

ELENA FALLETTI

SOVRANITÀ DIGITALE, TUTELA DELLA SICUREZZA NAZIONALE E LIBERTÀ DI MANIFESTAZIONE DEL PENSIERO: I FATICOSI EQUILIBRI DELLA SENTENZA *TIKTOK V. GARLAND*

SOMMARIO: 1. Stato di diritto, impatto tecnologico e frammentazione geopolitica. — 2. Influenza straniera, interesse nazionale e sovranità digitale. — 3. La valenza del bilanciamento costituzionale tra la protezione della sicurezza nazionale e la libertà di manifestazione del pensiero. — 4. Stati Uniti v. UE: riflessioni comparate sul trattamento massivo dei dati degli utenti raccolti dalle piattaforme digitali.

1. STATO DI DIRITTO, IMPATTO TECNOLOGICO E FRAMMENTAZIONE GEOPOLITICA.

Il potere dello Stato sovrano, caratterizzato dal trinomio “governo-popolo-territorio”¹, sembra essersi indebolito², perdendo l’esclusiva dell’esercizio della sovranità nelle scelte politiche e dell’influenza strategica a causa della concorrenza di altre entità di governance orizzontale, rappresentate soprattutto da attori sovranazionali³, come le “Big Tech Company”⁴. Sono soprattutto queste ultime a incarnare il potere finanziario e tecnologico⁵, la cui influenza concorrente è maggiormente percepibile nella c.d. “Data Litigation”⁶.

* Il commento è alla decisione della Corte Suprema degli Stati Uniti *TikTok Inc., et al. v. Garland*, 604 U. S. ____ (2025) depositata il 17 gennaio 2025.

¹ Per come è stato stereotipato dal “paradigma vestfaliano”, risalente al 1648 (S. D. KRASNER, *Rethinking the sovereign state model*, in *Review of international studies*, 2001, 27(5), 17-42).

² M. R. FERRARESE, *Poteri nuovi. Privati, penetranti, opachi*, Il Mulino, Bologna, 2022, *passim*.

³ H. GU, *Data, big tech, and the new concept of sovereignty*, in *Journal of Chinese political science*, 2023, 1-22.

⁴ C. SAURA GARCÍA, *Datafeudalism: the domination of modern societies by big tech companies*, in *Philosophy & Technology*, 2024, 37(3), 90.

⁵ A. K. WOODS, *Litigating data sovereignty*, in *The Yale Law Journal*, 2018, 328-406.

⁶ K. WÖRLE, O. J. GSTREIN, *Collective Data Protection Litigation: A comparative*

Da tempo ⁷, tecnica ed economia si sono diffuse globalmente, superando i confini degli Stati ⁸ e rendendo così evidente la crisi della sovranità popolare ⁹. Parrebbe infatti che il popolo sovrano preferisca sfogare le proprie frustrazioni polarizzandosi online ¹⁰ invece che esercitando il diritto di voto ¹¹. Si manifestano indizi in tal senso attraverso la crescita dell'astensionismo elettorale ¹², soprattutto in Occidente ¹³.

Paradossalmente, la crisi della sovranità territoriale ha fatto emergere la necessità della difesa della sovranità digitale ¹⁴, al fine di preservare l'integrità delle infrastrutture tecnologiche, senza le quali uno Stato efficiente ed evoluto non sarebbe in grado di esistere. Per esempio, è sufficiente rievocare il periodo pandemico quando, a causa del lockdown, molte attività ¹⁵ come quelle lavorative ed educative, si sono dovute svolgere per mezzo di piattaforme proprietarie straniere ¹⁶. In quell'occasione ci si è resi conto, forse per la prima volta, che tali infrastrutture sono nella esclusiva disponibilità di *Big Tech Company* estere, prevalentemente americane o cinesi.

analysis of EU representative actions and US class actions enforcing data protection rights, in *European Journal of Comparative Law and Governance*, 1(aop), 2024, 1-34.

⁷ J. MOKYR, *Long-Term Economic Growth and the History of Technology*, in P. ACHION, S. N. DURLAUF, (eds), *Handbook of economic growth*, 2005, Elsevier, Vol. 1, 1113-1180.

⁸ N. IRTI, *Tramonto della sovranità e diffusione del potere*, in E. DEL PRATO, *Studi in onore di Antonino Cataudella*, Napoli, ESI, II, 1164.

⁹ J. P. BEETZ, *Saving Popular Sovereignty From a Slow Death in the European Union*, in *JCMS: Journal of Common Market Studies*, 2024, 62(2), 508-524; F. NASI, *The crisis of the democratic imaginary: How anti-democratic imaginaries foster democratic malaise*, in *Communication and Democracy*, 2024, 1-21.

¹⁰ N. KERR, B. A. KING, M. WAHMAN, *The Global Crisis of Trust in Elections. Public Opinion Quarterly*, 2024, 88(SI), 451-471; M. SANTILLÁN-VÁSQUEZ, E. MONARD, *Discursive Practices during an Electoral Cycle: Public Opinion and Political Disillusionment on Twitter*, in *Communication & Society*, 2024, 73-90.

¹¹ H. SCHOLTZ, *Polarization and partitioning representation: how an overlooked aspect of contemporary democracy leads to polarizing societies*, in *Sociology Compass*, 2024, 18(10), e70008.

¹² F. KOSTELKA, S. P. SINCH, A. BLAIS, *Is compulsory voting a solution to low and*

declining turnout? Cross-national evidence since 1945, in *Political Science Research and Methods*, 202412(1), 76-93.

¹³ R. M. MEDEL, *When do active citizens abstain from the polls? Civic associations, non-electoral participation, and voting in 21st-century democracies*, in *Acta Politica*, 2024, 59(1), 220-244; M. HOFFMANN, C. NEUMAYER, *Movement parties on social media between protest and polity arena*, in *Protest and Democracy*, Routledge, 2025, pp. 120-136. Tuttavia, si segnala che le elezioni del Bundestag svoltesi in Germania lo scorso 23 febbraio sono state in controtendenza perché hanno visto un'alta partecipazione degli elettori con un'affluenza del 82,5% di votanti alle urne, in aumento rispetto al 76,4% delle elezioni politiche federali del 2021 (BUNDESWAHLEITERIN, *Pressemitteilung Nr. 27/25*, 24.2.2025).

¹⁴ V. BERTOLA, S. QUINTARELLI, *The Regulated Internet. Europe's Quest for Digital Sovereignty*, Springer, Cham, 2025, *passim*.

¹⁵ E. RISI, R. PRONZATO, G. DI FRAIA, *Living and working confined at home: Boundaries and platforms during the lockdown*, in *Journal of Cultural Analysis and Social Change*, 2020, 5(2), 1-4.

¹⁶ P. ZUDDAS, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio AIC*, 3/2020, 304, n. 83; C. SCOGNAMIGLIO, *Didattica a distanza ed equivoci digitali*, in *MicroMega-online*, 28.4.2020, V. BERTOLA, S. QUINTARELLI, *The Regulated Internet*, cit.

In siffatto contesto, e sulla base di questi presupposti, si è svolta, senza essere ancora giunta a conclusione nel momento in cui si scrive, la controversia giudiziaria che ha visto gli Stati Uniti d'America ¹⁷ contro TikTok, il social network di origine e pas-saporto cinesi ¹⁸.

Come è noto, TikTok è una piattaforma che consente la crea-zione, pubblicazione, visione, condivisione e interazione di video brevi, editati con musica e commenti. Il nome stesso richiama in modo onomatopeico il ticchettio di un orologio, evocando rapidità e diffusione virale dei contenuti, soprattutto tra gli utenti più giovani ¹⁹. Per rendersi conto dell'ampiezza del mercato ameri-cano si consideri che dal 2017, anno di lancio negli Stati Uniti, si sono contati 170 milioni di utenti, i quali nel 2023 hanno caricato 5 miliardi e mezzo di video a loro volta visti 13 trilioni di volte ²⁰.

Seppure operi negli Stati Uniti attraverso una filiale califor-niana, TikTok è affiliata alla società madre cinese ByteDance, che è anche proprietaria dell'algoritmo, a sua volta sviluppato in Cina, secondo la disciplina legislativa cinese, cui ByteDance stessa è soggetta ²¹. Siffatta disciplina richiede che la piattaforma assista ovvero cooperi con il governo cinese nell'attività di intelligence, assicurando l'accesso e il controllo dei dati personali degli utenti raccolti, trattati e conservati ²².

Si tratta di una situazione speculare a quella delle grandi piattaforme americane che raccolgono e trattano i dati di cittadini stranieri e li custodiscono nei loro server sul territorio statuni-tense, sottoponendoli a elaborazioni di *mass surveillance* ²³.

La vicenda che ha dato vita alla controversia è interessante per

¹⁷ S. A. FELIX, *Big Tech Companies' Unprecedented Success and the Abuse of Dominance in the EU and the US: A Comparative Analysis*, in *Southampton Student L. Rev.*, 2022, 12, 137; C. SAURA GARCÍA, *Datafeudalism*, cit.; C. HOEFFLER, F. MÉRAND, *Digital sovereignty, economic ideas, and the struggle over the digital markets act: a political-cultural approach*, in *Journal of European Public Policy*, 2024, 31(8), 2121-2146; C. RIKAP, *The US National Security State and Big Tech: frenemy relations and innovation planning in turbulent times*, in *The Political Economy of War, Peace, and the Military-Industrial Complex*, Edward Elgar Publishing, 2025.

¹⁸ S. D. SCHWINN, *Does the Federal Ban on TikTok, and Application Owned by a Corporation with Significant Ties to China, Violate the First Amendment?*, in 52 *Pre-view U.S. Sup. Ct. Cas.*, Jan. 10, 2025, at 3

¹⁹ C. MCCLAIN, W. DAWSON, *Support for a U.S. TikTok ban continues to decline*,

and half of adults doubt it will happen, Pew Research Center, 5.9.2024; L. WANG, G. STOCKING, S. BESTVATER, R. WIDJAYA, *A Clo-ser Look at Americans' Experiences With News On Tiktok*, *ibidem*.

²⁰ Dati contenuti in *TikTok Inc. et al v Merrick Garland et al.*, 604 U.S. ____ (2025), 2.

²¹ S. YANG, *Research on the Interna-tionalization Strategy of Chinese Internet Enterprises-Taking ByteDance Company as an Example*, in *Advances in Economics, Management and Political Sciences*, 2024, 124, 204-211.

²² A. BERNOT, D. COONEY, O'DONOGHUE, M. MANN, *Governing Chinese technologies: TikTok, foreign interference, and techno-logical sovereignty*, in *Internet Policy Re-view*, 2024, 13(1).

²³ Sul punto la bibliografia è im-po-nente, per brevità si rinvia a S. ZUBOFF, *The Age of Surveillance Capitalism*, New York, 2019, *passim*.

lo scambio di ruoli che investe le autorità americane, che in queste circostanze si trovano a perdere il controllo sui dati dei propri cittadini a favore della Cina, un Paese che considerano un avversario, se non addirittura un potenziale nemico ²⁴.

Inoltre, sebbene l'argomento affrontato in questo contributo abbia una chiara dimensione legale e tecnologica, è inevitabile riconoscerne anche le implicazioni geopolitiche ed economiche. Oltre a ciò, va tenuto a mente che in Cina il trattamento dei dati personali da parte della piattaforma è regolamentato dal *Personal Information Protection Law of the People's Republic of China (PIPL)*, il quale disciplina la raccolta dei dati personali dalle piattaforme e li convoglia su obiettivi governativi molto ampi come la sorveglianza, la tutela della salute e la gestione del "social credit system" ²⁵, riconducibili ai sistemi di *social scoring*, violativi dei diritti fondamentali e stigmatizzati dalla dottrina occidentale ²⁶.

In sintesi, gli interessi in gioco creano una dinamica triangolare. Al primo vertice ci sono gli utenti della piattaforma, che la utilizzano per divertimento o affari, spesso inconsapevoli della raccolta e dell'uso massivo dei loro dati personali. Il secondo vertice è rappresentato dalla piattaforma stessa, che raccoglie e sfrutta questi dati, presumibilmente anche a beneficio del governo cinese. A contrapporsi è il terzo vertice, il governo federale degli Stati Uniti, determinato a difendere la propria sovranità digitale e a proteggere la sicurezza nazionale impedendo il trasferimento dei dati dei suoi cittadini in mani potenzialmente avversarie.

Per risolvere le criticità di questo tipo, l'Unione Europea ha approvato dapprima il Regolamento EU 679/2016 ²⁷ e successivamente ha predisposto il *Digital Services Package* ²⁸ concentrandosi sulla disciplina del trattamento massivo dei dati a tutela dei cittadini europei dal potere economico-politico delle grandi piattaforme americane nell'Unione Europea.

²⁴ N. FERGUSON, *How to Win the New Cold War: To Compete with China, Trump Should Learn from Reagan*, in *Foreign Aff.*, 2025, 104, 24; Z. MA, X. WEN, S. ZHANG, X. SUO, J. GUO, C. CAO, *Who will win the competitive game between China and United States?*, in *Research in Globalization*, 2024, 9, 100261.

²⁵ N. DZICAL, D. SAFARPOUR, D. GODOIJA, L. SÜSSLIN, *Digital Sovereignty and Geopolitics in the Field of Data Protection: A Comparison of the EU, China, and the USA*, Wien, 2025.

²⁶ Per tutti, G. CERRINA FERONI, *Intelligenza artificiale e sistemi di "scoring" sociale. Tra distopia e realtà*, in questa Rivista, 2023, 1 ss.

²⁷ A. NAGI, *Comparing GDPR against*

the United States' Approach to Data Breach Notification by Examining Texas and California and the Feasibility of a Universal Standard, in *Cybaris Intell. Prop. L. Rev.*, 2024, 15, 208.

²⁸ M. EIFERT, A. METZGER, H. SCHWEITZER, G. WAGNER, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, 2021, 58(4); S. HEIDEBRECHT, *From market liberalism to public intervention: Digital sovereignty and changing European union digital single market governance*, in *JCMS: Journal of Common Market Studies*, 2024, 62(1), 205-223; G. DE GRECORIO, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 2021, 19(1), 41-70.

È importante evidenziare la differenza di approccio e la finalità nella gestione della conservazione e del trasferimento dei dati. Gli Stati Uniti, considerando la Cina un Paese avversario, temono che i dati raccolti possano essere usati per scopi di intelligence, offrendo un vantaggio a un potenziale nemico politico, economico o militare. L'Europa, invece, affronta la questione dal punto di vista della tutela della privacy, mirando a impedire l'uso dei dati per profilazione pubblicitaria, attività politiche o pratiche discriminatorie.

Da un lato, quindi, gli Stati Uniti vedono la protezione dei dati come una questione di sicurezza nazionale e di strategia geopolitica, per evitare che informazioni sensibili finiscano nelle mani di un Paese rivale. Dall'altro lato, l'Unione Europea considera la tutela dei dati un diritto fondamentale dell'individuo. Sullo sfondo di questo scenario si colloca TikTok, una piattaforma di enorme successo sia negli Stati Uniti che in Europa, oltre che in Cina.

L'approccio degli Stati Uniti appare più deciso, prevedendo un intervento diretto del Governo federale, che ha gli strumenti legali necessari per imporre un *ultimatum*, cioè: oscurare la piattaforma o obbligare la società madre (*Bytedance*) alla vendita dell'azienda (*TikTok*), afferente a un Paese considerato avversario (*Cina*), a un'impresa americana (*Oracle?*²⁹ *Microsoft?*³⁰, *Amazon?*³¹). Ciò nonostante, nel momento in cui si scrive, la conclusione della *disinvestiture*, organizzata come una operazione economica forzata e di impronta politica, non è ancora avvenuta, lasciando spazio all'emanazione di un nuovo *Executive Order* presidenziale di ulteriori 75 giorni³².

Questa partita si inserisce in un contesto geopolitico in rapido mutamento, dove gli equilibri di potere e le relazioni internazionali stanno cambiando in modi tanto inattesi quanto repentini e imprevedibili³³. Di fronte a siffatto panorama, il giurista deve analizzare gli eventi alla luce della normativa vigente, nel rispetto dei principi dello Stato di diritto e della gerarchia delle fonti.

2. INFLUENZA STRANIERA, INTERESSE NAZIONALE E SOVRANITÀ DIGITALE.

Come già anticipato, l'approccio americano al rischio di sorveglianza massiva dei dati dei propri cittadini è stato differente rispetto a quello dell'Unione Europea, privilegiando la tutela

²⁹ D.BURNS, M. MESSERLY, B. BORDELON, M. LEE HILL, *White House seriously considering deal from Oracle to run TikTok*, in *Politico*, 16.3.2025; B. BORDELON, *Trump's TikTok-Oracle deal could break the law - but nobody can stop him*, *ibidem*, 21.3.2025.

³⁰ REUTERS, *Trump says Microsoft is in talks to acquire TikTok*, 28.1.2025.

³¹ L. HIRSCH et al., *Amazon Said to Make a Bid to Buy TikTok in the U.S.*, in *New York Times*, 3.4.2025.

³² REUTERS, *Trump says he will extend TikTok deadline for 75 days*, 4.4.2025.

³³ R. MACMANUS, *The Limits of the Madman Theory*, in *Foreign Affairs*, 24.1.2025.

dell'interesse nazionale in materia di sicurezza, attraverso l'emanazione di uno specifico *Executive Order*, il n. 13942, già durante la prima Presidenza Trump ³⁴.

Siffatto provvedimento stabiliva la proibizione dei trattamenti dei dati dei cittadini americani da parte di ByteDance o di sue affiliate ai sensi dell'*International Emergency Economic Power Act* ³⁵ (IEPPA) e del *National Emergencies Act* ³⁶ al fine di proibire le transazioni ovvero gli scambi che coinvolgessero ByteDance o le società ad essa collegate ³⁷. Tuttavia, le Corti federali ³⁸ hanno bloccato gli effetti dell'*Executive Order* ³⁹ perché considerati sproporzionati rispetto allo scopo dello IEPPA ⁴⁰. Ciò nonostante, la prima Presidenza Trump aveva ordinato a ByteDance di cedere beni e diritti volti a consentire lo svolgimento dell'ope-

³⁴ Exec. Ordr No. 139422 CFR 412 (8/11/2020), "Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain", ove veniva espressa particolare preoccupazione perché TikTok "automatically captures vast swaths of information from its users" e che tali dati potevano essere usati nell'interesse del governo cinese.

³⁵ 50 U.S.C. §1701. In senso critico, S. FERNANDES, *Ending a National Emergency: the Constitutional Conundrum*, in *Georgia Journal of International and Comparative Law*, 2024, 1-45.

³⁶ 50 U.S.C. §1601. In senso critico, N. GLASS, *Partisan Emergencies: How the Judiciary Can Reign in Dubious Invocations of the National Emergencies Act*, in *Virginia Law Review*, 2025, 111.

³⁷ Per contrastare l'influenza di operatori economici stranieri particolarmente rilevanti e influenti il Legislatore americano nel corso del tempo aveva già predisposto un quadro normativo completato dal Defense Production Act (DPA) (50 USC 55, §4565), e dal *Foreign Investment Risk Review Modernization Act* (FIRRMA). In dottrina, J. R. BLAKEY, *The Foreign Investment Risk Review Modernization Act: The Double-Edged Sword of US Foreign Investment Regulations*, in *Loy. LAL Rev.*, 2019, 53, 981; A. LAW, *The "Legal Black Hole" CFIUS and the Implications of Trump's Executive Order against TikTok*, in *Cornell JL & Pub. Pol'y*, 2021, 31, 217.

³⁸ *TikTok Inc. v. Trump*, 507 F. Supp. 3d 92 (DC 2020); *Marland v. Trump*, 498 F. Supp. 3d 624 (ED Pa. 2020). In dottrina,

M. JIA, *American Law in the New Global Conflict*, in *NYUL Rev.*, 2024, 99, 636; T. CHECK, *Are TikTok "Bans" a Bill of Attainder?*, in *Tul. J. Tech. & Intell. Prop.*, 2024, 26, 57.

³⁹ Tuttavia, alcuni governi statali hanno vietato TikTok dalle proprie reti e dispositivi governativi. Tra questi stati vi sono: Alabama, Georgia, Idaho, Montana, New Hampshire, North Dakota, Utah, Texas, Maryland, South Dakota, South Carolina e Nebraska (T. CHECK, *Are TikTok "Bans"*, cit., 66; W. LUO, *The Spy in Your Pocket: Montana's TikTok Ban and the Federalism Limits of State-level Foreign Policy*, in *51 Hastings Const. L.Q.* 585, 2024).

⁴⁰ L'*"International Emergency Economic Powers Act* (IEEPA)" (Title II of Pub. L. 95-223, 91 Stat. 1626) è stato emanato il 28 ottobre 1977 sotto la presidenza Carter. Esso consente al Presidente di dichiarare uno stato di emergenza in conseguenza di minacce "insolite e straordinarie" conferendo il potere di bloccare i rapporti commerciali, congelare gli asset economici e condurre una guerra di natura economica al fine di contrastare le suddette minacce. Tuttavia, l'esercizio dei poteri attribuiti dallo IEPPA, se non controbilanciato, manifesta due rischi: da un lato compromettere i rapporti economici e commerciali con le imprese straniere; dall'altro il rischio di minare il "delicato equilibrio dei poteri su cui si regge il governo federale" (J. W. ELLISON, *Trust the Process? Rethinking Procedural Due Process and the President's Emergency Powers over the Digital Economy*, in *Duke LJ*, 2021, 71, 499; J. REISKIN, *Delegating Regulating the President's Section 232 and IEPPA Trade Powers*, in *Geo. Wash. L. Rev.*, 2021, 89, 1280.).

rattività di TikTok negli USA, oltre ai dati degli utenti statunitensi già ottenuti o dei prodotti informativi da questi derivati ⁴¹.

Ciò ha provocato la reazione giudiziaria degli ingiunti che hanno impugnato il provvedimento presidenziale presso la Corte distrettuale del *District of Columbia* per testare la costituzionalità del summenzionato *Executive Order 13942*. Nel febbraio 2021 la causa è stata sospesa ⁴² per consentire all'Amministrazione Biden di permettere alle parti di negoziare una soluzione alternativa alla cessione, nonché di esaminare la questione inerente la sicurezza nazionale.

Se sotto il primo profilo le parti non hanno mai raggiunto un accordo, sotto il secondo l'iniziativa politica è stata portata a termine dal Congresso che ha approvato il "*Protecting Americans from Foreign Adversary Controlled Applications Act*" (PAFACAA) ⁴³, ai fini di risolvere i contenziosi riguardanti tanto TikTok quanto altre aziende straniere di pari portata collegate a Paesi ostili. Il PAFACAA consente al Governo federale, in particolare al Presidente degli Stati Uniti, di avvalersi di misure straordinarie, in precedenza non ammissibili, al fine di "perseguire obiettivi di sicurezza economica nell'ambito digitale" ⁴⁴ attraverso l'adozione di misure coercitive contro gli "*Foreign Adversary Controlled Applications*" (FACA), cioè "un sito web, un'applicazione desktop, un'applicazione mobile o un'applicazione di tecnologia aumentata o immersiva, gestita direttamente o indirettamente".

In particolare, si fa riferimento a qualsiasi entità appartenente gruppo ByteDance-TikTok ⁴⁵, oppure a una società tecnologica soggetta a questa normativa ⁴⁶ in quanto controllata da un Paese avversario, straniero e ostile per la sicurezza nazionale degli Stati Uniti, sulla base di una valutazione politica effettuata dalle auto-

⁴¹ A. CHANDER, *Trump v. TikTok*, in *Vand. J. Transnat'l L.*, 55, 2022, 1145.

⁴² Order in *TikTok Inc. v. Committee on Foreign Investment*, No. 20-1444 (CADC, 19 febbraio 2021) consultabile su <https://www.courtlistener.com/docket/67048770/tiktok-inc-v-committee-on-foreign-inv/>.

⁴³ Pub. L. 118-50, div. II, 138 Stat. 955. Tra i primi contributi pubblicati, si vedano: M. D. SUTHERLAND, P. J. BENSON, K. E. BUSCH, *TikTok: Frequently Asked Questions and Issues for Congress*, *Congressional Research Service*, Washington D.C., 2024, *passim*; P. MAZZOTTI, *The 'Protecting Americans from Foreign Adversary Controlled Applications Act': 'TikTok Ban' or New Milestone in US Economic Security Law?*, in CELIS, Institute Blog, 2024.

⁴⁴ P. MAZZOTTI, *The 'Protecting Americans from Foreign Adversary Controlled Applications Act'*, cit.

⁴⁵ Sect. 2(g)(3)(A).

⁴⁶ Nello specifico, la definizione è contenuta nel PAFACAA stesso e stabilisce che: "(A) IN GENERAL. - The term "covered company" means an entity that operates, directly or indirectly (including through a parent company, subsidiary, or affiliate), a website, desktop application, mobile application, or augmented or immersive technology application that- (i) permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content; (ii) has more than 1,000,000 monthly active users with respect to at least 2 of the 3 months preceding the date on which a relevant determination of the President is made pursuant to paragraph (3)(B); (iii) enables 1 or more users to generate or distribute content that can be viewed by other users of the website, desktop application, mobile application, or augmented or immersive techno-

rità federali competenti ⁴⁷. Infatti, nel PAFACAA è esplicitamente stabilito che tale azienda tecnologica è considerabile “covered company” a seguito dell’atto del Presidente che la indica come una minaccia significativa ⁴⁸ per la sicurezza nazionale degli Stati Uniti, nel caso in cui sia controllata da un avversario straniero.

Potenzialmente, e apparentemente, il PAFACAA è applicabile a un numero indefinito di operatori tecnologici stranieri che siano ritenuti un rischio per la sicurezza nazionale ⁴⁹, ma in realtà il PAFACAA è stato designato su uno specifico obiettivo, cioè limitare l’operatività di TikTok negli Stati Uniti, visto il suo enorme successo commerciale, e la conseguente raccolta massiva di informazioni sensibili e dati di utenti americani a favore della proprietà cinese.

Nel contesto così delineato, il PAFACAA vieta agli operatori tecnologici ed economici negli Stati Uniti di svolgere determinate attività ⁵⁰, cioè “(o)ffrire servizi per distribuire, mantenere o aggiornare un’applicazione controllata da un operatore straniero attraverso un marketplace”, ovvero “(f)ornire servizi di hosting Internet per permettere la distribuzione, la manutenzione o l’aggiornamento di tale applicazione straniera”.

Nel testo del PAFACAA il termine stabilito per risolvere la questione posta dall’esercizio delle attività di impresa dell’operatore tecnologico straniero “avversario” era qualificato come preclusivo. Nel caso di TikTok, esso scadeva dopo 270 giorni dall’entrata in vigore del PAFACAA medesimo ⁵¹. Durante tale periodo, è consentita una “cessione qualificata”, ossia un’operazione valutata dal Presidente, attraverso il parere del *Committee*

logy application; and (iv) enables 1 or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology application. (B) EXCLUSION. - The term “covered company” does not include an entity that operates a website, desktop application, mobile application, or augmented or immersive technology application whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews. In dottrina, M. PARK, *A Fear of Ideas? Social Media, Foreign Influence, and National Security in a New Era of Great-Power Competition*, in *Fordham Intellectual Property, Media and Entertainment Law Journal*, 35(2), 244.

⁴⁷ Le “covered company” pertanto sono aziende che operano, “direttamente o indirettamente”, utilizzando un’applicazione con un’ampia base di utenti che permette agli stessi di generare e condividere

contenuti (compresi “testi” e altre “comunicazioni in tempo reale”) (Sezione 2(g)(2)) (P. MAZZOTTI, *op. cit.*).

⁴⁸ Sect. Sezione 2(g)(3)(B).

⁴⁹ Gli “avversari stranieri” sono identificati con riferimento al complesso normativo sulla sicurezza militare (Sezione 2(g)(4)): l’elenco attuale comprende Cina, Russia, Corea del Nord e Iran, con la Cina che rappresenta una priorità chiave per i decisori statunitensi. Una società coperta è considerata “controllata” da un avversario straniero se presenta una serie di legami con la giurisdizione di tale avversario, che di fatto consentirebbero alle relative autorità di esercitare influenza sulle operazioni dell’applicazione (Sezione 2(g)(1)) (P. MAZZOTTI, *op. cit.*).

⁵⁰ Come stabilito dalla Sezione 2(a)(1).

⁵¹ Oppure dalla designazione quali FACA nei confronti di altre app che fossero in analoghe condizioni (P. MAZZOTTI, *op. cit.*).

on *Foreign Investments in the United States* (CFIUS) ⁵², deputato a vagliare le opportune iniziative per eliminare la minaccia alla sicurezza nazionale e a interrompere i legami operativi con l'avversario straniero ⁵³.

Il principio sotteso è che le FACA non siano intrinsecamente rischiose, ma lo diventino se controllate da entità straniere ostili. Pertanto, l'esercizio di attività commerciali o tecnologiche negli Stati Uniti di tali entità non è consentito se il risultato di siffatto controllo è negativo. Tuttavia, la cessione non è necessariamente imposta dalla legge, ma è incentivata dal rischio di divieto delle attività o dall'oscuramento. L'efficacia di tale incentivo è incerta, specialmente per TikTok, data l'opposizione cinese alla cessione dell'azienda e delle sue tecnologie sensibili perché strategiche per il governo cinese.

Alcune voci hanno espresso preoccupazione per il possibile squilibrio dei poteri presidenziali all'interno della disciplina approvata, ritenendo che, in questo contesto, risultino pressoché assoluti ⁵⁴. Un esempio significativo è proprio l'*Executive Order* firmato da Donald Trump il 20 gennaio 2025 ⁵⁵: da un lato, ha revocato il blocco di TikTok imposto dalla Corte Suprema; dall'altro, ha violato le disposizioni del PAFACAA, che prevedevano la cessione dell'app entro i summenzionati 270 giorni dall'approvazione della normativa ⁵⁶.

Tuttavia, il PAFACAA consente al Presidente di prorogare tale termine di ulteriori 90 giorni, ma non oltre. Ed è ciò che ha fatto Trump con un *Executive Order* di prolungamento dell'attività di TikTok di 75 giorni ⁵⁷ firmato nel giorno del suo insediamento, poche ore dopo il *blackout* dell'app sui dispositivi degli utenti americani, a seguito alla pubblicazione della sentenza *Garland*. Ciò nonostante, trascorsi inutilmente i suddetti giorni, la *disinve-*

⁵² F. JALINOUS, T. SENSENIG, *Keeping up with CFIUS: A Practitioner's Report on National Security Trends in the United States*, in *Erasmus L. Rev.*, 2022, 15, 266; A. LAW, *The "Legal Black Hole" CFIUS and the Implications of Trump's Executive Order against TikTok*, in *Cornell J.L. & Pub. Pol'y*, 2021, 31, 217.

⁵³ B. HOROWITZ, T. CHECK, *TikTok v. Trump and the uncertain future of national security-based restrictions on data trade*, in *J. Nat'l Sec. L. & Pol'y*, 2022, 13, 61.

⁵⁴ J. GRIMMELMANN, *The TikTok Ban and Its Consequences*, in *Communications of the ACM*, 23.3.2025; M. PARK, *A Fear of Ideas? Social Media, Foreign Influence, and National Security in a New Era of Great-Power Competition*, in *Fordham Intell.*

Prop. Media & Ent. LJ, 2024, 35, 244. Tra gli attivisti digitali si segnala una campagna di raccolta firme promossa dalle associazioni American Civil Liberties Union e Electronic Frontier Foundation contro l'approvazione del PAFACAA, *Letter Opposing the Protecting Americans from Foreign Adversary Controlled Applications Act*, 12.3.2024.

⁵⁵ *Executive Order: Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok*.

⁵⁶ *Supra*, n. 51.

⁵⁷ Nonché dalla disponibilità della app degli store di Apple e Google (U. SAXER, R. KOLLENBERG, *TikTok's last dance*, in *VerfBlog*, 29.1.2025, disponibile su <https://verfassungsblog.de/tiktoks-last-dance/>; H. N. AHMED, N. JOHNSON, *12 Hours Without TikTok*, in *Spectator*, 23.1.2025).

stitute dell'app è stata nuovamente rinviata con un altro provvedimento del 5 aprile, configurando una violazione del PAFACAA per il superamento del limite dei 90 giorni, posto che il rinvio contenebbe 150 giorni e non più 90.

Nonostante ciò, il quadro normativo prevede una limitata possibilità di adire la *District Court of Columbia*, come stabilito dal PAFACAA medesimo, cioè esclusivamente nei seguenti casi: a) con un ricorso diretto contro il PAFACAA, da presentarsi entro 165 giorni dalla sua promulgazione; oppure b) attraverso un ricorso contro qualsiasi azione, accertamento o decisione adottata in base allo stesso PAFACAA, da proporre entro 90 giorni dalla relativa data.

In questo caso tali rimedi si rivelano tuttavia puramente ipotetici e privi di reale efficacia poiché il primo termine è già spirato, visto che il PAFACAA è entrato in vigore il 24 aprile 2024; mentre sul secondo si è già espressa in via definitiva la Corte Suprema degli Stati Uniti e un nuovo ricorso si scontrerebbe con gli effetti sia della *res judicata*, sia del *collateral estoppel* ⁵⁸.

Ciò nonostante, nel più ampio contesto della rivalità tecnologica USA-Cina, analoghe iniziative di *disinvestiture* potrebbero ripetersi in futuro e rimarrebbe possibile esercitare il rimedio giudiziario federale.

3. LA VALENZA DEL BILANCIAMENTO COSTITUZIONALE TRA LA PROTEZIONE DELLA SICUREZZA NAZIONALE E LA LIBERTÀ DI MANIFESTAZIONE DEL PENSIERO.

In questo contesto, la reazione giudiziaria di Tik Tok ⁵⁹ presenta due obiezioni di natura costituzionale, relative all'applicazione in combinato disposto del *Fifth Amendment* e del *I First Amendment*.

In relazione alla prima prospettiva si parte dall'osservazione relativa alla "*qualified disinvestiture*" che dovrebbe colpire TikTok nel momento in cui gli venga imposta la cessione dell'affiliata americana. La difesa afferma che siffatta cessione "comporta un'illegittima appropriazione di proprietà privata senza un giusto compenso", in violazione della "*Fifth Amendment's Ta-*

⁵⁸ H. SMIT, *International Res Judicata and Collateral Estoppel in the United States*, in *UCLA L. Rev.*, 9, 1963, 44.

⁵⁹ Azione contenuta proprio nella *Petition for Review of Constitutionality of the*

Protecting Americans from Foreign Adversary Controlled Applications Act, 62, TikTok Inc., et al v. Garland, No. 24-01113 (D.C. Cir. May 7, 2024).

kings Clause”⁶⁰, a meno che il proprietario non venga compensato⁶¹.

Anche se l'ipotesi di esproprio non sembra mai essere stata presa in esame, l'argomento è molto forte, in considerazione della tradizione interpretativa che si è formata in materia⁶². Infatti, tale clausola è stata inizialmente applicata al sequestro fisico di proprietà private da parte del governo, ma è stata successivamente estesa per includere beni intangibili e sequestri regolatori. Recentemente, l'applicazione della clausola sui sequestri alle piattaforme online e ai sistemi automatizzati è diventata un argomento di grande interesse e preoccupazione⁶³.

A questo proposito, la Corte Suprema degli Stati Uniti aveva già avanzato alcuni spunti di riflessione in merito al trattamento delle piattaforme e dei dati da queste raccolti nella causa *Biden v. Knight First Amendment Institute at Columbia*⁶⁴, nella quale il Justice Thomas aveva redatto una *concurring opinion* ove riconosceva le difficoltà nella regolamentazione delle piattaforme di social media. In particolare, la questione se questi ultimi siano vettori comuni e se le piattaforme stesse potessero venire utilizzate

⁶⁰ Come è noto, il testo del V Emendamento recita: “Nessuno sarà tenuto a rispondere di un reato capitale o altrimenti infamante se non su denuncia o accusa di un Gran Giurì, eccetto nei casi che si verifichino nelle forze di terra o di mare, o nella milizia, quando questa si trovi in servizio attivo in tempo di guerra o di pericolo pubblico; né alcuno potrà essere sottoposto due volte, per il medesimo reato, a un procedimento che comprometta la sua vita o la sua integrità fisica; né potrà essere obbligato, in qualsiasi causa penale, a testimoniare contro sé stesso, né essere privato della vita, della libertà o della proprietà, senza un regolare procedimento legale; né si potrà espropriare una proprietà privata per uso pubblico, senza un giusto indennizzo”.

⁶¹ La Corte Suprema ha interpretato la clausola sui sequestri in senso riconoscativo di un indennizzo per il sequestro di proprietà privata in tutte le sue forme, inclusi i beni intangibili quale la proprietà intellettuale. La risalente sentenza della Corte nel caso *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393 (1922) da tempo stabilisce la portata della clausola sui sequestri per includere situazioni in cui “la regolamentazione del governo ‘va troppo oltre’ nel diminuire il valore della proprietà privata”. Tuttavia, la Corte ha anche riconosciuto che le regolamentazioni volte a promuovere il bene comune sono generalmente accettate e non considerate sequestri regolatori (M. AMARIKWA, *Rules for Robots: Con-*

stitutional Challenges with the AI Bill of Rights Principles Regulating Automated Systems, in *University of Pennsylvania Journal of Constitutional Law*, 26(4), 2024, 1176-1211).

⁶² K. MARIEN, *TakeTok: Does a TikTok Ban Violate the Takings Clause?*, in *U. Chi. Legal F.*, 2024, 515.

⁶³ La clausola sui sequestri del Quinto Emendamento si è evoluta nel tempo per applicarsi a vari tipi di sequestri, inclusi quelli di beni intangibili e sequestri regolatori. Con il continuo avanzamento della tecnologia, l'applicazione della clausola sui sequestri alle piattaforme digitali e ai sistemi automatizzati è diventata sempre più complessa. A complicare ulteriormente la questione sollevando domande sul valore economico dei beni digitali e sull'impatto delle regolamentazioni sul loro valore (M. AMARIKWA, *Rules for Robots*, cit.).

⁶⁴ 141 S. Ct. 1220 (2021). La questione verteva sulla circostanza se il Primo Emendamento privasse un funzionario governativo del diritto di controllare il suo account personale su Twitter bloccando gli account di terzi e se potesse utilizzare tale account personale in parte per annunciare azioni e politiche ufficiali. Nonostante il Writ of Certiorari concesso, la Corte non ha affrontato la questione posta dalla causa per via del mutamento della giurisdizione dalla Presidenza Trump a quella Biden, rinviandolo al Secondo Circuito con istruzioni di dimmetterlo come irrilevante a causa del cambiamento dell'Amministrazione.

come *forum* pubblici ⁶⁵. A questo proposito, il *Justice Thomas* proponeva due metodi per regolamentare le piattaforme online: il modello del vettore comune e il modello delle strutture pubbliche. Il modello del vettore comune afferma che, poiché il governo offre ai vettori comuni “privilegi speciali,” questi devono “servire tutti i clienti” ⁶⁶. Citando i “Civil Rights Cases”, il *Justice Thomas* effettuava una interpretazione analogica affermando che le aziende, le quali si presentino come aperte al pubblico, possano vedere i loro diritti di esclusione limitati dal Governo federale. Inoltre, sosteneva l’idea che la clausola sui sequestri possa applicarsi a beni intangibili, come dati e algoritmi ⁶⁷.

In sintesi, la clausola sui sequestri del Quinto Emendamento può rappresentare una sfida per la regolamentazione governativa federale delle aziende tecnologiche, poiché le limitazioni significative sull’uso della proprietà privata possono essere considerate violazioni del *Fifth Amendment* medesimo e ciò costituirebbe un ostacolo di non facile soluzione per la regolamentazione delle aziende produttrici di tecnologia.

In questo contesto viene evidenziato il ruolo giocato dal *First Amendment*. La questione quindi si pone nel come realizzare una “*qualified disinvestiture*” ai sensi del PAFACAA. Ci si potrebbe chiedere come si debba delineare la volontà presidenziale nella qualificazione fattuale nell’applicazione della locuzione “*no longer being controlled by a foreign adversary*”. Il Presidente deve determinare come la “*disinvestiture*” concretamente precluda ogni operazione relativa alle attività svolte negli Stati Uniti dell’applicazione controversa controllata dal *foreign adversary*, inclusa ogni cooperazione con l’algoritmo di raccomandazione ovvero ogni accordo sulla condivisione dei dati.

Tuttavia sussiste anche un aspetto relativo all’interesse della controparte che può essere suddiviso in due sottoinsiemi: da un lato sono gli stessi utenti americani che sono interessati al mantenimento in funzione dell’app (*anche se a costoro possa non importare a chi appartenga l’app*) e dall’altro lato, vi è l’inte-

⁶⁵ S. S. SEO, *Failed Analogies: Justice Thomas’s Concurrence in Biden v. Knight First Amendment Institute*, in *Fordham Intell. Prop. Media & Ent. LJ*, 2021, 32, 1070.

⁶⁶ I precedenti che possono essere affini a questo tema sono per esempio *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984), in cui la Corte Suprema federale ha stabilito che la proprietà intellettuale è da considerarsi proprietà ai fini della clausola sui sequestri. La Corte Suprema ha anche osservato che, quando si tratta di proprietà

“intangibili”, come i segreti commerciali, “l’estensione del diritto di proprietà in essi è definita dall’estensione in cui il proprietario del segreto protegge il suo interesse dalla divulgazione ad altri” (M. AMARIKWA, *Rules for Robots*, cit.).

⁶⁷ Ciò conferma un orientamento già presente nella giurisprudenza della Corte Suprema secondo cui siffatta clausola sia validamente applicabile per garantire pari tutela a tutti i tipi di proprietà, compresa quella intellettuale (*Horne v. Dep’t of Agriculture*, 576 U.S. 351 (2015)).

resse governativo cinese di mantenere il controllo sulla sua app, la sua fetta di mercato, i suoi introiti e sui big data raccolti e trattati.

La principale obiezione sottoposta dalla resistente ByteDance nella controversia federale riguardava la violazione da parte del PAFACAA del *First Amendment*, nei confronti sia della società, sia dei suoi utenti.

La Corte analizza la questione chiedendosi se il PAFACAA interferisca in modo sproporzionato con la libertà protette dal Primo Emendamento, in particolare quelle di espressione e di associazione.

L'opinione di maggioranza della Corte sottolinea che una legge volta a controllare l'influenza di uno Stato avversario su una piattaforma di comunicazione è diversa dalle norme riguardanti attività non legate alla libertà di espressione, che la Corte ha esaminato in base ai criteri del Primo Emendamento. Tale diversità si focalizza sul fatto che il PAFACAA si concentri su un governo straniero ostile e sulle differenze tra quest'ultimo e il governo federale degli Stati Uniti, altresì entrano in gioco i legami causali tra la normativa e i limiti della libertà di espressione tutelata: pertanto tali elementi possono incidere sull'applicazione del Primo Emendamento.

Non di meno, tutto ciò che si compie e che si esprime sulla piattaforma di TikTok non va solo a vantaggio diretto ed esclusivo dei suoi utenti e degli affari che essi hanno intrapreso con le loro attività economiche allocate sulla piattaforma stessa, ma va anche a vantaggio, per lo meno indiretto, di un potenziale avversario particolarmente significativo per gli Stati Uniti, cioè il competitor cinese. Oltre a questo, non bisogna tralasciare che TikTok a sua volta è un concorrente aggressivo che ha eroso quote di mercato alle piattaforme social americane.

Siffatto ragionamento non impedisce alla Corte Suprema, almeno in via generale e astratta, di effettuare una breve introduzione sulla portata del Primo Emendamento, ribadendo che al suo cuore si colloca il principio che ogni persona dovrebbe decidere per se stessa quali idee e quali credenze siano meritevoli di espressione, divulgazione, considerazione e adesione⁶⁸. Se l'azione governativa sopprimesse tale libertà violerebbe questo diritto essenziale. Ciò nonostante, tale prospettiva concerne principalmente i cittadini degli Stati Uniti ed è dibattuto se tale previsione sia applicabile anche nei confronti degli stranieri, in particolare se costoro sono considerati una minaccia "esistenziale"⁶⁹, comprese le piattaforme digitali.

⁶⁸ Turner Broadcasting System Inc., v. FCC 512 U.S. 622, 641, (1994) (Turner I).

⁶⁹ E. GRANDE, *I mobili confini della libertà di espressione negli Stati Uniti e il metro della paura*, in *Questione Giustizia*,

2015, n. 4. Sul punto, United States v. Mehanna (735 F.3d 32 (1st Cir. 2013), dove si sottolinea che siano richiesti sforzi ai giudici "to patrol the fine line between vital national security concerns and forbidden

Nel caso di TikTok, la minaccia consiste nella potenziale accessibilità di accesso delle informazioni di 170 milioni di cittadini americani utenti di TikTok da parte delle autorità cinesi e quindi al di fuori del controllo di quelle statunitensi. Pertanto, la questione riguarda come una società di un ente straniero cerchi di proteggersi dall'applicazione di una norma giustificata dal V Emendamento, a sua volta difendendosi invocando il I Emendamento.

In altri termini: può una piattaforma afferente a un'entità straniera ostile avvalersi strumentalmente della libertà di espressione prevista dal Primo Emendamento e al contempo cercare di mantenere intatti i vantaggi, economici e informativi, legati alla raccolta massiva dei dati dei cittadini americani?

La risposta negativa parrebbe ovvia anche agli occhi più ingenui, ma deve essere abbigliata in modo da apparire elegante sotto il profilo costituzionale e inattaccabile sotto quello politico attraverso un opportuno bilanciamento degli interessi in gioco: la libertà di manifestazione del pensiero (*sia dei cittadini americani, sia — e soprattutto — della piattaforma aliena*) *versus* la tutela della sicurezza nazionale. La Corte Suprema non considera questi elementi sullo stesso piano, ed effettua tale bilanciamento mettendo le mani avanti, con l'affermazione che la questione in discussione coinvolge “*totally new problems*” relativi a tecnologie aventi capacità trasformative. Infatti, essa afferma di voler agire con cautela ed essere strettamente focalizzata sulle circostanze di causa, che non riguarderebbero il Primo Emendamento, perché non concernono i contenuti espressivi, ma i rapporti di forza in ambito geopolitico.

Anche se la Corte, per pura ipotesi, prendesse in considerazione l'idea che il PAFACAA possa coinvolgere i diritti di TikTok protetti dal Primo Emendamento, i giudici Supremi americani hanno sostenuto che questi diritti non sono soggetti allo *strict scrutiny*, ma all'*intermediate scrutiny*, proprio perché ad essere coinvolto è un “avversario straniero” in grado di sfruttare il controllo della sua piattaforma per raccogliere e spremere tutte le informazioni possibili dai *big data* provenienti dai già più volte menzionati 170 milioni di utenti americani.

La Corte specifica che solo in questo caso è possibile “abbassare” il livello dello scrutinio costituzionale, dato che TikTok è una Big Tech Company straniera, potenzialmente nemica, né è possibile escludere, nonostante le rassicurazioni, che non possa mai cedere tali big data al governo cinese. Se invece una legge come il PAFACAA fosse mirata nei confronti di qualsiasi altro soggetto economico (*specie se americano*), il livello di attenzione

sullo scrutinio muterebbe di approfondimento, aumentandone le garanzie proprie di uno *strict scrutiny*.

Il trattamento differenziato legato all'applicazione dell'*intermediate scrutiny*, infatti, richiede alla Corte di valutare se le disposizioni del PAFACAA proteggano un interesse governativo importante (*e quindi prevalente*) e che non siano in relazione con la libertà di espressione, né limitino la libertà di parola in misura superiore all'obiettivo del Primo Emendamento stesso. Del resto, argomenta la Corte Suprema, “(d)istinzioni di questo tipo non si presumono invalide ai sensi del Primo Emendamento”.

Il trattamento differenziato, ovvero l'applicazione dell'*intermediate scrutiny* invece dello *strict scrutiny*, è indiscutibilmente giustificata dal fatto che TikTok, pur avendo una sede negli Stati Uniti, è affiliato a un'entità straniera che potrebbe essere potenzialmente ostile. Nell'era digitale, la raccolta e l'analisi dei dati sono pratiche comuni. Tuttavia, la potenza di TikTok, la sua possibile influenza da parte di entità straniere e la quantità di dati sensibili che raccoglie rendono necessario un trattamento specifico per affrontare le preoccupazioni del governo sulla sicurezza nazionale. Di conseguenza, il nodo della questione non è la libertà di espressione, ma la gestione dei dati personali degli utenti, sensibili o meno, tra cui età, nazionalità, indirizzo, preferenze, inclinazioni, comportamenti, contatti, relazioni e interazioni con le quali è possibile profilare con precisione attività individuali e collettive.

Sul punto, la Corte precisa che il divieto di controllo da parte di un avversario straniero tiene conto del fatto che, a meno che TikTok non venga ceduta, il solo funzionamento dell'app negli Stati Uniti alimenta le preoccupazioni del governo in merito alla raccolta dei dati. I requisiti che definiscono una cessione come ‘qualificata’ garantiscono invece che tali preoccupazioni vengano affrontate — e auspicabilmente risolte — prima che TikTok possa riprendere le proprie operazioni negli Stati Uniti.

Le altre opzioni proposte da TikTok e dai suoi creatori come alternative al divieto — quali richiesta di requisiti di divulgazione e restrizioni sulla condivisione dei dati — non mutano il problema di fondo, cioè la preoccupazione dell'uso dei dati a fini di *intelligence*.

Secondo la Corte suprema americana sarebbe necessario concedere all'Esecutivo un certo “margine di manovra” in situazioni come questa. In particolare, la costituzionalità delle disposizioni della legge in discussione non dovrebbe dipendere “dal fatto che siamo d'accordo con la conclusione del governo che il percorso regolatorio scelto sia il migliore o il ‘più appropriato’”.

A questo proposito si osserva che nel recente passato la stessa Corte di Giustizia dell'Unione Europea ha adottato un approccio altrettanto pragmatico nei confronti delle interferenze straniere che minacciassero il regolare svolgimento del dibattito pubblico e

quindi del processo democratico. Ciò si è verificato quando i giudici di Lussemburgo hanno confermato il divieto di trasmissione delle emittenti di propaganda russa, citando la specifica minaccia alla sicurezza in Europa rappresentata dalla guerra di aggressione della Russia contro l'Ucraina ⁷⁰.

La decisione della Corte Suprema degli Stati Uniti, emessa *per curiam*, è accompagnata da due brevi opinioni concordanti dei giudici Sotomayor e Gorsuch. Sotomayor sottolinea che, secondo la giurisprudenza della Corte Suprema, il Primo Emendamento è rilevante nel caso. Gorsuch, invece, sostiene che la Corte ha agito correttamente nel non riconoscere come valido l'interesse del governo a prevenire la cosiddetta "manipolazione occulta dei contenuti" per giustificare il divieto di TikTok. Ha inoltre osservato che ciò che per alcuni è "manipolazione occulta dei contenuti" potrebbe essere visto da altri come semplice "discrezione editoriale".

4. STATI UNITI V. UE: RIFLESSIONI COMPARATE SUL TRATTAMENTO MASSIVO DEI DATI DEGLI UTENTI RACCOLTI DALLE PIATTAFORME DIGITALI.

La contrapposizione tra un governo nazionale, gli Stati Uniti, e una piattaforma straniera di origine cinese, riguardo all'accesso ai dati personali dei cittadini americani ⁷¹, offre un contesto ideale per una comparazione. In particolare, permette di esaminare come il governo statunitense reagisca quando a raccogliere i dati dei cittadini americani sia una piattaforma straniera, in particolare cinese ⁷², rispetto alle raccolte che coinvolgono gli europei da parte, invece, di piattaforme appartenenti agli Stati Uniti ⁷³.

Oltre a siffatte emergenze fattuali, occorre tenere presente la complessità del procedimento comparativo considerando che gli

⁷⁰ Corte di Giustizia dell'Unione Europea, Grande Camera, 27 luglio 2022, causa T-125/22, RT France contro Consiglio dell'Unione Europea. Sul punto, U. SAXER, R. KOLLENBERG, *TikTok's last dance*, cit. Questi autori hanno osservato che in generale, l'equilibrio tra la tutela della sicurezza nazionale e internazionale o regionale e la limitazione della libertà di espressione e di informazione è un caso unico. I tribunali spesso concedono alle autorità politiche un notevole margine di manovra in situazioni come queste. In dottrina, A. GIURICKOVIC, *L'Unione europea contro la propaganda di regime*, in CERIDAP, 2023, (4), 24-46; S. DE VIDO, *La sentenza del tribunale nel caso RT France c. Consiglio: la propaganda di guerra e il ruolo di imprese operanti nel settore della radiodiffusione nell'aggres-*

sione russa contro l'Ucraina, in *Ordine Internazionale e Diritti Umani*, 2022, 4, 1076-1084; S. SASSI, *La Soft War dell'Unione europea: il caso RT-France vs. Consiglio*, in questa Rivista, 2022, 6, 1199-1259.

⁷¹ Y. S. LEE, B. C. LARSEN, J. WU, *US-China tech decoupling increases willingness to share personal data in China*, in *Humanities and Social Sciences Communications*, 2025, 12(1), 1-13.

⁷² W. XU, S. WANG, X. ZUO, *Global data governance at a turning point? Rethinking China-US cross-border data flow regulatory models*, in *Computer Law & Security Review*, 2024, 55, 106061.

⁷³ W. G. VOSS, E. PERNOT-LEPLAY, *China data flows and power in the era of Chinese big tech*, in *Nw. J. Int'l L. & Bus.*, 2024, 44, 1.

ordinamenti coinvolti sono differenti tra loro poiché anche in questo caso si è in presenza di una relazione trilaterale ⁷⁴ tra un ordinamento autoritario (quello cinese) e due ordinamenti appartenenti alla Western Legal Tradition, ma afferenti al Common Law (Stati Uniti) e al Civil Law (nello specifico, l'Unione Europea post-Brexit).

Alla luce di ciò, apparirebbe ragionevole rilevare un interesse pubblicistico dello Stato nell'implementazione di normative focalizzate su un medesimo oggetto: cioè la disciplina dell'uso dei dati massivamente raccolti dalle piattaforme sui propri cittadini, ma con scopi antitetici. Nella prospettiva statunitense tali scopi concernono la protezione di natura difensiva degli interessi nazionali di sicurezza, posto che i big data prelevati dagli utenti americani, e in teoria ottenibili dal governo cinese, rappresentano un enorme e vantaggioso valore aggiunto a favore dell'intelligence. Nella prospettiva dell'Unione Europea, l'espansione extraterritoriale dell'applicazione della disciplina prevista dal GDPR ⁷⁵, DMA ⁷⁶/DSA ⁷⁷, AI Act ⁷⁸ concerne la tutela dei dati degli utenti europei ovunque si questi siano conservati ovvero trattati in quanto lo scopo non è difensivo, ma concerne anche la protezione dei diritti fondamentali dei soggetti, ovvero cittadini, cui quei dati sono stati prelevati ovvero estrapolati.

In entrambi i casi si tratta della manifestazione della sovranità statale nella realtà digitale su enti extraterritoriali, cioè le piattaforme, avulsi da quei meccanismi propri della sovranità tradizionale, le quali a loro volta hanno interessi da proteggere. Tali interessi si possono identificare nell'ottenimento di una *deregulation* il più ampia possibile attraverso il pressante lobbismo nelle sedi degli enti regolatori tanto americani quanto europei ⁷⁹.

⁷⁴ In passato tensioni di natura geopolitica e giuridica si erano già sviluppate attorno alle preoccupazioni sulla protezione dei dati inerenti all'uso della tecnologia 5G di Huawei (A. BERNOT, D. COONEY-O'DONOGHUE, M. MANN, *Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty*, in *Internet Policy Review*, 2024, 13(1); R. HERZOG, *Geopolitical Competition for 5G Technology between China and the United States: Former US President Trump's Ban on Huawei*, 2021; M. RYAN, S. BURMAN, *The United States-China 'tech war': Decoupling and the case of Huawei*, in *Global Policy*, 2024, 15(2), 355-367).

⁷⁵ Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

⁷⁶ Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14

settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

⁷⁷ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

⁷⁸ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

⁷⁹ A. TARRANT, *Lobbying and the EU's Digital Markets Act*, in *Handbook on*

In questo ambito la presenza di diritto positivo diventa sfuggente, dato che entrano in scena influenze di natura storica, geopolitica ed economica, le quali rivelano come la comparazione sia uno strumento utile per comprendere il manifestarsi sia dei rapporti di forza economica sia dei retaggi storici e culturali presenti anche in un ambito come quello digitale. Un esempio, tra i molti, potrebbe riguardare la diffusione dei programmi di GenAI che assorbono indiscriminatamente i dati che li nutrono⁸⁰, svincolandosi da qualsiasi controllo, sia quest'ultimo statutale, sia della fonte ovvero dalla tutela autoriale⁸¹.

L'attenzione di questa sommaria analisi riguarda il trattamento dei big data degli utenti delle piattaforme: da un lato ci si preoccupa di prevenire l'uso dei dati degli utenti americani da una piattaforma cinese alla luce dei rapporti potenzialmente conflittuali tra Cina e Stati Uniti; dall'altro lato l'elemento confliggente non concerne (ancora) una possibile controversia politica, ma lo sfruttamento economico dei dati degli utenti/cittadini dell'Unione Europea da parte delle piattaforme americane.

Immaginando che siffatta rappresentazione avvenga su un palcoscenico, le sfide sull'uso dei dati si svolgono sul proscenio, cosicché le conseguenze e i valori in gioco appaiono evidenti a tutti gli spettatori, mentre sul retropalco si compie l'analisi giuridico comparatistica vera e propria sulla regolamentazione dell'innovazione tecnologica, rilevante per stabilire chi riuscirà a imporre il proprio modello giuridico.

Anche se gli attori sono noti, ci si può chiedere se le loro credibilità e persuasione si sono mantenute nel corso del tempo. Da un lato si pone il sistema di Common Law americano che, nel corso della sua ormai non breve storia, ha abituato i promotori delle innovazioni a sperimentare senza troppi vincoli legali le loro novità tecnologiche direttamente sul mercato, eventualmente risarcendo i consumatori/utenti danneggiati dall'uso della tecnologia, a seguito dello svolgimento di class action, davanti alle Corti⁸².

Dall'altro lato, sembra aver trovato nuova energia l'approccio di Civil Law (mantenuto nel metodo anche dall'Unione Europea),

Lobbying and Public Policy, 2024, Edward Elgar Publishing, 444-456; A. NASTASE, *A tale of two cities: regulating lobbying through public and private instruments in Brussels and Washington DC*, in *Interest Groups & Advocacy*, 2024 1-29.

⁸⁰ S. SAHA, S. K. PANDEY, H. GUPTA, M. CHOUDHURY, *Reading between the Lines: Can LLMs Identify Cross-Cultural Communication Gaps?*, 2025 in arXiv preprint arXiv:2502.09636.

⁸¹ Q. LI, C. CAUFFMAN, *Abuse of Rela-*

tive Dominance by Digital Platforms: A Law and Economics Perspective, in *GRUR International*, 2025, ika001.

⁸² A. ZHUK, *Navigating the legal landscape of AI copyright: a comparative analysis of EU, US, and Chinese approaches*, in *AI and Ethics*, 2024 4(4), 1299-1306; X. WANG, Y. C. WU, *Balancing innovation and Regulation in the age of generative artificial intelligence*, in *Journal of Information Policy*, 20024, 14.

con l'adozione di regolamentazioni *ex ante* in materia di tutela dei consumatori/utenti in un'ottica di prevenzione del rischio (e quindi del danno)⁸³. Ciò nonostante, neppure la disciplina anticipatoria dell'UE è riuscita a prevenire l'effetto distruttivo delle tecnologie digitali e quindi in certuni casi anche nell'Unione Europea si è visto mutare il ruolo del giudice di vertice, cioè della Corte di Giustizia, intervenuta in senso innovativo e costruttivo nei confronti della legislazione.

È possibile individuare alcuni esempi di questo fenomeno, come quando la Corte di Giustizia ha elaborato il concetto di *right to be forgotten*, cioè del diritto all'oblio, nella controversia Costeja Gonzales⁸⁴, oppure quando ha reso stringente la tutela della privacy dei cittadini europei sui dati raccolti dalle piattaforme e trasferiti all'estero, come nella complessa vicenda Schrems⁸⁵. Tuttavia, non si può ignorare che le regolamentazioni europee quali il GDPR⁸⁶ e l'AI Act⁸⁷ sono diventate se non dei veri e propri modelli per gli altri ordinamenti⁸⁸, almeno delle fonti di ispirazione.

In questa sommaria ricostruzione emerge il ruolo politico delle Big Tech Company e del loro fastidio nei confronti della regolamentazione, soprattutto per quel che riguarda ciò che è stato definito come l'"attivismo normativo europeo"⁸⁹, che si è espresso nel tempo con la promulgazione di una amplissima serie di Regolamenti e Direttive⁹⁰. Tuttavia, anche l'esempio americano del

⁸³ R. PAUL, *European artificial intelligence "trusted throughout the world": Risk-based regulation and the fashioning of a competitive common AI market*, in *Regulation & Governance*, 2024, 18(4), 1065-1082.

⁸⁴ N. GUMZEJ, *Google Me and Tell Me Who I Am (Not): The Legal Intricacies of Global Delisting Orders in the "Right to Be Forgotten" Cases*, in *Se. Eur. LJ*, 2024, 12, 133.; D. ZHANG, P. FINCKENBERG-BROMAN, T. HOANG, S. PAN, Z. XING, M. STAPLES, X. XU, *Right to be forgotten in the era of large language models: Implications, challenges, and solutions*, in *AI and Ethics*, 2024, 1-10.

⁸⁵ J. H. B. PEDERSEN, *The EU-US Data Privacy Framework and the Schrems Saga: Is there Light at the End of the Tunnel?*, in *ZEuS Zeitschrift für Europarechtliche Studien*, 27(2), 2024, 213-240; A. ZAC, P. WEY, S. BECHTOLD, D. RODRIGUEZ, J. M. DEL ALAMO, *The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR*, in *Center for Law & Economics Working Paper Series*, 2024, 1; E. FAHEY, *Strategic Litigation and EU Law on Cross-Border Data Transfers: On the Place of EU Law in the Work of Schrems and NOYB*, in *Nordic*

Journal of European Law, 2024, 7(4), 130-153.

⁸⁶ K. BLIND, C. NIEBEL, C. RAMMER, *The impact of the EU General data protection regulation on product innovation. Industry and Innovation*, 2024 31(3), 311-351; E. KHAZAEI, A. ARAHSORKHI, *Comparative Studies: Blockchain Technology Applications in GDPR-Representing an Applicability Model*, in *2024 10th International Conference on Web Research (ICWR)* (pp. 187-194). IEEE.

⁸⁷ C. NOVELLI, F. CASOLARI, P. HACKER, G. SPEDICATO, L. FLORIDI, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, in *Computer Law & Security Review*, 2024, 55, 106066.

⁸⁸ A. BRADFORD, *The false choice between digital regulation and innovation*, in *Nw. UL Rev.*, 2024, 119, 377.

⁸⁹ Si veda, ad esempio, M. CITI, M. K. JUSTESEN, *Institutional constraints, legislative activism and policy change: The case of the European Union in European journal of political research*, 2016, 55(3), 609-625.

⁹⁰ Nel 2024 si potevano contare 104 fonti normative, tra adottate e in corso di approvazione (J. S. MARCUS, K. SEKUT, K.

PAFACAA, seppure non lontanamente paragonabile al complesso quadro europeo, parrebbe andare nella medesima direzione.

In merito alla comparazione normativa, a parere di chi scrive, comparabile con il PAFACAA (nonostante le numerose diversità sopra menzionate) è il DMA che ha introdotto una disciplina preventiva nei confronti dei *gatekeeper*. Quest'ultimo è un ruolo riconducibile a un numero ridotto di grandi imprese proprietarie di alcune piattaforme di base "dotate di considerevole potere economico"⁹¹ e che presidiano l'ingresso al mercato dei servizi digitali⁹².

Ciò posto, non "qualunque" grande impresa può essere considerata *in re ipsa* un *gatekeeper*, ma essa deve essere qualificata come tale a seguito di una decisione della Commissione Europea ai sensi dell'art 3 del DMA⁹³. Si tratta di piattaforme che erogano servizi di intermediazione online, di condivisione video, fornitrici di browser, di motori di ricerca, di social network, di comunicazione interpersonale, di assistenti virtuali, di sistemi operativi, di cloud computing⁹⁴. Tra il 2023 e il 2024 la Commissione ha qualificato come *gatekeeper* Alphabet, Amazon, Apple, Booking, Bytedance, Meta, Microsoft⁹⁵.

Data l'importanza del ruolo svolto dai suddetti *gatekeeper*, è legittimo porsi, in un'ottica comparatistica, una domanda rilevante sul ruolo delle imprese: se da un lato il PAFACAA sembra considerare le piattaforme straniere come potenzialmente ostili,

ZENNER, *A dataset on EU legislation for the digital world*, disponibile su <https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world>, consultato il 31.3.2025).

⁹¹ Considerando n. 3 del Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le Direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali).

⁹² G. SANTONI, *Un approccio comparatistico all'interpretazione degli obblighi dei gatekeepers nel Digital Markets Act*, 1 EJPLT, 2024, 205-218.

⁹³ Per essere definito *gatekeeper* l'impresa deve: 1. Un'impresa è designata come *gatekeeper* se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro. 2. Si presume che un'impresa soddisfi i rispettivi requisiti di cui al paragrafo 1: a) in rela-

zione al paragrafo 1, lettera a), se raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di EUR in ciascuno degli ultimi tre esercizi finanziari, o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di EUR nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri; b) in relazione al paragrafo 1, lettera b), se fornisce un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10 000 utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato; c) in relazione al paragrafo 1, lettera c), se le soglie di cui alla lettera b) del presente paragrafo sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

⁹⁴ L. PELLIZZONI, *Gatekeeper: vecchie idee o nuove soluzioni*, in CERIDAP, 2024, 1, 214 ss.

⁹⁵ EUROPEAN COMMISSION, *Gatekeepers*, https://digital-markets-act.ec.europa.eu/gatekeepers_en (consultato il 4.4.2025).

dall'altro è sufficiente che il DMA si concentri esclusivamente sulla tutela dei consumatori e degli utenti, senza spingersi a definire tali *gatekeeper* come “nemici”, sulla scia del PAFACAA?

In conclusione, da questa sommaria comparazione emerge che, anche in assenza di *gatekeeper* europei, le affiliate europee delle piattaforme digitali rivestono un indubbio ruolo strategico, che i regolatori europei devono valutare con attenzione. Pertanto, la vera domanda da porsi tanto a livello politico quanto istituzionale è: l'Unione Europea potrebbe adottare una normativa simile al PAFACAA per proteggere le informazioni dei cittadini considerandole un asset strategico, oltre che economico?

Abstract

La decisione TikTok v. Garland della Corte Suprema degli Stati Uniti evidenzia il difficile equilibrio tra sovranità digitale, sicurezza nazionale e libertà di espressione. L'analisi si sviluppa considerando l'impatto della tecnologia sullo Stato di diritto e le tensioni geopolitiche legate all'influenza straniera. Centrale è il bilanciamento costituzionale tra la protezione della sicurezza e i diritti fondamentali, con un confronto tra Stati Uniti e UE sul trattamento dei dati degli utenti raccolti dalle piattaforme digitali.

The U.S. Supreme Court's decision in TikTok v. Garland highlights the challenging balance between digital sovereignty, national security, and freedom of expression. The analysis develops by considering the impact of technology on the rule of law and the geopolitical tensions related to foreign influence. At the core, there is the constitutional balancing between the protection of security and fundamental rights, with a comparison between the U.S. and EU on the handling of user data collected by digital platforms.