibilità di una vera e propria sorveglianza di massa.

Alla luce di ciò, la base giuridica del trattamento difficilmente potrebbe essere rinvenuta nel legittimo interesse del Viminale in quanto l'interesse a garantire la sicurezza nazionale deve essere bilanciato con i diritti e le libertà fondamentali dei soggetti interessati. L'intrusione nella vita privata degli individui coinvolti comporterebbe una sproporzionata e ingiustificata lesione del diritto fondamentale alla privacy e alla protezione dei dati. Conseguentemente, secondo il Garante privacy, un trattamento del genere deve essere necessariamente fondato su una norma di legge che lo autorizzi e lo disciplini in maniera adeguata, tenendo conto di tutti i diritti e le libertà coinvolte e definendo le situazioni e le modalità in cui è possibile l'uso di tali sistemi, senza lasciare una discrezionalità ampia a chi li utilizza. La legge, inoltre, dovrebbe definire i criteri di individuazione dei soggetti che possono essere inseriti nella *watch-list* e stimare le conseguenze in caso di c.d. "falsi positivi". Infine, il Garante segnala l'esigenza di assicurare l'accuratezza dei sistemi e di contrastare il rischio di discriminazione con particolare riguardo alle persone appartenenti a minoranze etniche, le quali potrebbero con maggiore facilità essere erroneamente identificate dagli algoritmi, posto che essi sono notoriamente basati su stime statistiche, "intrinsecamente fallibili", di corrispondenza tra elementi confrontati.

Il Garante ha sottolineato che una norma del genere, ad oggi, non è presente nel nostro ordinamento giuridico e non può essere rinvenuta in nessuna delle fonti normative individuate dal Ministero dell'Interno in materia di pubblica sicurezza e persecuzione dei reati.

CHIARA RAUCCIO

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877

4. Lo studio del 05.02.2021 pubblicato dal Parlamento europeo sulla responsabilità delle piattaforme *online*.

A febbraio 2021 è stato pubblicato lo studio sulla responsabilità delle piattaforme online (*Scientific Foresight Unit* - PE 656.318) commissionato dal *Panel for the Future of Science and Technology* al Centro di Eccellenza Jean Monnet *on the Regulation of Robotics and Artificial Intelligence* della Scuola Sant'Anna di Pisa (lo "**Studio**"). Lo Studio si colloca al centro del dibattito sul crescente rilievo sociale ed economico assunto dalle piattaforme *online* nel corso dell'ultimo decennio. L'incremento del loro impiego nelle operazioni di scambio di beni e servizi, la pervasività nell'accesso e nella diffusione di informazioni non permettono più di ignorare il problema legato al controllo che le piattaforme possono o, in taluni casi, devono esercitare sui contenuti ospitati (*hosting*). Esperienze recenti hanno difatti dimostrato come il loro utilizzo agevoli attività illegali di varia natura e dia, di conseguenza, luogo a nuove forme di vulnerabilità: diffusione di contenuti offensivi, pirateria *online*, *hate speech* e disinformazione, violazioni delle norme sul *copyright* e sulla tutela dei minori, *data protection breach*, incitamento al terrorismo. Più intensa si è pertanto fatta l'esigenza di una risposta unitaria in termini di regolazione per definire il ruolo di prevenzione e la responsabilità che le piattaforme assumono per le attività realizzate attraverso di esse. La prima sezione dello Studio muove dalla valutazione dell'attuale contesto normativo, con particolare riferimento alla Direttiva e-commerce e alle eccezioni che essa dispone nei riguardi della responsabilità delle piattaforme. Dall'analisi compiuta ad ampio raggio sulle fonti di *hard* e di *soft law*, emergono alcune coordinate dalle quali lo Studio suggerisce di muovere per regolare questo fenomeno. Da un lato, la scelta, condivisa dagli autori dello Studio, di non adottare un approccio *one-size-fits-all*. Viene osservato come lo stesso Parlamento Europeo abbia riconosciuto, attraverso la Risoluzione del 2017 *«l'estrema difficoltà di concordare a livello di UE un'unica definizione di piattaforme online che sia giuridicamente pertinente e adeguata alle esigenze future, a causa di fattori quali la grande varietà di tipi delle piattaforme online esistenti e dei loro settori di attività nonché del mondo digitale in rapido cambiamento»* (Risoluzione del Parlamento europeo del 15 giugno 2017 sulle piattaforme online e il mercato unico digitale (2016/2276(INI)), paragrafo 6*:* https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_IT.html). Dall'altro lato, viene evidenziata l'esigenza di non rinunciare a definire alcune classi di riferimento all'interno delle quali inquadrare l'economia delle piattaforme. Nello Studio si nota come il quadro normativo attuale contenga un'ampia serie di definizioni specifiche per singoli segmenti di regolazione, raramente comunicanti e di difficile coordinamento fra loro. La proposta dello Studio è dunque quella di abbandonare un proposito di codificazione di una

law of platform, adottando invece una prospettiva funzionale di classificazione *case-by-case* delle diverse strutture digitali. Questa tassonomia fa comunque riferimento ad una identificazione a monte della nozione di *online platform* come entità che *«(i) offer (primarily) OTT digital services or infrastructures to users, (ii) are or can be operated as a two- or multi-sided market business model, but may choose not to do so, and (iii) allow the overall facilitation of interaction of the different sides of the market, even when there is no direct interaction among them»* (Studio, p. 16). Su questa base, lo Studio propone una mappatura di diverse categorie di piattaforme sulla base delle attività svolte, del settore di rilevanza, delle modalità di utilizzo dei dati, degli attori coinvolti, della fonte dei proventi e del livello di controllo sui contenuti. La seconda sezione dello Studio approfondisce l'analisi della responsabilità legale delle piattaforme e formula alcune *policy options* a disposizione del Parlamento, sconsigliando un mantenimento inalterato dello *status quo*. Le proposte muovono dalla considerazione di criteri differenti (analisi costi-benefici, sostenibilità, coerenza con gli obiettivi dell'Unione, impatto etico e sociale, etc.) e dal grado progressivo di pervasività della regolazione. Il gruppo di ricerca suggerisce inoltre l'adozione di due approcci complementari: l'uno, volto a considerare la regolazione della responsabilità delle piattaforme come parte di una strategia più ampia di creazione di un ambiente digitale sicuro; l'altro, diretto a costruire un regime *technology specific*, formato da strumenti atti a porre rimedio a specifiche violazioni da parte di piattaforme con precise caratteristiche. La prima proposta consiste nella diffusione di iniziative volte al rafforzamento della consapevolezza e dell'educazione degli utenti di servizi di piattaforme *online* sulle potenzialità lesive derivanti da un loro utilizzo. Viene tuttavia osservato che questa misura, se non coordinata con altre più incisive, rischia di risultare estremamente inefficiente, poiché la sola informazione ha una capacità di impatto del tutto marginale per gli utenti e non è dunque in grado di indirizzare le scelte verso piattaforme che mantengano *standard* più elevati di tutela. Una seconda proposta attribuisce alle autorità europee un ruolo di incentivo alla *self regulation* delle piattaforme, attraverso *voluntary committments*. Lo Studio osserva che questi meccanismi hanno l'indubbio vantaggio di coinvolgere i grandi *players* nella definizione delle regole e nella ricerca di soluzioni condivise, ma scontano il problema del non necessario allineamento fra interessi pubblici e privati. Si nota anche che l'autoregolazione viene di frequente formulata attraverso impegni generici e con obiettivi non ben definiti, ostacolandone così l'*enforcement*. La terza proposta suggerisce dunque di stabilire un regime di co-regolazione fra soggetto pubblico e attori privati. Secondo questo modello, le autorità pubbliche svolgerebbero delle funzioni di supervisione più penetrante sul rispetto delle pratiche di autoregolazione delle piattaforme, favorendo la creazione di *sandboxes* per testare alcune soluzioni più innovative (come l'utilizzo degli algoritmi per la identificazione degli *hate speeches*). L'ultima proposta è quella che riconosce infine il ruolo più pervasivo della regolazione europea. Due sono in particolare gli obiettivi identificati nello Studio. Il primo è quello di introdurre specifici obblighi primari in capo alle piattaforme nel *design* delle proprie infrastrutture e nel monitoraggio sui contenuti. Le piattaforme sarebbero, ad esempio, obbligate ad attività di *reporting* standardizzato sulle modalità con le quali hanno svolto il monitoraggio, all'adozione di filtri automatici e sistemi di riconoscimento di contenuti inappropriati, ad obblighi di *compliance* sulla neutralità dei processi e sulla diversificazione dei servizi. Il secondo è quello di definire un regime uniforme di responsabilità, sulla base di due possibili modelli. Una prima via consisterebbe nell'adattamento della disciplina introdotta dalla Direttiva E-Commerce, per come interpretata e applicata nel corso degli anni dalla Corte di Giustizia Europea. Questa soluzione garantirebbe un grado elevato di certezza, ove accompagnata da opportuni chiarimenti, quali la distinzione fra "*specific content monitoring obligations*" e "*general duty of care*" della piattaforma. Una via ulteriore passerebbe invece dall'armonizzazione, a livello europeo, di alcune delle condizioni per ritenere la piattaforma responsabile per i contenuti e le condotte degli utenti. È il caso, ad esempio, della responsabilità per danni, ove la piattaforma sia rimasta inerte nonostante sussistessero prove evidenti di una condotta illecita perpetrata attraverso di essa, o ancora, di forme di responsabilità in specifici settori, come quello della vendita di prodotti nocivi. Questa linea di *policy*, anche in via complementare rispetto ad altre opzioni suggerite nello studio, avrebbe il merito di garantire un livello più elevato di tutela degli utenti, assicurando allo stesso tempo il *level playing field* fra gli operatori.

FEDERICO PISTELLI

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf

5. I *Final Reports* del marzo 2021 del gruppo di esperti dell'Osservatorio sulla *platform economy*.

L'*Observatory for the Online Platform Economy*, costituito dalla Commissione Europea per studiare il fenomeno delle piattaforme digitali e per fornire una consulenza sulla *digital strategy* europea (vedi notizia 4 in questa Rubrica nel numero 3/2020), ha pubblicato cinque *reports* a conclusione del suo primo mandato. Ciascuno di essi corrisponde ad un preciso *workstream*, che il Gruppo di Esperti ha preso a riferimento per affrontare ad ampio raggio lo studio dell'economia delle piattaforme digitali: l'individuazione di parametri econometrici per misurare adeguatamente il mercato, il problema del trattamento differenziato degli utenti, l'utilizzo dei dati nell'ecosistema digitale ed il profilo del potere delle piattaforme. Quest'ultimo, in particolare, nasce con l'obiettivo di definire la posizione di potere (*power*) che contraddistingue il funzionamento dell'economia delle piattaforme digitali, rendendolo un unicum rispetto a fenomeni apparentemente analoghi di dominazione di un'impresa sul mercato. La posizione di potere che connota le piattaforme *online* non è difatti inquadrabile unicamente secondo i canoni tradizionali del *market power*, poiché il controllo viene esercitato su scala molto più ampia. Esso non si limita all'assoggettamento economico degli utenti del servizio, ma si estende sulla collettività, influenzando i comportamenti di consumatori, professionisti, individui e, in ultima analisi, della società nel suo insieme. L'emergenza da COVID-19 ha determinato un aumento esponenziale del volume di attività realizzate attraverso piattaforme *online*, dal commercio di beni sui *marketplaces*, all'ingegneria dei trasporti, fino alle iniziative legate alla cultura, all'educazione scolastica e alla tutela sanitaria. Il *report* struttura l'analisi in due sezioni, nelle quali si dà prima conto delle diverse fonti e delle tipologie di potere esercitato delle piattaforme, per poi concludere in ordine agli aspetti che meritano particolare attenzione.

In particolare, il Gruppo di Esperti individua tre circostanze che definiscono l'unicità del potere esercitato dalle piattaforme. In primo luogo, esse assumono la posizione di *gatekeeper*, ossia di necessario *trading partner* per la collocazione di specifici prodotti sul mercato. Se, ad esempio, lo sviluppatore di un'app vuole rendere disponibile il *software* su iPhone deve interfacciarsi con la piattaforma App Store, che diviene, al tempo stesso, controparte e regolatore privato della transazione. In secondo luogo, il *business* delle piattaforme digitali si basa su strategie *"*darwiniane*"* di sopravvivenza, che richiedono l'eliminazione sistematica della concorrenza come *step* fondamentale nella crescita e nell'assunzione di una posizione di dominio sul mercato. Lo sfruttamento dell'economia di scala e del cosiddetto *network effect* si fondano difatti su di un meccanismo per cui maggiore è il numero di utenti della piattaforma, migliore è la qualità e l'ampiezza dei servizi offerti (come nel caso delle applicazioni di messaggistica o di *marketplace*). Ciò implica che il successo dei propri modelli di sviluppo dipende in gran parte da strategie di acquisizione anticipata dei concorrenti, dalla sottrazione di clientela ai *competitors* e dall'imposizione di barriere e restrizioni all'ingresso sul mercato. Questo aspetto compromette significativamente il regime di concorrenza sul mercato interno, aumentando i costi pagati dagli utenti per la migrazione verso *providers* di servizi analoghi (cd. *switching costs*), quali la perdita di crediti reputazionali o di altri benefici legati alla continuità d'uso. Consenso unanime è, però, quello attorno all'elemento ritenuto determinante nella definizione della posizione di potere delle piattaforme: il possesso e l'elaborazione di *big data*. Le piattaforme digitali hanno difatti accesso ad un'ampia porzione di dati generati dalle singole transazioni, anche di proprietà di soggetti che non ne hanno consentito direttamente la diffusione – secondo un fenomeno che viene definito in linguaggio economico *data externalities*. Il possesso di questi dati, unito alla loro elaborazione per mezzo delle tecniche di *machine learning*, consente alla piattaforma di sviluppare servizi e offrire prodotti basandosi sulla conoscenza delle preferenze degli utenti e sulla predizione dei loro bisogni futuri. Questi processi consentono pertanto di approfittare dei vantaggi dell'economia di scopo, sfruttando i medesimi fattori produttivi per la diversificazione della propria offerta. In ottica di teoria economica e regolazione, la conclusione del Gruppo di Esperti è netta*:* occorre ripensare ai presupposti che fino ad oggi hanno informato la disciplina normativa sulla nozione di "mercato". Essa non è più in grado di ricomprendere l'intero ambito di attività coperte dalle piattaforme digitali, non più distinguibili su base territoriale e per comparti industriali. La soluzione proposta è quella di muovere dunque verso una nozione di "ecosistema", da intendersi come un insieme di prodotti e servizi compatibili fra loro e in grado di esaltare le reciproche caratteristiche all'interno di un ambiente digitale (*es.* "*Apple ecosystem*", "*Google ecosystem*"). L'attuale contesto normativo pare, secondo l'analisi

del Gruppo di Esperti, eccessivamente incentrato sulla promozione del requisito di trasparenza, mentre minor attenzione è dedicata al contrasto a pratiche che possono risultare lesive di utenti professionisti e consumatori. In particolare, occorre chiarire il legame che sussiste fra la regolazione *ex ante* e la disciplina della concorrenza, come ambiti che non devono mirare a sovrapporsi, ma ad integrarsi fra loro. Il *report* analizza, da ultimo, il crescente ruolo assunto dalle piattaforme come intermediario fra sfera pubblica e sfera privata. Rispetto ai mass media tradizionali, le piattaforme detengono oggi il cosiddetto *opinion power*, in quanto si presentano come canali privilegiati di una comunicazione di massa fondata su di un uso dei dati e degli algoritmi in funzione di attrazione del consenso. Le piattaforme sono così in grado di definire le agende dell'azione politica, attribuendo visibilità a specifiche tematiche e figure. Gli stessi attori politici non necessitano più del filtro dei mezzi di comunicazione di massa, potendo interagire direttamente con il proprio elettorato attraverso i *social networks* e sono assistiti dagli stessi nella costruzione di campagne elettorali attraverso messaggi targettizzati a specifiche fasce di pubblico. La regolazione si è fin d'ora mossa verso l'attribuzione alle piattaforme di compiti di moderazione del dibattito, portando all'effetto paradossale per cui si riconosce - in definitiva - alle stesse il ruolo di garante della comunicazione *online*. La conclusione raggiunta dal Gruppo di Esperti è l'invito ad approfondire la comprensione di questo fenomeno, non soffermandosi unicamente sugli aspetti di carattere economico, ma analizzandoli in tutta la loro complessità. L'impatto dell'economia delle piattaforme su alcuni aspetti di rilievo centrale nelle politiche dell'Unione, come l'innovazione, la tutela della salute, la democrazia rendono questo fenomeno di prioritaria importanza all'interno dell'agenda europea.

FEDERICO PISTELLI

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=73962

6. Il Parere della BCE del 19.02.2021 sulla Proposta di Regolamento sui mercati di crypto-assets.

Il 19 febbraio 2021, la Banca Centrale Europea ("**BCE**") ha emanato un parere, ai sensi degli articoli 127, paragrafo 4, e 282, paragrafo 5, del Trattato sul Funzionamento dell'Unione Europea (TFUE), sulla proposta del 24 settembre 2020 della Commissione europea (COM(2020) 593 final-2020/0265(COD)) di un regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività, volto a modificare la direttiva UE 2019/1937 (sulla quale v. notizia 2 nel numero 4/2020 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf).

Nonostante la BCE abbia accolto con favore l'iniziativa della Commissione europea di istituire un quadro armonizzato a livello europeo per le cripto-attività, al fine di evitare la frammentazione all'interno del mercato unico, permangono tuttavia, secondo la medesima BCE, alcuni aspetti della Proposta che necessitano di ulteriori approfondimenti e azioni correttive.

In particolare, la BCE sottolinea come, ai sensi della suddetta proposta (la "**Proposta**"), le cripto-attività (*rectius*, le due sotto-categorie dei *token* collegati ad attività e dei *token* di moneta elettronica) abbiano una evidente dimensione di sostituzione monetaria, alla luce delle tre funzioni a cui la moneta tradizionale deve assolvere: (i) mezzo di scambio, (ii) riserva di valore e (iii) unità di conto. A tal riguardo, la BCE rileva come sussista il rischio che, in considerazione dell'utilizzo concreto dei *token* collegati ad attività e dei *token* di moneta elettronica e dell'importanza sistemica che potrebbero acquisire, questi possano essere *de facto* equiparati agli strumenti di pagamento, indipendentemente dalla loro presunta funzione o applicazione principale ai sensi della Proposta. Ad avviso della BCE, al fine di prevenire il rischio di arbitraggio normativo tra i regimi applicabili ai *token* collegati ad attività e ai *token* di moneta elettronica, occorrerebbe sottoporre entrambi a requisiti analoghi e, in particolare, con riferimento ai *token* collegati ad attività, (i) imporre agli emittenti di concedere ai possessori di tali *token* diritti di rimborso sull'emittente o sulle attività di riserva, (ii) procedere alla creazione di una nuova categoria di «*token* di pagamento» volta ad assoggettare tali *token* a un insieme di requisiti identici a quelli applicabili agli emittenti di *token* di moneta elettronica e (iii) nel caso di *token* collegati ad attività significativi, ampiamente utilizzati per i pagamenti all'interno dell'Unione Europea, assoggettare gli emittenti di tali *token* significativi agli stessi requisiti di autorizzazione applicabili agli emittenti di *token* di moneta elettronica.

Inoltre, la Proposta prevede che un'autorità competente possa rifiutare l'autorizzazione a un emittente di *token* collegati ad attività, tra l'altro, qualora il modello imprenditoriale dell'emittente possa costituire una grave minaccia per la stabilità finanziaria, la trasmissione della politica monetaria

o la sovranità monetaria. La BCE osserva inoltre che, qualora un dispositivo collegato ad attività fosse equiparato a un sistema o a uno schema di pagamento, la valutazione ai fini della concessione dell'autorizzazione dovrebbe rientrare nella competenza esclusiva della BCE e, a tal fine, sottolinea come il suo intervento dovrebbe tradursi nell'emissione di un parere vincolante.

In merito alla sorveglianza sui sistemi di compensazione e di pagamento, la BCE ritiene che la funzione dei dispositivi relativi ai *token* collegati ad attività e ai *token* di moneta elettronica che servono all'esecuzione di ordini di trasferimento può essere equiparata a quella di un «sistema di pagamento» qualora tale funzione presenti tutti gli elementi tipici di un sistema di pagamento, precisamente: a) un accordo formale; b) almeno tre partecipanti diretti; c) processi e procedure, secondo le regole del sistema, comuni per tutte le categorie di partecipanti; d) l'esecuzione degli ordini di trasferimento all'interno del sistema e comprendente l'avvio del regolamento e/o l'adempimento di un'obbligazione e quindi avente un effetto giuridico sugli obblighi dei partecipanti; e e) ordini di trasferimento eseguiti tra i partecipanti. All'uopo, la BCE precisa che, nella misura in cui i dispositivi relativi ai *token* collegati ad attività e ai *token* di moneta elettronica e i dispositivi che stabiliscono norme comuni per l'esecuzione delle operazioni di pagamento tra utenti finali, siano considerati «sistemi di pagamento», ad essi si applicherebbe il quadro di sorveglianza dei sistemi di pagamento dell'Eurosistema basato sui principi per le infrastrutture dei mercati finanziari emanati dal *Committee on Payment and Settlement* Systems e dall'*International Organization of Securities Commissions*.

Per quanto concerne i profili di vigilanza prudenziale, la BCE rileva come la Proposta preveda un trattamento differente tra gli emittenti di *token* di moneta elettronica significativi e gli emittenti di *token* collegati ad attività significativi. In particolare, i primi sarebbero soggetti ad un duplice sistema di vigilanza costituito dall'*European Banking Authority* (EBA) e dall'autorità nazionale competente, mentre gli altri soltanto alla vigilanza dell'EBA. Tale approccio potrebbe comportare incongruenze e duplicazioni dei compiti di vigilanza tra le autorità coinvolte che potrebbero addirittura sfociare in misure confliggenti adottate dai regolatori coinvolti.

EUGENIO PROSPERI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021AB0004&from=IT

7. Il comunicato di Consob e Banca d'Italia sui crypto-assets del 28.04.2021.

Il 28 aprile 2021, in considerazione dell'assenza di un quadro normativo unitario in ambito europeo, la Commissione Nazionale per le Società e la Borsa (Consob) e la Banca d'Italia (le "**Autorità**"), congiuntamente, hanno rilasciato un comunicato stampa, mediante il quale hanno inteso rappresentare gli elevati rischi connessi con l'operatività in cripto-attività (*crypto-asset*), rivolgendosi in particolare ai piccoli risparmiatori (il "**Comunicato**").

Il Comunicato si è reso necessario stante il riscontrato interesse crescente della collettività, a livello europeo e internazionale, nei confronti delle cripto-attività. A tal riguardo, le Autorità hanno rilevato come, data l'assenza di un quadro regolamentare di riferimento, l'operatività in cripto-attività presenti determinati rischi che comprendono, *inter alia*, (i) la scarsa disponibilità di informazioni in merito alle modalità di determinazione dei prezzi, (ii) la volatilità delle quotazioni, (iii) l'assenza di tutele legali e contrattuali, di obblighi informativi da parte degli operatori e di specifiche forme di supervisione su tali operatori nonché di regole a salvaguardia delle somme impiegate. Inoltre, le Autorità sottolineano la presenza di rischi insiti nella tecnologia applicabile alle cripto-attività quali, ad esempio, la perdita a causa di malfunzionamenti, attacchi informatici o smarrimento delle credenziali di accesso ai portafogli elettronici.

Le Autorità hanno, inoltre, richiamato, la proposta di Regolamento UE per disciplinare l'emissione, l'offerta al pubblico, la prestazione dei servizi e il contrasto agli abusi di mercato in relazione alle diverse tipologie di cripto-attività, su cui la BCE ha rilasciato un parere in data 19 febbraio 2021 (vedi in questa la notizia n. 6 *supra* in questo numero della Rubrica).

In conclusione, le Autorità dando atto della totale non soggezione delle cripto-attività ad alcuna forma di supervisione o di controllo da parte delle autorità di vigilanza, invitano la collettività a prestare particolare attenzione con riferimento a questo tipo di investimenti.

EUGENIO PROSPERI

https://www.consob.it/web/consob/dettaglio-news/-/asset_publisher/hZ774IBO5XPe/content/comunicato-stampa-consob-banca-d-italia-del-28-aprile-2021/10194

8. La sentenza 2631 del Consiglio di Stato del 29.03.2021 nel caso Facebook (gratuità del servizio e divieto di pratiche commerciali scorrette).

La pronuncia del Consiglio di Stato, Sez. VI n. 2631 del 29 marzo 2021 conferma la sentenza del Tribunale amministrativo regionale per il Lazio, Sez. I, 10 gennaio 2020 n. 260 con la quale è stato parzialmente accolto il ricorso proposto dalla società Facebook Ireland Limited ("**FB**") nei confronti del provvedimento dell'Autorità garante della concorrenza e del mercato n. 27432 del 29 novembre 2018 (il "**Provvedimento**").

Con il Provvedimento, l'Autorità garante della concorrenza e del mercato ("**AGCM**") aveva contestato a FB due distinte pratiche commerciali scorrette in violazione degli artt. 20, 21, 22, 24 e 25 d.lgs. 6 settembre 2005, n. 206 (cd. "**Codice del consumo**"):

- la "Pratica a)-pratica ingannevole" consisteva nelle "*violazione degli artt. 20, 21 e 22 del Codice del consumo",* in quanto l'Autorità aveva rilevato che "*Sino al 15 aprile 2018, l'utente che accedeva alla homepage di FB per registrarsi sulla Piattaforma (sito web e app), a fronte di un* claim *sulla gratuità del servizio offerto "Iscriviti E' gratis e lo sarà per sempre", non trovava un altrettanto evidente e chiaro richiamo sulla raccolta e uso a fini commerciali dei propri dati da parte di FB*";

- la "Pratica b)-pratica aggressiva" si riferiva alla "*violazione degli artt. 20, 24 e 25 del Codice del consumo, in quanto il professionista eserciterebbe un indebito condizionamento nei confronti dei consumatori registrati, i quali, in cambio dell'utilizzo di FB, verrebbero costretti a consentire a FB/terzi la raccolta e l'utilizzo, per finalità informative e/o commerciali, dei dati che li riguardano (informazioni del proprio profilo FB, quelle derivanti dall'uso di FB e dalle proprie esperienze su siti e app di terzi), in modo inconsapevole e automatico, tramite un sistema di preselezione del consenso alla cessione e utilizzo dei dati, risultando indotti a mantenere attivo il trasferimento e l'uso dei propri dati da/a terzi operatori, per evitare di subire limitazioni nell'utilizzo del servizio, conseguenti alla deselezione*".

Il TAR per il Lazio, con la sentenza n. 260/2020 e quella gemella n. 261/2020 emessa in pari data, aveva respinto le censure edotte da FB con riferimento alla parte del Provvedimento riferita alla "Pratica a" (pratica ingannevole), confermando le sanzioni inflitte dall'AGCM (sul punto v. la notizia n. 4 sul numero 1/2020 di questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf); diversamente aveva accolto il ricorso proposto da FB con riferimento a quella parte del Provvedimento riferita al comportamento indicato come "Pratica b" (pratica aggressiva).

Nei confronti della sentenza del TAR per il Lazio 260/2020 hanno proposto appello sia FB (nella parte in cui la sentenza ha respinto l'impugnazione proposta da FB, con riferimento alla Pratica a), ossia la pratica ingannevole), sia l'AGCM (nella parte in cui la sentenza ha accolto l'impugnazione proposta in primo grado da FB, con riferimento alla Pratica b), ossia la pratica aggressiva).

Il Consiglio di Stato, con riferimento all'appello proposto da FB ha affermato che – seppure si volesse aderire alla tesi della parte appellante secondo cui il dato personale sarebbe una *res extra commercium* - tale impostazione non sarebbe in ogni caso di ostacolo all'applicazione della disciplina consumeristica e neanche renderebbe esclusivamente applicabile, in quanto normativa speciale, il GDPR. Infatti, in primo luogo, il Collegio afferma che nonostante la tesi per la quale i dati personali sarebbero una *res extra commercium*, è evidente che qui essi hanno subito una "patrimonializzazione" da parte di FB**.** E tale patrimonializzazione avviene all'insaputa dell'utente che è persuaso di iscriversi gratuitamente alla piattaforma, mentre invece i suoi dati vengono impiegati per effettuare una profilazione a fini commerciali. In secondo luogo, secondo il Collegio, l'ambito operativo della disciplina speciale costituita dal GDPR non è assoluto e non esclude – come sostenuto da FB - l'applicazione di altre discipline, quale il Codice del Consumo, dovendosi piuttosto ricavare dall'interpretazione dello stesso GDPR (e del suo Considerando 9 in particolare) l'«*esigenza di garantire "tutele multilivello"*». Conseguentemente il Consiglio di Stato ha respinto l'appello proposto da FB.

Il Consiglio di Stato, inoltre, con riferimento all'appello proposto dall'AGCM ha affermato che la "pre-attivazione" della piattaforma FB (vale a dire la "preselezione" delle opzioni a disposizione) non solo non comporta alcuna trasmissione di dati in modo diretto ed immediato dalla piattaforma FB a quella di soggetti terzi, ma è seguita da una ulteriore serie di passaggi necessitati, in cui l'utente

è chiamato a decidere se e quali dei suoi dati intende condividere al fine di consentire l'integrazione tra le piattaforme. Conseguentemente, il Consiglio di Stato ha respinto anche l'appello proposto dall'AGCM.

MARISTELLA GIANNINI

https://www.giustizia-amministrativa.it/web/guest/provvedimenti-cds

9. La comunicazione di addebiti del 30.04.2021 della Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in *streaming* su App Store.

Il 30 aprile 2021 la Commissione Europea ha pubblicato una comunicazione di addebiti ("*Statement of Objections*") contro Apple, sostenendo che la società americana ha abusato della sua posizione dominante, *ex* articolo 102 TFUE, nel mercato della distribuzione di applicazioni di streaming musicale. In base alle risultanze preliminari acquisite dalla Commissione, Apple ha una posizione dominante ed è un *gatekeeper* per gli utenti di iPhone e iPad attraverso la propria piattaforma online di distribuzione di app, l'App Store, in quanto per gli sviluppatori di app, l'App Store è la sola porta di accesso ai consumatori che usano *smart mobile devices* che utilizzano il sistema operativo iOS di Apple. La Commissione ha rilevato innanzitutto la criticità delle regole che prevedono l'uso obbligatorio del meccanismo di acquisto in-app di Apple imposto agli sviluppatori di applicazioni di *streaming* musicale per la distribuzione delle loro applicazioni attraverso l'App Store. Inoltre, secondo gli addebiti, Apple imposterebbe regole (di natura contrattuale e di design informatico) rigide e più onerose nell'App Store a svantaggio dei concorrenti, con ciò privando i consumatori finali di informazioni che consentirebbero loro di operare scelte di *streaming* musicale più economiche, e, quindi, distorcendo la concorrenza.

Lo *Statement of Objections* riguarda l'applicazione di queste regole a tutte le applicazioni di *streaming* musicale che competono con la applicazione di *streaming* musicale di Apple "Apple Music" nello Spazio Economico Europeo (SEE).

La comunicazione di addebiti segue un'indagine già avviata dalla Commissione europea e una denuncia di Spotify. In particolare, il 16 giugno 2020, la Commissione europea, nella veste di regolatore europeo della concorrenza e del mercato, ha aperto un'indagine sulle condizioni dell'App Store di Apple praticate nei confronti degli sviluppatori di app di *streaming* di musica. Ciò seguiva alla denuncia sporta l'anno precedente da parte del fornitore di musica in *streaming* Spotify, concorrente di Apple Music, attraverso la quale veniva richiesto l'intervento del regolatore per ristabilire una situazione di libera concorrenza nel mercato europeo dei servizi di *streaming* musicale. A questa denuncia, in data 5 marzo 2020, si aggiungeva quella di un distributore di e-book e audiolibri, il quale sollevava le medesime questioni in relazione all'app di distribuzione *online*, Apple Books. Veniva richiesto alla Commissione europea di valutare se le condizioni applicate da Apple nei contratti di licenza con gli sviluppatori di app, in merito alla distribuzione di queste attraverso l'App Store, e l'imposizione dell'uso del sistema proprietario di acquisti in-app di Apple (*in-app purchase:* "IAP"), limitassero in maniera anticoncorrenziale la possibilità per gli sviluppatori di informare gli utenti di iPhone e iPad delle opportunità alternative di fruizione dei medesimi servizi al di fuori della piattaforma di Apple. Questo perché gli utenti di iPhone e iPad possono scaricare applicazioni che non si trovano sul web solo attraverso l'App Store.

In dettaglio, le disposizioni esaminate dal regolatore nei contratti di licenza impongono, in primo luogo, l'uso del sistema IAP per la distribuzione di contenuti digitali a pagamento, attraverso cui Apple addebita agli sviluppatori di app una commissione del 30% su tutti gli abbonamenti venduti tramite la piattaforma. La Commissione ha verificato che la maggior parte dei fornitori di musica in *streaming* ha "trasferito" questa commissione agli utenti finali, aumentando i prezzi.

In secondo luogo, l'obbligo di usare il sistema IAP darebbe ad Apple il pieno controllo sul rapporto con i clienti dei concorrenti di Apple Music nella fornitura di *streaming* di musica, nonché la possibilità di raccogliere dati sulle attività e le offerte distribuite tramite l'App Store dai medesimi.

Inoltre, mentre Apple permette ai propri utenti di utilizzare servizi digitali in abbonamento acquistati altrove, al di fuori dell'App Store (ad esempio accedendo a contenuti di musica, e-book e audiolibri direttamente dal sito web dello sviluppatore dell'app), le sue condizioni contrattuali impediscono agli sviluppatori di app di informare gli utenti dei dispositivi Apple, iPhone e iPad, di queste possibilità alternative, che di solito sono più economiche (c.d. "*anti-steering provisions*").

Gli addebiti sono basati su risultanze e convincimenti preliminari, come allo stato acquisiti e formati dalla Commissione europea. L'invio di una comunicazione degli addebiti consente ad Apple di presentare le proprie osservazioni e difese dinanzi alla Commissione e non condiziona l'esito delle successive indagini e di un eventuale successivo contenzioso.

DOMENICO PIERS DE MARTINO

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2061?fbclid=IwAR3j2jP92hYsaCQpdVGC20nTcolJUgbcix0l20eFHeZvCKG-Prrt3b10Srk

10. *Fair use* e *open source*: la decisione della Corte Suprema degli Stati Uniti d'America del 05.04.2021 nel caso della API di Java (Oracle c/ Google).

Il 5 aprile 2021 la Corte Suprema americana ha deciso l'annosa controversia *Google Llc v. Oracle America, Inc.*, che ha avuto inizio più di 10 anni fa dinanzi alla Corte distrettuale di San Francisco.

La questione giuridica ha seguito il processo di creazione del sistema operativo Android di Google. Infatti, durante la fase genetica del nuovo sistema operativo, Google ha utilizzato oltre 11 mila linee di codice scritto in Java, contenente varie API («*Application Programming Interface*»), al fine di velocizzare il processo di implementazione e sviluppo delle applicazioni. I codici erano stati inizialmente generati dalla società Sun Microsystem, acquistata nel 2009 da Oracle che è diventata titolare di tutti i diritti d'autore sulla piattaforma Java.

Dopo il primo grado di giudizio dinanzi alla Corte distrettuale di San Francisco che aveva respinto le istanze di Oracle, nel 2018 la Corte d'Appello ha accolto la richiesta di risarcimento, considerando l'utilizzo delle linee di codice un uso illegittimo in violazione del diritto d'autore spettante a Oracle.

Google ha, quindi, formulato un c.d. «*writ of certiorari*», rimettendo la controversia dinanzi alla Corte Suprema per la sua decisione. La richiesta di Google ha proposto due questioni. La prima, se le API di Java sono «*copyrightable*». La seconda, se l'uso da parte di Google è stato un «*fair use*». La Corte ha deciso di rispondere soltanto alla seconda domanda, in quanto in ogni caso risolutiva ove anche dovesse assumersi una risposta affermativa alla prima (e più impegnativa) questione, alla quale pertanto la Corte non ha risposto, ma la cui risposta affermativa ha presupposto per pura ipotesi al fine di affrontare la seconda questione. Interessante come la Corte, per motivare questa scelta, abbia fatto riferimento al contesto tecnologico, economico ed imprenditoriale in rapido cambiamento: «*Given the rapidly changing technological, economic, and business-related circumstances, we believe we should not answer more than is necessary to resolve the parties' dispute. We shall assume, but purely for argument's sake, that the entire Sun Java API falls within the definition of that which can be copyrighted. We shall ask instead whether Google's use of part of that API was a "fair use"*».

Il tema principale della questione e delle argomentazioni della Corte ha quindi ruotato intorno alla possibilità di considerare l'utilizzo del codice Java compiuto da Google senza la preventiva autorizzazione di Oracle, come una ipotesi di «*fair use*» e, quindi, di uso legittimo di un'opera tutelata (in ipotesi) dal *copyright*.

Il problema consequenziale attiene ai sistemi c.d. «*open source*» (come quello utilizzato da Google con Android) e alla possibilità di applicare le ipotesi derogatorie a favore di questi progetti anche nel caso di colossi del mercato digitale che, grazie a simili strutture operative, riescono ad ottenere notevoli profitti, come, d'altronde, sostenuto da Oracle dinanzi alla Corte.

Bisogna notare che le linee Java "copiate" costituiscono soltanto una piccolissima parte dell'intero codice di programmazione di Android e che, come riportato dalla Corte Suprema, le API «*allow[s] programmers to use … prewritten code to build certain functions into their own programs*», rappresentando, di fatto, un tassello essenziale nello sviluppo della programmazione informatica.

La Corte Suprema, con parere favorevole di sei degli otto giudici, si è espressa a favore di Google, rigettando le richieste risarcitorie di Oracle. La Corte, infatti, ritiene che, sebbene l'uso delle linee di codice Java sia avvenuto senza autorizzazione da parte del titolare dei diritti d'autore, la questione proposta vada a configurare una ipotesi di «*fair use*».

Il principio («*an equitable rule of reason*») è, difatti, volto a mitigare proprio i diritti di esclusiva del titolare del *copyright* e trova riconoscimento all'interno del *Copyright Act* statunitense. Come ribadito dalla Corte nelle sue ricostruzioni, la §107 definisce il perimetro entro cui collocare le ipotesi di uso legittimo di un'opera tutelata dal diritto d'autore. In particolare, nel giudizio di bilanciamento da compiersi è richiesto che l'utilizzo sia trasformativo, ovvero che aggiunga all'opera originaria elementi e scopi nuovi, e che vadano tenuti in considerazione la quantità dell'opera protetta impiegata, lo scopo dell'attività alla base

dell'uso del materiale protetto e l'impatto economico sul titolare dell'opera protetta e sull'utilizzatore della stessa.

Sul punto, la Corte sottolinea che l'utilizzo di codici Java è considerabile come un uso corretto in quanto si inserisce in una attività trasformativa avvenuta in un contesto – quello dei dispositivi mobili – e con modalità del tutto differenti rispetto all'utilizzo originario ed in quanto esso è finalizzato a facilitare le operazioni di programmazione che già sfruttavano le linee dei codici in questione.

La sentenza, invece, come detto, non si esprime in maniera definitiva sulla controversa tutela da offrire ai titolari di *copyright* sui codici di programmazione e sulla possibilità di prevedere una forma di equo compenso nel caso di usi che abbiano generato notevoli vantaggi economici per l'utilizzatore, come nel caso di specie e come evidenziato dal giudice Thomas nella sua *dissenting opinion.*

È indubbio che la portata di questa sentenza possa generare prospettive nuove sia nell'ambito dei sistemi c.d. *open source* sia nel contesto dell'applicazione del principio di *fair use* all'interno dell'ordinamento statunitense, specialmente in relazione ad attività connesse al mercato digitale.

ENZO MARIA INCUTTI

https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf