RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0056
Articolo sottoposto a peer review

Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma

Giuseppe De Ruvo

L'articolo intende mostrare lo stretto legame che intercorre tra raccolta dati e sicurezza nazionale. L'obiettivo è quello di mostrare come la raccolta dati non sia solo importante per le operazioni commerciali e di profilazione delle grandi aziende digitali, perché essa è fondamentale anche per lo sviluppo dell'intelligenza artificiale in campo bellico. In questo senso, l'articolo mostra come l'intervento dello Stato – particolarmente negli USA – nel mercato dei dati abbia come principale obiettivo non quello di garantire la protezione dei dati dell'individuo, ma quello di instaurare un rapporto con le aziende in modo che i dati raccolti possano essere utilizzati per lo sviluppo dell'IA, in una prospettiva strategica e non meramente commerciale. In questo senso, primaria per gli USA è la protezione dei dati domestici per mezzo di limitazioni di mercato ad aziende cinesi, attraverso il *Committee on Foreign Investments in the US* (CFIUS) e lo *International Emergency Economic Powers Act* (IEEPA). Questa impostazione a somma zero dello spazio digitale rende estremamente difficile arrivare ad una data governance globale. In conclusione, analizzeremo il caso TikTok come esempio paradigmatico, dal momento che gli USA hanno consapevolmente deciso di utilizzare lo IEEPA in funzione anti-cinese, sebbene essi avrebbero potuto usarlo per generare un effetto domino in grado di innescare un circolo virtuoso che avrebbe potuto aprire la strada ad un effettivo processo di regolamentazione del flusso di dati. La conclusione principale di questo lavoro è che a rendere difficile il raggiungimento di una data governance globale sono le dinamiche geopolitiche, e non solamente l'opposizione delle grandi aziende a politiche di questo genere.

Intelligenza Artificiale – Raccolta dati – Sicurezza nazionale – Stati Uniti – Cina

G. De Ruvo è laureato in Filosofia teoretica e geopolitica presso l'Università Vita-Salute del San Raffaele di Milano. Attualmente frequenta il master in Filosofia del digitale presso l'Università degli studi di Udine. Ha pubblicato articoli su *Limes – Rivista italiana di geopolitica*.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

1. Introduzione: la raccolta dati oltre la privacy

La ricerca intorno alla raccolta dati ha vissuto un impressionante sviluppo negli ultimi anni, in svariati campi. Da un punto di vista filosofico e sociologico, la letteratura è sostanzialmente unanime nel ritenere che, grazie alle nuove tecnologie digitali, si stia assistendo ad una vera e propria *mediatizzazione integrale del mondo della vita*, cioè del mondo di cui l'individuo fa ordinariamente esperienza[1]. Questo processo, oltre a dar luogo a dinamiche di potere descritte da autori come Couldry[2] e Zuboff[3], genera una vera e propria metamorfosi strutturale della nozione di *medium*: esso passa dall'essere – per l'appunto – il *mezzo* in grado di collegare differenti mondi della vita, *a essere esso stesso il mondo della vita comunemente esperito dai soggetti*. La tecnologia, dunque, passa dall'essere uno strumento per raggiungere un particolare fine all'essere l'ambiente che quotidianamente abitiamo. In questo senso, appare giustificato il neologismo coniato da Luciano Floridi, per il quale non ha più senso parlare, astrattamente, di una vita offline e di una online, poiché la nostra vita è sempre *onlife*: «non ha molto senso chiedersi se qualcuno è online o offline mentre guida seguendo le istruzioni del navigatore»[4]. Proprio per queste ragioni, la raccolta dati è divenuta pervasiva come non mai e, di conseguenza, il dibattito sulla protezione dei dati, sulla privacy e sulla data governance si è a sua volta sviluppato proporzionalmente[5]. Tuttavia, non è nostra intenzione, in questo articolo, entrare nel dibattito circa le diverse policy che sono state intraprese o che potrebbero essere intraprese. Nostro interesse è mostrare come la partita dei dati si giochi soprattutto a livello geopolitico, e come gli interessi geo-strategici delle grandi potenze digitali – oltre ad influenzare il loro approccio giuridico nei confronti di queste tematiche – rendano estremamente difficile arrivare ad una data governance trasparente che possa, dal canto suo, agire come forma di empowerment dei cittadini. Per fare ciò, dovremmo innanzitutto mostrare tre fattori: in primo luogo, lo strettissimo legame che intercorre tra le *big tech* della Silicon Valley e gli apparati governativi americani, illustrando come sia in atto un vero e proprio processo di fusione tra la sfera militare e la sfera civile anche nell'ambito del data mining; in secondo luogo, analizzeremo due istituti giuridici americani, il CFIUS (*Committee on Foreign Investments in the US*) e lo IEEPA (*International Emergency Economic Powers Act*), protagonisti della guerra digitale sino-americana, per mostrare in che termini si configura la sovranità tecnologica e la data governance in questo contesto; in terzo luogo, analizzeremo il caso TikTok, particolarmente istruttivo perché – come mostreremo – gli USA, davanti alla minaccia cinese di TikTok, hanno plasticamente mostrato il loro disinteresse a giungere ad una data governance concertata e condivisa dalla comunità internazionale, considerando anche il mondo digitale come un'arena a somma zero[6], mostrando quindi una continuità con la loro impostazione geopolitica post-guerra fredda. Usare come filo conduttore la politica americana è molto istruttivo, per due ordini di ragioni: in primo luogo, perché le più grandi aziende digitali – ad esclusione di ByteDance, proprietaria di TikTok –, che contribuiscono alla raccolta dati, sono americane e devono, in qualche forma, intrattenere dei rapporti con l'Amministrazione; rapporti che non sono sempre ottimi, ma che sono l'impalcatura decisiva di quello che è stato chiamato "capitalismo politico" americano[7]; in secondo luogo, è decisivo studiare *ora* il caso americano, perché gli USA stanno completando – in questi anni – una transizione decisiva. Nel 1982 – in pieno reaganismo e al crepuscolo dell'URSS – il Presidente della *Federal Communications Commission* aveva una linea molto chiara: appaltare la gestione della privacy ad aziende private[8]. Ciò ha contribuito a creare, per le grandi piattaforme del Web, quello che Zuboff ha denominato "habitat neoliberista", nel quale esse potessero muoversi nella raccolta dati senza eccessivi intoppi legislativi[9]. Tuttavia, questa stagione politica sta venendo meno. Eric Schmidt – ex CEO di Google e ad ora uomo centrale nell'amministrazione Biden per quanto riguarda i temi del digitale e dell'innovazione tecnologica[10] –, in un lungo articolo per il New York Times, invoca un intervento del governo «in grado di creare innovazione, di guidare l'impresa privata e rinnovare la leadership americana»[11]. Per Schmidt, il Governo deve intervenire donando alla raccolta dati una direzione strategica, slegandola da mere dinamiche di mercato. Gli USA stanno andando proprio verso questa direzione e, dunque, anche i loro strumenti giuridici stanno venendo utilizzati in tal senso, cercando di perseguire i *loro* obiettivi strategici, piuttosto che lavorare per arrivare ad una data governance globale[12]. La raccolta e l'uso dei dati, come vedremo, non hanno rilevanza solo per il singolo e per la sua sfera di riservatezza, ma pongono delle vere e proprie minacce alla sicurezza nazionale, che non si limitano alle – seppur presenti – attività di *hacking*, poiché, come già notava Rodotà «il caratterizzarsi della nostra organizzazione sociale sempre più come società basata sull'accumulazione e la circolazione delle informazioni comporta la nascita di una vera e propria nuova "risorsa" di base, alla quale si collega lo stabilirsi di nuove situazioni di potere»[13].

I dati come risorse di base, dunque. Ma risorse di che genere? Rispondendo a questa domanda, capiremo anche perché essi sono considerati materia di sicurezza nazionale.

2. Estrazione dati e sicurezza nazionale negli Stati Uniti: oltre il paradigma commerciale

Buona parte della letteratura si concentra soprattutto su come la raccolta dati invada la sfera di riservatezza del singolo, acquisendo informazioni su di esso con un consenso che a volte non è pienamente consapevole[14]. Affrontando il problema in questi termini, le operazioni di sorveglianza e di data mining vengono tuttavia intese da un punto di vista strettamente commerciale, concentrandosi in particolare sui dati estratti dalle grandi piattaforme a scopo pubblicitario[15]: la raccolta dati, infatti, permette alle aziende di identificare e conoscere meglio i consumatori, in modo da poter fornire servizi di advertising personalizzati. Non bisogna sottovalutare la pervasività di questa nuova forma di capitalismo: quello che Zuboff ha chiamato capitalismo della sorveglianza, infatti, non semplicemente genera plusvalore attraverso la raccolta dati, ma riorganizza – nel contesto delle mediatizzazione del mondo della vita – l'esperienza vissuta degli individui, generando tutta una serie di problemi psicologici e politici che, ampiamente discussi[16], noi non tematizzeremo. Non li tematizzeremo perché scopo di questo articolo è mostrare che il motivo principale per cui non si è ancora giunti ad una data governance globale non è solamente l'opposizione delle *big tech* a policy di questo genere, quanto – soprattutto – la rilevanza, per gli Stati Uniti, della raccolta dati per lo sviluppo dell'intelligenza artificiale in campo bellico. Negli ultimi anni, infatti, gli USA si sono scoperti in pericoloso ritardo rispetto alla Cina in questa nuova corsa agli armamenti[17]. Questo ritardo è dovuto a numerosi fattori: in primo luogo, Internet ha conosciuto il suo grande sviluppo nel momento *unipolare* degli USA, dopo la caduta dell'URSS e prima dell'ascesa della Cina: «la coincidenza tra la fine della guerra fredda e l'avvento di Internet è largamente interpretata come il trionfo della società aperta»[18]. Ancora nel 2016, diversi studiosi mostravano – a ragione – come i report governativi toccassero soltanto di sfuggita il problema delle *Lethal Autonomous Weapons* (LAWs), sottolineando soprattutto «gli irrisolti dilemmi etici»[19] ad esse collegati. In secondo luogo, come nota Eric Schmidt nell'articolo precedentemente citato[20], gli USA hanno sottovalutato la capacità cinese di innovare autonomamente, convinti che essi fossero soltanto in grado di copiare le tecnologie a stelle e strisce. Ciò ha portato i decisori americani a non considerare la rete come un asset strategico, ma come una mera protesi commerciale. In questo senso, la raccolta dati che le *big tech* portavano avanti serviva ad aumentare i loro profitti, e non veniva conferita ad essa una rilevanza strategica, se non come forma di *soft power*[21]. La situazione è drasticamente cambiata quando si è scoperta la possibilità di utilizzare l'intelligenza artificiale in campo bellico, con la costruzione di armi estremamente precise ed indipendenti da qualsiasi controllo umano[22]. Come scrive il Generale Fabio Mini, infatti, «in campo militare si sta passando dal controllo sulle forze con il miglior equipaggiamento al controllo della migliore *informazione* e *informatizzazione* che consentono di pianificare in fretta, coordinare ed attaccare con precisione»[23].

Per capire l'importanza dei dati in questo campo, basta intendersi su come funziona – in linea di massima – l'intelligenza artificiale: le nuove tecnologie dell'intelligenza artificiale e del *machine learning*, infatti, non si limitano ad applicare regole precostituite, ma ricavano da sé regole e soluzioni. Il "carburante", però, sono proprio i dati: il sistema riceve dall'esterno una grande quantità di dati grezzi, ma esso è capace di generalizzazione, che naturalmente diventa più precisa aumentando la quantità di dati che vengono immessi nel sistema. Per ottenere il primato nelle tecnologie emergenti dell'intelligenza artificiale – anche in campo bellico – *conditio sine qua non* è possedere una banca dati enorme, per volume e varietà. Non basta, tuttavia, che questi dati siano presenti: essi devono essere anche integrati, ovvero devono essere racchiusi in un cloud, nel quale questi possano interagire[24]. Tuttavia, gli americani – proprio a causa di una protratta percezione unipolare di sé e dello spazio geopolitico – non si erano mai posti il problema di integrare l'enorme mole di dati che possedevano e che le grandi aziende del digitale andavano raccogliendo: il loro obiettivo era semplicemente quello di legare a sé i satelliti cavalcandone il consumismo. È a questa sfida che si è dedicato il *China Strategy Group*, presieduto da Eric Schmidt, che ha prodotto un report fondamentale per capire la direzione che gli USA stanno prendendo. La proposta fondamentale che il report porta avanti è quella di integrare le conoscenze, il know-how e i dati che sono presenti, seppure in maniera diffusa, nelle varie sfere della società. Il settore privato – Schmidt, fondatore di Google, ne è consapevole probabilmente più di chiunque altro – ha certamente dati e know-how superiori rispetto alla comunità dell'intelligence, in particolare nella capacità di estrarre e aggregare i dati. Questo, però,

non significa che la politica di innovazione tecnologica debba essere lasciata nelle mani della Silicon Valley. Al contrario, «c'è bisogno di aggregare [*marshalling*]»[25] questi dati e questo know-how, creando un «National S&T Analysis Center (NSTAC)»[26], gestito dal dipartimento della difesa. Il NSTAC dovrebbe configurarsi come una agenzia pubblica in grado di creare una condivisione di dati, di tecnologie e di know-how tra agenzie federali ed aziende private – attraverso modalità di lavoro *open source* nei settori strategici – in modo da mettere a sistema il patrimonio di dati che, al momento, è diffuso nei vari meandri della burocrazia (pubblica e privata) americana, così da produrre «dei piani di investimento a lungo termine per le autorità federali»[27]. Gli americani, dunque, sono consapevoli del ritardo accumulato nei confronti dei cinesi, i quali, anche per la loro organizzazione statuale[28], da sempre riescono ad integrare un'enorme mole di dati, che estraggono attraverso piattaforme come WeChat, che copre, in un'unica app, le funzionalità dei maggiori social media occidentali[29]. Se, dunque, il ritardo nella raccolta dati americana rispetto a quella cinese mette il Celeste Impero nella condizione di sviluppare in maniera più efficace l'intelligenza artificiale in campo bellico, è evidente che questa diventa, per gli USA, una tematica che tira in ballo la sicurezza nazionale. Anche perché la raccolta dati cinese non sembra volersi fermare in Asia e in Africa, ma sembra aver preso di mira anche il Nuovo ed il Vecchio Continente.

3. Sicurezza nazionale e interesse geopolitico: l'istituto del CFIUS

È sulla base di questa minaccia alla sicurezza nazionale che interviene, sempre più spesso, il *Committee on Foreign Investments in the US* (CFIUS). L'analisi di questo istituto è decisiva per comprendere come, in realtà, a rendere estremamente difficile una data governance globale non siano soltanto le congiunture geopolitiche, ma anche la natura delle istituzioni giuridiche che negli USA intervengono in questo contesto. Il CFIUS nasce negli anni '50, ma diventa centrale nelle dinamiche internazionali negli anni '70 e '80 in un'altra guerra tecnologica: quella tra Giappone e Stati Uniti inerente ai semiconduttori[30]. In quella congiuntura, il CFIUS, ha bloccato l'acquisizione di Fairchild Semiconductor da parte di Fujitsu, non permettendo al Giappone di superare gli USA nella *semiconductor race*. I poteri del CFIUS sono stati rafforzati, nel 1988, dall'Exon-Florio *amendment*, che permette al Presidente, tramite un *executive order*, di bloccare, sulla base di un'indagine del CFIUS, qualsiasi fusione o acquisizione straniera che possa mettere a rischio la sicurezza nazionale[31]. Il CFIUS, dunque, è un istituto che serve a *proteggere* gli interessi geo-economici americani. Come funziona, però, da un punto di vista procedurale? Quando un'azienda straniera decide di fare degli investimenti negli USA, essa è tenuta ad informare il CFIUS. Inizialmente si apre un dibattito informale tra le aziende e il CFIUS. Se la situazione sembra essere rischiosa per la sicurezza nazionale – non significa necessariamente che ci sia dolo, ma soltanto che gli USA vogliono procedere con ulteriori verifiche – si apre la *National security review*. Questa, di solito, viene chiesta congiuntamente dall'azienda e dal CFIUS, ma quest'ultimo può anche richiederla *sua sponte* – tendenza che, in questa congiuntura, sta aumentando nei confronti degli investimenti cinesi[32]. Se gli USA nutrono ancora dei dubbi, possono aprire la *National security investigation*, obbligatoria per ogni infrastruttura critica, che si può concludere con un *executive order* del Presidente, in grado di bloccare qualsiasi operazione commerciale, se sussistono le criticità inerenti alla sicurezza nazionale, senza possibilità di appello da parte della controparte[33]. Il punto problematico, evidentemente, è la nozione di sicurezza nazionale: è possibile inquadrarla normativamente? Come si fa a definire "critica" un'infrastruttura? Proprio in questa direzione sono andati gli sforzi di diversi studiosi, che hanno cercato di delineare il perimetro di intervento del CFIUS, provando a definire positivamente quali asset fossero da considerare delle infrastrutture critiche. Il tentativo più autorevole è stato quello di Theodore Moran che, in uno studio intitolato *Three Threats: An Analytical Framework for the CFIUS Process*, pubblicato nell'agosto del 2009, ha cercato di circoscrivere il campo di intervento del CFIUS a tre tipi di minacce alla sicurezza nazionale: la minaccia energetica, per la quale gli USA rischierebbero di diventare dipendenti da un'altra nazione per quanto riguarda il proprio fabbisogno energetico; la minaccia dovuta ad un possibile furto di know-how in ambito tecnologico; la minaccia inerente alla possibilità di spionaggio industriale[34]. Se lo studio di Moran ha il merito di essere il più completo in assoluto, è evidente che questo framework normativo non è più adatto alla circostanza attuale, perché non tiene conto delle nuove forme di minaccia alla sicurezza nazionale. La sicurezza nazionale, dunque, diventa un concetto di difficile definizione normativa, perché essa non può essere definita *a priori*, ma dipende dalle contingenze geopolitiche e geoeconomiche. Se si pensa al caso di TikTok, è evidente che, se il CFIUS avesse seguito la *policy* descritta da Moran, esso, semplicemente, non sarebbe potuto intervenire: TikTok non

ha sottratto nessun bene energetico agli USA; non ha copiato nessuno e non ha alcuna intenzione di sabotare le aziende americane o di spiarle, dato che i suoi algoritmi sono semplicemente migliori. Eppure, TikTok – come vedremo – è effettivamente una minaccia alla sicurezza nazionale. Poiché il concetto di sicurezza nazionale evolve e si ridefinisce continuamente, sulla base delle nuove tecnologie e dei nuovi obiettivi geostrategici che le potenze cercano di perseguire, non è possibile definirlo una volta per tutte: «una definizione statica è impossibile e non è fornita dalla legge degli Stati Uniti, nemmeno dal *Defense Production Act* su cui si basa l'edificio normativo del CFIUS. [...] la sicurezza nazionale, per un impero, è ciò che esso vuole che sia per mantenersi»[35].

Dal momento che, come abbiamo mostrato nel precedente paragrafo, i dati sono da considerarsi a tutti gli effetti come un asset decisivo per la sicurezza nazionale data la loro rilevanza in campo bellico, le aziende straniere che li raccolgono – per operare negli USA – dovranno passare per un'istruttoria del CFIUS. Ma se il campo d'azione del CFIUS non risponde a principi normativi ben definiti, ma solamente alla nozione di sicurezza nazionale che viene di volta in volta ridefinita dai decisori politici sulla base delle esigenze geopolitiche, ne segue che – in questo contesto – la data governance diventa, per l'appunto, una questione di sicurezza nazionale, nella quale le esigenze geostrategiche delle grandi potenze sono prioritarie rispetto alle esigenze – e ai diritti – dei singoli individui. Gli stessi istituti giuridici di cui gli USA si servono – il CFIUS e, come vedremo, lo IEEPA – non sono in alcun modo disegnati per giungere ad una data governance realmente trasparente nei confronti degli utenti e, anche quando essi potrebbero essere utilizzati in tal senso, le potenze geopolitiche preferiscono farne un uso geo-strategico, riflettendo la loro visione a somma zero dell'arena tecnologica. Il punto fondamentale è il seguente: non sono le dinamiche di mercato o la potenza delle *big tech* ad ostacolare la transizione verso una data governance globale e concertata, ma sono le esigenze geopolitiche delle grandi potenze – in particolare degli USA – legittimate attraverso la nozione di sicurezza nazionale. Analizziamo ora il caso TikTok, nel quale queste pratiche appaiono evidenti.

4. L'algoritmo strategico di Tiktok e il capitalismo politico cinese

TikTok è una vera creatura della Cina contemporanea, fin dalla sua nascita. Esso diventa il colosso che conosciamo con l'acquisto da parte di ByteDance di Musical.ly nel 2017. Musical.ly era un'azienda cinese con sede a San Francisco, e la fusione non è stata casuale: nel 2015, infatti, il Partito Comunista Cinese ha rilasciato *China 2025*, il piano decennale inerente alle nuove tecnologie, nel quale è esplicita la richiesta al settore privato di procedere con fusioni aziendali ed acquisizioni così da creare campioni nazionali in grado di rivaleggiare con le grandi aziende occidentali[36]. Tale piano ha avuto un incredibile successo e alcuni autori cinesi sostengono che – dopo il periodo "manifatturiero" targato Deng Xiaoping – l'economia della Cina di Xi Jinping – non più timoniere, come Mao, ma CEO della Cina[37] – sia oramai centrata e basata soprattutto sulle nuove tecnologie dell'informazione[38]. Il grande giorno della fusione è stato il 2 agosto 2018: Musical.ly sarebbe scomparso per sempre semplicemente aggiornando l'applicazione, e gli utenti si sarebbero ritrovati TikTok al suo posto, creando un colosso da 600 milioni di utenti. Analizzare le funzionalità tecniche di TikTok può essere molto importante per comprendere per quale motivo esso abbia destato tanta preoccupazione negli USA. Intanto, TikTok ha un pubblico giovanissimo, e ciò gli permette di entrare profondamente nel processo di formazione della personalità dei giovani utenti, favorendo la promozione di determinati contenuti[39]. Ma il fattore decisivo è l'algoritmo che ByteDance ha sviluppato perché, come nota Zhang, «nonostante sia pubblicamente considerata come una comunità di intrattenimento, il vero potere che rende TikTok fondamentale è la sua applicazione nell'intelligenza artificiale»[40]. TikTok è un laboratorio fondamentale per lo sviluppo dell'intelligenza artificiale cinese perché il suo algoritmo deve comportarsi in maniera più autonoma rispetto a quello di Instagram o di Facebook. Se su Instagram o Facebook gli utenti danno inizio alla loro azione di profilazione seguendo pagine o persone, su TikTok l'algoritmo deve fare tutto da solo, ovviamente coadiuvato dai *like*, ma senza ricevere dall'utente indicazioni precise. L'algoritmo di TikTok, inoltre, avendo a che fare con un pubblico di giovani, con gusti in rapida evoluzione, deve essere in grado di adattarsi repentinamente, cosa che invece Facebook e Instagram non riescono a fare, anzi, scoraggiano. L'algoritmo di Facebook ed Instagram è un algoritmo conservatore ed adattivo per consumatori, ha l'intenzione di migliorarsi solo per migliorare l'esperienza di consumo dell'utente, e qualsiasi cambiamento improvviso – dell'algoritmo o dell'utente – è aborrito: esso ci incastra «nei nostri gesti muti senza consentirci di modificarli»[41]. L'algoritmo di TikTok, al contrario, è un algoritmo che ha come fine lo sviluppo del *machine learning* e dell'intelligenza artificiale. Il cambiamento significa possibilità di sviluppo e di miglioramento: è un *algoritmo strategico* che deve

imparare costantemente, perché è lui a scegliere cosa l'utente deve vedere senza ricevere da esso indicazioni specifiche. Un tale algoritmo, dunque, gioca ad un livello di complessità maggiore di quello di Instagram e Facebook e quindi, quando raccoglie dati, ne raccoglie di migliori: raccoglie dati che sono già stati processati da meccanismi di *machine learning* e che possono essere immediatamente utilizzati da altre forme di intelligenza artificiale, come quella bellica. Era inevitabile che un'applicazione di questo genere – il cui legame con il Partito Comunista Cinese è evidente – finisse sotto la lente del CFIUS, che infatti ha aperto un'investigazione non appena ByteDance ha acquisito Musical.ly. L'investigazione è stata resa possibile dal fatto che Musical.ly avesse sede a San Francisco, e dunque l'investimento di ByteDance è stato considerato un investimento cinese in territorio americano. Il ragionamento americano, in questo contesto, è stato molto semplice. Dato che ByteDance è un'azienda cinese, essa è soggetta alla giurisdizione e alle pressioni cinesi. Questo non significa necessariamente che ByteDance sia controllata dal Partito Comunista Cinese, ma – come nota Mark Wu – nel sistema economico cinese «lo Stato apre dei canali informali, secondari, con le aziende private»[42], attraverso i quali si configura il "patto" che tiene in piedi il capitalismo politico cinese: il governo non interviene direttamente nelle dinamiche di mercato delle aziende private, che anzi si sviluppano sempre più rapidamente a scapito di quelle pubbliche[43], ma le aziende private – per operare in Cina – devono tenere presente che il loro interesse non può andare contro le linee guida del Partito Comunista Cinese e con gli interessi strategici del Celeste Impero[44]. In sintesi, le aziende private in Cina sono libere di operare e di fare profitto, ma «lo Stato richiede i contributi delle piattaforme per raggiungere obiettivi di governo»[45]. Data la consapevolezza di questa organizzazione politico-economica, per gli USA «ogni capacità cinese su larga scala di collezione ed analisi di dati degli utenti americani resterà sempre un pericolo»[46], e legittimerà l'intervento del CFIUS. Tuttavia, non sarà direttamente il CFIUS a chiedere il *ban* di TikTok, ma esso avverrà tramite IEEPA, e questo fatto, per quanto controverso, ci permetterà di intendere ancora meglio la postura americana nei confronti della data governance.

5. L'interpretazione americana del caso TikTok: la guerra digitale a somma zero

Per comprendere il caso TikTok e l'atteggiamento americano, è opportuno tornare nelle pagine del report curato da Schmidt. Davanti ad uno scenario in cui una tecnologia strategica è coinvolta, gli Stati Uniti devono decidere se intervenire sul mercato in base alla logica esemplificata dalla Figura 1.

Il procedimento è molto semplice: appurato che una piattaforma è strategicamente rilevante, i decisori politici devono capire se è possibile risolvere il problema «attraverso soluzioni tecniche e/o attraverso negoziati con l'azienda o il governo cinese»[47], oppure se ci si trova davanti ad una situazione «estremamente rischiosa, che presenta problemi che non possono essere tollerati o gestiti con successo»[48]. Ora, davanti ad una situazione del genere, il *China Strategy Group* propone uno spettro di policy di intensità crescente. La prima possibilità è quella di negoziare con il governo cinese, cercando di ottenere delle garanzie *soprattutto per quanto riguarda la crittografia e l'uso dei dati personali*. Le tattiche utilizzate per portare i cinesi a negoziare possono essere dei dazi, oppure una *Transaction Scrutinity* operata dal CFIUS. Sulla base delle indagini del CFIUS si può procedere, attraverso lo IEEPA, a «bloccare le transazioni e a congelare [*freeze*] gli asset in risposta ad una minaccia straordinaria»[49]. Di norma, in questi casi si apre una fase legale nella quale gli USA e la compagnia sottoposta a IEEPA cercano di raggiungere un accordo su alcuni punti come il crittaggio, la chiarezza della proprietà o la proprietà intellettuale. Qualora neanche ciò si rivelasse sufficiente, un'opzione per il governo americano è quella di richiedere alle aziende cinesi di adottare specifici requisiti tecnici, in particolare l'inserimento della crittografia *end-to-end*. Un'altra opzione è quella di chiedere alle aziende cinesi di rendere le piattaforme open access per continuare ad operare negli Stati Uniti. L'*extrema ratio* è rappresentata dal *ban*. Lo strumento chiave, in questo contesto, è lo IEEPA. Esso «può essere esercitato per affrontare una particolare e straordinaria minaccia [...] alla sicurezza nazionale, alla politica estera, o all'economia degli Stati Uniti»[50]. Il vantaggio dello IEEPA è la sua versatilità, perché lascia aperta una vasta gamma di opzioni ai decisori, che vanno dal blocco delle operazioni economiche del soggetto sottoposto a IEEPA, al congelamento delle operazioni commerciali per ulteriori verifiche. Lo IEEPA, inoltre, a differenza dell'*executive order* che deriva direttamente da un indagine del CFIUS, essendo fondato normativamente, è più aperto a possibili ricorsi, ed è quello che è avvenuto con TikTok. Rimane, ovviamente, il fatto che esso può essere utilizzato in condizioni di minaccia alla sicurezza nazionale, che come abbiamo visto è un concetto ai limiti dell'arbitrario. Utilizzare lo IEEPA, dunque, non significa necessariamente impedire che l'asset ad esso sottopo-

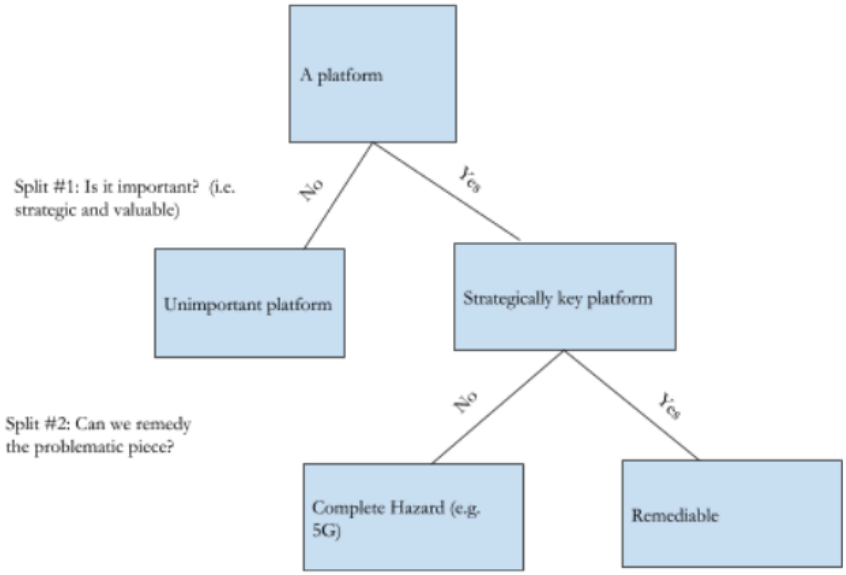

Figura 1: Fonte: China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 10.

sto possa continuare ad operare – nel momento in cui la controparte ricorre contro lo IEEPA, la piattaforma può infatti continuare ad operare fino a sentenza definitiva, ed è quello che è avvenuto con TikTok – ma esso può essere utilizzato come arma di deterrenza per raggiungere determinati obiettivi che lo stesso Eric Schmidt, come abbiamo mostrato, individuava nella possibilità di chiedere alle piattaforme cinesi – ma in generale di qualsiasi nazionalità – di rendere i propri server open access. Ciò significa che, attraverso lo IEEPA, gli USA sarebbero dotati di uno strumento in grado di promuovere una politica di trasparenza per quanto riguarda il flusso di dati. Da un punto di vista normativo, lo IEEPA – come mostrato da Schmidt – può congelare un asset fino a quando esso non rispetta le condizioni che gli USA dettano, e tra queste condizioni vi può essere la richiesta di rendere i server open access per continuare ad operare negli USA. Questa pratica, se applicata al caso TikTok, avrebbe potuto generare un precedente importante, che avrebbe potuto essere utilizzato anche – da altri paesi – nei confronti degli USA, obbligando le grandi potenze a giungere ad un accordo per non vedere – tutte – la propria raccolta dati compromessa. Tuttavia, non è così che gli USA hanno agito e non lo hanno fatto proprio per evitare un effetto domino di questo tipo. Piuttosto che chiedere ai cinesi di rendere i dati raccolti da TikTok open access, gli americani hanno direttamente bannato TikTok, ponendo come condizione che esso avrebbe potuto continuare ad operare *se e solo se fosse stato venduto ad un'azienda americana*. Tradotto: TikTok può continuare ad operare e ad estrarre dati, ma quei dati devono restare in America, perché servono per migliorare l'intelligenza artificiale a stelle e strisce, e non quella cinese. La protezione dei dati dei cittadini non è entrata minimamente nel ragionamento americano. È lo stesso Eric Schmidt, in un libro scritto insieme a Kissinger, a mettere nero su bianco questa intenzione americana: «Washington si è mossa per forzare la vendita di TikTok a un'azienda americana che potesse gestire i dati in patria, evitando che venissero esportati in Cina»[51]. Non è intenzione americana quella di giungere ad una data governance globale: strumenti come il CFIUS non sono disegnati per alcun tipo di multilateralismo, e strumenti come lo IEEPA – che pure potrebbero essere utilizzati in tal senso – vengono sfruttati, al contrario, come arma geoeconomica, nel tentativo di impossessarsi dello spazio economico digitale, piuttosto che per arrivare ad una sua regolamentazione.

6. *Excursus.* Limiti e virtù della strategia europea: la normativa GDPR e l'effetto Bruxelles

Se tra Cina e Stati Uniti la situazione conflittuale sembra rendere impossibile anche semplicemente pensare ad una normativa di protezione dati efficace, l'Unione Europea sembra muoversi in maniera diffe-

rente. La normativa GDPR – entrata ufficialmente in vigore nel 2016 – sembra infatti seguire una duplice direzione: da un lato, la creazione di un mercato comune di dati e di informazioni viene ritenuta strategica; dall'altro lato, viene ritenuta della massima importanza la costruzione di un'infrastruttura legale che possa – al contempo – garantire la *data protection* e stabilire regole chiare che i gestori di dati debbono seguire. La normativa GDPR ha forti radici europee, nella misura in cui trova il suo centro nevralgico nella nozione di accountability, che nel testo italiano è stata tradotta con *responsabilizzazione*. L'idea normativa alla base della GDPR è quella di evitare due estremi: da un lato, non viene considerato adeguato un approccio *top-down*, attraverso il quale l'autorità centrale imporrebbe positivamente una serie di obblighi specifici volti a regolamentare dall'alto le pratiche dei *data holders*; dall'altro lato, la GDPR rifiuta anche un approccio *bottom-up* di autoregolamentazione da parte dei gestori di dati. Il problema può essere espresso in questi termini: in un mondo sempre più mediatizzato, la raccolta dati ha dimensione strategica e quindi non può essere limitata eccessivamente. Tuttavia, la normativa GDPR tiene presente il fatto che «l'analisi dei dati personali è un'attività che può generare dei rischi»[52], e quindi non viene considerato normativamente adeguato lasciare ai *data holders* la possibilità di autoregolarsi. Da questa apparente aporia giuridica – per la quale né l'impostazione *top-down* né l'impostazione *bottom-up* sembrano funzionare – la normativa GDPR riesce ad uscire grazie al concetto di accountability, che non va inteso semplicemente come *responsabilità*, ma – come abbiamo accennato – come *processo di responsabilizzazione*, secondo una tradizione europea che, da Weber a Jonas, caratterizza l'approccio giuridico europeo[53]. La normativa GDPR, infatti, richiede ai soggetti che possiedono dati semplicemente 1) di prevenire i possibili fattori di rischio (attraverso *blockchain*, ad esempio); 2) di introdurre misure preventive (sia *by design* che *by default*) per evitare che si generino effetti indesiderati e, 3), di organizzarsi internamente affinché la sicurezza dei dati sia garantita (chiarezza della proprietà, distribuzione delle responsabilità legali). In questo senso, alcuni studiosi hanno parlato di un approccio *middle-out*, ovvero di una via di mezzo tra l'assoluto *laissez faire* e un interventismo pubblico troppo pesante. Il modello *middle-out* della GDPR, dunque, stabilisce certamente i principi che devono essere seguiti, e definisce anche con chiarezza i risultati che dovrebbero essere raggiunti per essere *accountable*, ma non stabilisce in alcun modo come ciò debba avvenire: «capire come raggiungere tali obiettivi, comunque, rimane prerogativa di chi controlla i dati»[54]. Le aziende che estraggono dati – se vogliono aprirsi al mercato europeo, che rimane fondamentale sia in termini di know-how che di consumo – devono adeguarsi alla normativa GDPR, e rendersi dunque accountable, così da «garantire una protezione preventiva dei dati personali, piuttosto che rimediare in seguito»[55]. La prospettiva europea, dunque, sembra essere effettivamente efficace nella protezione dati, e sembrerebbe anche essere geoeconomicamente strategica. Dato che il mercato dei dati europeo è estremamente ricco (di dati e di consumatori), le grandi aziende del Web non sembrano poterne fare a meno. Sulla base di questa consapevolezza, il GDPR rientra pienamente in quella strategia che è stata denominata *Brussels effect*: le normative europee tendono ad essere assimilate dagli altri attori perché nessuno può rinunciare ad intrattenere buoni rapporti (politici ed economici) con l'UE, e dunque, spesso, esse svolgono il ruolo di apripista verso un modello di *governance globale*[56]. La GDPR, tuttavia, non prevede – e non rientra neppure nelle sue prerogative – alcuna visione strategica per l'Europa, oltre al tentativo di agire come *benchmark* mondiale nella legislazione sulla *data protection*. In breve: la GDPR costituisce un ottimo strumento di tutela per i cittadini, ma – in una fase storica nella quale attorno all'intelligenza artificiale si sta generando una vera e propria corsa agli armamenti – non indica una prospettiva strategica e comunitaria per l'*uso* dei dati – che vengono sostanzialmente lasciati nelle mani dei *data holders* senza particolari restrizioni – scontando evidentemente l'assenza – o l'impossibilità[57] – di una politica estera comunitaria. È per questo che gli USA, nell'affrontare queste tematiche, tendono a non considerare l'UE come un'unica entità, ma a riferirsi ai singoli Stati membri, sfruttando quanto richiamato dal considerando 16 del Regolamento, che permette ai singoli Stati di non attuare la normativa se ad essere in ballo vi è la politica estera o la sicurezza nazionale. Su questa base, Eric Schmidt propone – in funzione anticinese – un'alleanza delle "tecno-democrazie" composta da singoli Stati europei che – riconoscendo la minaccia alla sicurezza nazionale dovuta allo sviluppo cinese – decidano di integrare i dati che vengono raccolti nel loro territorio con l'amministrazione americana, sostanzialmente aggirando la normativa GDPR[58]. Se dunque il tentativo europeo di garantire la *data protection* attraverso il *middle-out approach* rappresentato dalla GDPR sembra essere estremamente efficace dal punto di vista della regolamentazione, della tutela del cittadino e dell'*accountability*, esso – isolatamente – non riesce a rispondere alle sfide geopolitiche che l'aumento della tensione tra Cina e Stati Uniti gene-

ra e, in virtù del considerando 16 sopra citato, rischia di legittimare il *free-riding* di alcuni paesi sulla base della nozione di sicurezza nazionale e dell'interesse geopolitico che, come abbiamo più volte specificato, sono concetti ai limiti dell'arbitrario. L'Unione europea, dunque, necessiterebbe di una politica digitale estera comune che accompagni il GDPR, per evitare di rimanere incastrata nello scontro tra Cina e Stati Uniti, a cui torniamo adesso a volgere lo sguardo.

7. Conclusione. La strettoia americana: proteggere i dati dei cittadini o dominare il mondo?

Prima di diventare una delle voci più influenti dell'intelligence americana, Eric Schmidt era CEO di Google. Davanti alle prime accuse di furto di dati e di violazione della privacy, Schmidt si rivolse direttamente al Congresso americano, nel quale cominciavano ad alzarsi le prime voci contro quello che oggi chiamiamo capitalismo della sorveglianza, ammonendolo: «technology will move faster than governments, so don't legislate before you understand the consequences»[59]. Pronunciata dal CEO di una delle più grandi aziende del mondo, questa affermazione può apparire epifania di liberismo. Ma pronunciata dal direttore del *Defence Innovation Board*, questa frase assume tutt'altro significato. Se gli Stati Uniti procedessero a regolamentare il flusso di dati che le grandi aziende del digitale raccolgono, limitandone l'accesso alle *big tech* o introducendo dei paletti simili a quelli della GDPR, l'innovazione tecnologica americana subirebbe un clamoroso rallentamento che – nella lettura a somma zero americana – non potrebbe che lasciare spazio ai cinesi, pronti ad approfittarne per ottenere l'unico vantaggio bellico ad ora conseguibile. Il monito di Schmidt, dunque, va riletto in questo contesto e assume un senso completamente diverso, coerente con la sua nuova posizione di esperto di sicurezza nazionale: piuttosto che legiferare *contro* la raccolta dati, il governo americano deve lavorare per costruire *insieme* alle grandi aziende del digitale una partnership strategica che permetta agli Stati Uniti di giocare la partita della raccolta dati e dell'intelligenza artificiale con i cinesi ad armi pari, aggregando – sia da un punto di vista quantitativo, sia da un punto di vista infrastrutturale – i dati raccolti dalle *big tech* con quelli raccolti da agenzie federali come la *National Security Agency*[60], attraverso la creazione del NSTAC[61]. Schmidt presiede anche la *National Security Commission on Artificial Intelligence* (NSCAI), che ha recentemente rilasciato un report di oltre 700 pagine, in cui viene delineata la strategia americana sull'intelligenza artificiale. La competizione con la Cina, nota Schmidt, si fa crescente, e il Governo «è lontano dall'essere pronto per l'intelligenza artificiale»[62]. Da ciò segue che lo Stato deve sicuramente intervenire nei confronti delle grandi aziende digitali, ma di certo non per limitarne la raccolta dati: «il bisogno di migliorare la forza di computing e la necessità di grandi quantità di dati per migliorare gli algoritmi sono gli elementi che guidano l'innovazione. Il governo federale deve lavorare insieme alle aziende americane per mantenere la leadership americana e per supportare lo sviluppo di diverse applicazioni dell'intelligenza artificiale che possano portare avanti l'interesse nazionale nel senso più ampio possibile»[63].

La differenza con la GDPR è evidente: gli USA parlano di lavorare con le imprese per portare avanti l'interesse nazionale e qualsiasi riferimento all'*accountability* o alla protezione dei dati dei consumatori è qui rimosso. Da ciò segue, inevitabilmente, che gli strumenti giuridici debbano essere utilizzati secondo una logica strettamente geopolitica. Come nota Kai-Fu Lee, informatico taiwanese formatosi in America che ha guidato il non fortunato tentativo di Google di aprirsi al mercato cinese, «la Cina ha già superato gli Stati Uniti per quanto riguarda la quantità totale di dati che è in grado di trattare e produrre. Questa raccolta dati non è impressionante solo per la quantità, ma grazie allo straordinario ecosistema tecnologico cinese – un universo alternativo di prodotti e funzioni mai visti – questi dati sono fatti su misura per costruire aziende legate all'intelligenza artificiale»[64].

Per competere in questa arena, dunque, la prima cosa da fare è proteggere i propri dati, per evitare che essi finiscano nelle mani del nemico. In una congiuntura del genere, il dibattito sulla *data protection* e sul diritto alla riservatezza non può che passare in secondo piano, non perché meno importante, ma perché la pervasività delle nuove tecnologie e la loro rilevanza in campo bellico fa sì che «la dipendenza digitale in tutti gli aspetti della vita sta trasformando le vulnerabilità personali e commerciali in potenziali debolezze inerenti alla sicurezza nazionale»[65]. Negli Stati Uniti, dunque, l'alternativa non è tra privacy ed assenza di privacy, ma è tra *data protection* e autonomia geopolitica. Ma questa alternativa, negli USA, si traduce immediatamente nella scelta tra il garantire la *data protection* e la perdita della primazia mondiale: «l'intelligenza artificiale sta allargando la finestra di vulnerabilità nella quale gli USA sono già entrati»[66]. È evidente che questa, per un paese come gli USA, è una non scelta, perché perdere la corsa tecnologica contro la Cina significherebbe rischiare di rinunciare al rango imperiale, scadendo a numero due

sullo scacchiere delle potenze. È su questa base che i suoi istituti giuridici e le sue prassi politiche sono sempre rivolte verso la conservazione della sua primazia, mettendo tra parentesi la possibilità – peraltro osteggiata anche dai cinesi, in preda ad un *Nazionalismo Digitale*[67] – di giungere ad una effettiva data governance globale e condivisa, nella quale, al primo posto, vi sia il totale rispetto della sfera di riservatezza del singoli e la protezione dei loro dati attraverso pratiche *accountable*. Gli Stati Uniti, dall'alto della loro «città sulla collina»[68], si sono fino ad ora limitati a controllare il mondo, a spiarlo, vendendo i propri prodotti per sfogare il *surplus commerciale* e per generare *soft power*. Si tratta ora, davanti alla minaccia cinese, di difendere quella città, e gli abitanti – cittadini giustamente preoccupati per l'uso dei loro dati – e grandi aziende digitali dovranno collaborare perché, scrive Schmidt nella lettera che apre il suo report sull'intelligenza artificiale, il nostro «non è il tempo per criticare astrattamente la politica industriale»[69], nemmeno per la sua pervasività nella raccolta dati.

Note

[1]Cfr., almeno, A. Hepp, *Deep mediatization*, Routledge, 2020, 260 p.

[2]N. Couldry, *The costs of connection*, Stanford University Press, 2019, 323 p.

[3]S. Zuboff, *Il capitalismo della sorveglianza* (trad. it. P. Bassotti), LUISS University Press, 2019, 622 p.

[4]L. Floridi, *La quarta rivoluzione* (trad. it. M. Durante), Cortina, 2017, p. 48.

[5] Si veda, al riguardo, l'interessantissimo e recentissimo articolo di N. Hajli, F. Shirazi, M. Tajvidi, N. Huda, *Towards an Understanding of Privacy Management Architecure in Big Data: an Experimental Research*, in "British Journal of Management", 2021, n. 1, p. 548-565, nel quale gli autori mostrano empiricamente come l'infrastruttura dei principali *social* riesca ad acquisire informazioni degli utenti, svelandone le tattiche più recenti. Sul tema del diritto all'accesso ai dati personali, cfr., invece, R. Mahieu, *The right of access to personal data: a genealogy*, in "Technology and Regulation", 2021, n. 1, p. 62-75, nel quale l'autore analizza le diverse scuole di pensiero recuperando, in conclusione, la tesi esposta in S. Rodotà, *Tecnologie e diritti* a cura di G. Alpa, M.R. Marella, G. Marini, G. Resta, il Mulino, 2021, 528 p., secondo la quale il diritto d'accesso ai dati dovrebbe essere legittimato e considerato come una forma di bilanciamento dei poteri nei confronti di chi estrae informazioni, sottolineando dunque la dimensione pubblica e non meramente privatistica del tema della privacy.

[6]G. Rachmann, *Zero Sum World. Power and Prosperity After the Crush*, Atlantic Books, 2011, 352 p. Si veda anche D. Castro, M. Mclaughlin, E. Chivot,*Who is winning the AI race: China, the EU or the United States?*, Center for Data Innovation, 2019, p. 13: «in molti credono che non vi è competizione quando si ha a che fare con l'innovazione. In quest'ottica, ci sarebbero solo vincitori, e non vinti. Ma in realtà, ci saranno vincitori e vinti nella corsa mondiale all'intelligenza artificiale».

[7]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, La Nave di Teseo, 2020, 509 p. Si veda anche, sugli ambigui rapporti tra *big tech* e Amministrazione americana, L. Mainoldi, *Washington e Silicon Valley non si amano ma spiano il mondo insieme* in "Limes. La rete a stelle e strisce", 2018, n. 10, pp. 53-62.

[8]A.F. Westin, *Home Information Systems: The Privacy Debate*, in "Datamation", 1982, n. 4, p. 112.

[9]S. Zuboff, *op. cit.*, pp. 47-50.

[10]Eric Schmidt, di simpatie dichiaratamente democratiche, presiede ad oggi il DIB (*Defence Innovation Board*) e il NSCAI (*National Security Commission on Artificial Intelligence*).

[11]E. Schmidt, *I Used To Run Google. Silicon Valley could Lose to China*, in "The New York Times", 27 February 2020.

[12]In questo senso, vi è una continuità con l'uso politico del diritto che sembra contraddistinguere la giurisprudenza americana, come notato da M.J. Horwitz, *La trasformazione del diritto americano. 1870-1960* (trad. it. M.R. Ferrarese), il Mulino, 2004, 504 p., con la differenza che ad essere al centro è, ora, la politica internazionale.

[13]S. Rodotà, *Tecnologie e Diritti*, cit., p. 35.

[14]Su questo, rimandiamo all'ottimo lavoro di N.S. Kim, D.A. Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consensus*, in "Missouri Law Review", vol. 80, 2015, n. 3, p. 725-770, che ha il merito di mostrare non solo le tecniche che le *big tech* usano per ottenere il consenso all'estrazione ed all'uso di dati, ma anche come la maggior parte delle persone sia molto più incline a fidarsi e ad accettare queste policy di quanto lo sia a lasciare i propri dati direttamente al Governo.

[15]Si veda il recentissimo lavoro di L. Balestrieri, *Le Piattaforme Mondo. L'egemonia dei nuovi signori dei media*, LUISS University Press, 2021, 200 p., nel quale l'autore mostra – sia quantitativamente che da un punto di vista operazionale – le strategie che le grandi piattaforme del Web seguono per aumentare i loro profitti attraverso il data mining e la cattura dell'attenzione, dando particolare rilievo alla transnazionalità dei nuovi media, che viene sfruttata per ottenere tutta una serie di vantaggi, sia politici che fiscali.

[16]La bibliografia è sterminata, si vedano almeno D. Palano, *Bubble Democracy. La fine del pubblico e la nuova polarizzazione*, Scholè, 2020, 224 p.; C. Sunstein, *#Republic. La democrazia ai tempi dei social media* (trad. it. A. Asioli), il Mulino, 2017, 337 p.; sui problemi psicologici, cfr. P. Wallace, *Psicologia di Internet* (trad. it. P. Ferri e S. Moriggi), Cortina, 2017, 542 p.; interessante anche il contributo di T. Cantelmi, *Tecnoliquidità. La psicologia ai tempi di internet: la mente tecnoliquida*, Edizioni San Paolo, 2013, 234 p.

[17]Si veda, D. Garcia, J. Haner, *The artificial intelligence arms race: trends and world leaders in autonomous weapons development*, in "Global Policy", 2019, n. 3, pp. 331-337.

[18]F. Balestrieri, L. Balestrieri, *Guerra Digitale*, LUISS University Press, 2019, p. 45.

[19]C. Cath, L. Floridi et al., *Artificial Intelligence and the "Good Society": the US, EU and UK approach*, in "Science and Engineering Ethics", 2018, n. 2, p. 511.

[20]Cfr., *supra*, nota 11.

[21]Su questo, decisivo è V. De Grazia, *L'Impero irresistibile. La società dei consumi americana alla conquista del mondo* (trad. it. L. Lamberti, A. Mazza), Einaudi, 2020, 621 p., dove viene mostrato chiaramente come la tendenza americana sia quella di ridurre gli alleati a satelliti attraverso l'imposizione di uno stile di vita consumistico ed economicistico, in grado di sopprimere qualsiasi velleità militarista e di autonomia geostrategica.

[22]Si veda, per una trattazione anche etico-morale, E. Schwarz, *Silicon Valley Goes to War: artificial intelligence, weapons systems and the de-skilled moral agent*, in "Philosophy Today", 2021, n. 3, pp. 549-569.

[23]F. Mini, *Che guerra sarà*, il Mulino, 2017, p. 130.

[24]Per un'introduzione al problema del *machine learning* e al suo funzionamento, cfr. P. Ferragina, F. Luccio, *Il pensiero computazionale. Dagli algoritmi al coding*, il Mulino, 2017, 247 p. Per la sua applicazione nell'IA, cfr. M.A. Boden, *L'Intelligenza Artificiale* (trad. it. D. Marconi), il Mulino, 2019, 188 p.

[25]China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 16 (traduzione mia).

[26]*Ibidem*.

[27]*Ibidem*.

[28]Su questo, si veda l'oramai classico, M. Wu, *The "China Inc." challenge to global trade governance*, in "Harvard International Law Journal", vol. 57, 2016, n. 2, pp. 261-324, in cui l'autore mostra approfonditamente i legami tra Stato, Partito ed aziende private. Traduzione sempre mia.

[29]A. Ghizzoni, G. Cuscito, *In Cina WeChat è Internet*, in "Limes. La rete a stelle e strisce", 2018, n. 10, pp. 161-164.

[30]Su questo si veda il classico testo di E. Vogel, *Japan as Number One. Lessons For America*, Harvard University Press, 2014, 288 p.

[31]Su questo, cfr. Congress of the USA, *AReview Of The CFIUS Process For Implementing The Exon-Florio Amendment*, ULAN Press, 2011, 196 p.

[32]Per un'analisi di questa tendenza, cfr. U. Khanapurkar, *CFIUS 2.0: An Instrument of American Economy Statecraft Targeting China*, in "Journal of current Chinese affairs", 2020, n. 1, p. 1-15.

[33]Per approfondire il funzionamento del CFIUS, si veda USA Treasury Department, *Guidance concerning the National Security Review conducted by CFIUS*, 73 Federal Register 74567, 8/12/2008. Si veda anche, per una lettura geopolitica dell'operato del CFIUS, A. Aresu, M. Negro, *La Geopolitica della Protezione. Investimenti e Sicurezza Nazionale: Gli Stati Uniti, L'Italia e L'UE*, Verso l'Europa, 2020, pp. 25-63.

[34]T.H. Moran, *Three Threats: An Analytical Framework for the CFIUS Process*, Peterson Institute for International Economics, 2009, 65 p.

[35]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, cit., p. 371.

[36]Si veda H. Ma et al., *Strategic Plan of Made in China 2025 and Its Implementations*, in R. Brunet-Thornton, F. Martinez (eds.), "Analysing the Impacts of Industry 4.0 in Modern Business Environments", IGI Global, 2018, p. 1-23, dove il piano China 2025 viene paragonato alle politiche industriali degli altri attori globali.

[37]K. Brown, *CEO, China. The Rise of Xi Jinping*, I.B. Tauris, 2017, 262 p.

[38]Su questo, si veda S. Li, X. Xu, *Has "Internet Plus" effectively promoted the innovation of small and micro enterprises?*, in "Shandong Social Sciences", 2019, n. 2, p. 151-156.

[39]Su questo, si veda G. De Ruvo, *Geopolitica della bassezza: TikTok e la post-storicizzazione degli adolescenti americani*, in "Limes. La Riscoperta del futuro", 2021, n. 10, pp. 139-144.

[40]Z. Zhang, *Infrastructuralization of Tik Tok: transformation, power relationships, and platformization of video entertainment in China*, in "Media, Culture and Society", vol. 43, 2020, n. 2, p. 6. Traduzione sempre mia.

[41]T. Numerico, *Big data e algoritmi. Prospettive Critiche*, Carocci, 2021, p. 13.

[42]M. Wu, *op. cit.*, p. 265.

[43]Si veda, D. Xu, X. Wu, *From political power to personal wealth: Privatization and Elite opportunity in Post-Reform China* in "Journal of contemporary China", 2021, p. 993-1013.

[44]Ciò è stato plasticamente dimostrato dalla scomparsa di Jack Ma che – a capo di Ant Group e di Alibaba – aveva criticato il sistema bancario cinese. Si veda, G. Cuscito, *Messaggio per Alibaba: la Cina non sarà degli oligarchi digitali*, in "Cina, scontro tra Pechino e Alibaba - Limes", 17 dicembre 2020.

[45]Z. Zhang, *op. cit.*, p. 14

[46]A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, cit., p. 412.

[47]China Strategy Group, *Asymmetric Competition: A Strategy for China & Technology*, 2020, p. 10.

[48]*Ibidem*.

[49]*Ivi*, p. 13.

[50]US Code, *Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities*, title 50, chapter 35, section 1701.

[51]D. Huttenlocher, H.A. Kissinger, E. Schmidt, *The Age of AI and Our Human Future*, John Murray Publishers, 2021, p. 117. Traduzione mia.

[52]U. Pagallo, P. Casanovas, R. Madelin, *The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data*, in "The Theory and Practice of Legislation", 2019, n. 1, p. 9. Traduzione sempre mia.

[53]Si veda, H. Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica* (trad. it. P.P. Portinaro), Einaudi, 2009, 322 p; M. Weber, *Il lavoro intellettuale come professione* (trad. it. M. Cacciari), Mondadori, 2018, 194 p.

[54]U. Pagallo, P. Casanovas, R. Madelin, *op. cit.*, p. 9.

[55]*Ivi*, p. 11.

[56]A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, 424 p. Questa, tra l'altro, è la strategia che l'UE ha seguito nel negoziare gli accordi di Parigi. Cfr. R. Falkner, *The Paris Agreement and the new logic of international climate politics* in "International Affairs", 2016, n. 5, p. 1107-1125.

[57]Non entriamo nel merito della questione, che ci porterebbe troppo lontano, ma ci limitiamo a rimandare a P. Müller, K. Pomorska, P. Tonra, *The Domestic Challenge to EU Foreign Policy-Making: From Europeanisation to de-Europeanisation?*, in "Journal of European Integration", 2021, n. 5, pp. 519-534, dove gli autori fanno i conti con il principale ostacolo alla creazione di una politica estera comune: la divergenza di interessi geostrategici degli Stati membri.

[58]China Strategy Group, *op. cit.*, p. 25-27.

[59]Citato in BBC News, *Zuckerberg and Schmidt warn on over regulation of web*, 25 May 2011.

[60]Sulle operazioni di sorveglianza della NSA, J. Bamford, *L'orecchio di Dio. Anatomia e Storia della National Security Agency* (trad. it. R. Masini), Fazi Editore, 2004, 700 p.

[61]È su questa visione dell'IA che si sta consumando la rottura – interna all'establishment americano – tra Schmidt e Zuckerberg, nella misura in cui il fondatore di Facebook ritiene che il digitale debba essere usato per scopi meramente commerciali. Schmidt, invece, ritiene che il digitale ha una forte valenza strategica, e per questo motivo è anche critico nei confronti del Metaverso, che il fondatore di Google interpreta come un mondo digitale che potrebbe distrarre gli americani dal loro ruolo storico. Mi permetto di rimandare, su questo, a G. De Ruvo, *Il virus del Metaverso, se l'America fugge dall'inferno della storia* in "Limes. L'altro virus", 2022, n. 1, pp. 41-46.

[62]National Security Commission on Artificial Intelligence, *Final Report*, 2021, p. 2. Traduzione sempre mia.

[63]*Ivi*, p. 4.

[64]Kai-Fu Lee, *AI superpowers*, Houghton Mifflin Harcourt, 2018, p. 23.

[65]National Security Commission on Artificial Intelligence, *op. cit.*, p. 9.

[66]*Ivi*, p. 7.

[67]F. Schneider, *China's digital nationalism*, Oxford University Press, 2018, 320 p.

[68]Questa l'espressione con cui i padri fondatori si rivolgevano a loro stessi appena sbarcati dall'Inghilterra. Tale espressione ha origine in J. Whintrop, *Un modello di carità cristiana* (trad. it. C. Vergaro), Morlacchi, 2015, p. 47.

[69]National Security Commission on Artificial Intelligence, *op. cit.*, p. 4.

* * *

Data mining, artificial intelligence and national security: The geopolitical use of American legal infrastructure as an obstacle for a global data governance. The TikTok case as a paradigm

Abstract: This article aims to show the close link between data mining and national security. The aim is to show how data mining is not only important for big tech's commercial and profiling operations, because it is also critical to develop AI driven warfare. Thus, the article shows how the main goal of the State intervention – particularly in the US – in the data market is not guaranteeing the protection of the individual's data, but is establishing a close relationship with the companies so that the collected data can be used for the development of AI, in a strategic – and not merely commercial – perspective. In this sense, primary for the US is the protection of domestic data through market restrictions to Chinese companies, achieved throughout the intervention of the Committee on Foreign Investments in the US (CFIUS) and the use of the International Emergency Economic Powers Act (IEEPA). The paper claims that this zero-sum approach to the digital space makes the achievement of a global data governance extremely difficult. In conclusion, the paper analyzes the TikTok case as a paradigmatic example, since the US consciously decided to use the IEEPA in an anti-Chinese way, although they could have used it to generate a domino effect capable of triggering a virtuous circle that could have opened the way to an effective process of data regulation. The main conclusion of this paper is that it is because of geopolitical dynamics that the achievement of a global data governance is difficult, and not just because of corporates opposition to such policies.

Keywords: Artificial Intelligence – Data mining – National security – United States – China