Il ruolo della comparazione giuridica nella contesa per la sovranità digitale•

di Guido Smorto

Abstract: *The role of comparative law in the fight for digital sovereignty* – The article scrutinises the main narratives adopted by the E.U., the U.S. and China in the fight for digital sovereignty. It analyses the ongoing dialogue between legal systems that is taking place in the digital sphere to ponder on the role of comparative law in this dialogue. With legal systems called to apply a territorial law to a global phenomenon, comparative law proves to be a fundamental tool in the dispute for digital sovereignty, widely employed across legal formants, with a critical role in creating a distinctive identity for the legal systems.

Keywords: Digital Sovereignty; Data Sovereignty; Cross-Border Data Flows; Privacy; Comparative Law.

1. Introduzione

La comparazione giuridica costituisce uno strumento essenziale nella contesa per la sovranità digitale.[1] In un ambito nel quale gli ordinamenti sono chiamati ad applicare un diritto territoriale ad un fenomeno globale, ed in cui la concorrenza riguarda i confini e le competenze istituzionali degli stessi[2], la comparazione diviene in molti casi lo strumento principe attraverso cui giustificare scelte strategiche e rappresentare una cultura giuridica.

La definizione delle regole di governo della sfera digitale in corso in questi

• *Il presente saggio è frutto della relazione al Convegno "Diritti nazionali in dialogo. Il ruolo della comparazione" che si è svolto all'Università di Roma La Sapienza nei giorni 11-12 luglio 2022. Il testo è destinato alla pubblicazione in M. Graziadei, A. Somma (cur.)*, Diritti nazionali in dialogo. Il ruolo della comparazione, *Roma, 2023*

[1] Per una panoramica della letteratura in tema di sovranità digitale si rinvia all'analisi di P. Hummel, M. Braun, M. Tretter, P. Dabrock, *Data sovereignty: A review*, 8 *Big Data & Society* (2021), i quali passano in rassegna oltre seicento articoli in materia e identificano sei differenti nozioni di sovranità. Sulla polisemia dell'espressione sovranità digitale si veda, inoltre, E.M.L. Moerel, P. Timmers, *Reflections on Digital Sovereignty*, EU Cyber Direct, Research in Focus series, 2021, ssrn.com/abstract=3772777 (ultimo accesso ai collegamenti riportati nelle note in data 13.2.2023).

[2] Di "functional allocation of power" parla, ad esempio, F. Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, in *Law and Political Economy (LPE) Project*, 6.12.2017, lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

DPCE online
ISSN: 2037-6677

decenni sta avvenendo all'interno di un fitto dialogo tra ordinamenti. Questa comunicazione tra i diversi attori della regolazione è di fondamentale importanza. Contribuisce a costruire le modalità di comprensione e di definizione dei problemi e delle sfide che presenta la rivoluzione digitale, a identificare le soluzioni a queste sfide e a mettere a punto le categorie attraverso cui ordinare e descrivere la nuova realtà. Soprattutto, il confronto con altri ordinamenti è funzionale alla costruzione delle identità nazionali o regionali, spesso definite in contrapposizione alle scelte e alle preferenze espresse dagli altri.[3]

In questi anni ciascuno dei tre principali attori della contesa globale per la sovranità digitale - gli Stati Uniti d'America, l'Europa e la Cina - ha dato vita non solamente a sistemi di regole distinti, ma soprattutto ad una peculiare narrazione che va ben oltre la sfera digitale, per conferire un'identità e una giustificazione alle scelte compiute, espressione di una precisa visione del mondo. In questo modo, la sfera digitale si è progressivamente trasformata nel terreno d'elezione per la definizione dei valori di fondo, dei diritti e degli interessi da tutelare, nel quale si condensano scelte, ideali e aspirazioni di una società nel suo complesso. Alla luce di queste premesse, scopo delle riflessioni che seguono è quello di ripercorrere le principali narrazioni che si contendono il campo nella contesa per la sovranità digitale e di riflettere in particolare sul ruolo della comparazione giuridica nel plasmare queste diverse identità.

2. Gli Stati Uniti d'America

Un'analisi di questo genere non può che iniziare con quella che è considerata la patria di internet e del web, non solamente sul piano tecnologico ma anche giuridico: gli Stati Uniti d'America. La pietra angolare della disciplina

[3] Cf. J. Black, *Regulatory Conversations*, 29 *J.L. & Soc'y* 163, at 165 (2002) ("(D)iscourse forms the basis of regulation. It constitutes regulation in that it builds understandings and definitions of problems (for example, 'market failure', 'risk') and acceptable and appropriate solutions (criminalization, 'meta-regulation', 'precautionary principle'), it builds operational categories (for example, 'compliance'), and produces the identities of and relations between those involved in the process. It is functional in that it is designed to achieve certain ends (for example, the strategic use of rule design; the deployment of skills of argumentation and rhetoric by all involved at every stage). It is coordinating in that it produces shared meanings as to regulatory norms and social practices which then form the basis for action (for example, the formation of regulatory interpretive communities"). D'altra parte, a dispetto della sua inafferrabilità, o forse proprio per questo, l'espressione stessa "sovranità" ha sempre avuto un ruolo di primo piano non solo per descrivere ma anche e soprattutto per plasmare la realtà. Sul punto cf. S. Beaulac, *The power of language in the making of international law: the word sovereignty in Bodin and Vattel and the myth of Westphalia*, Leiden, 2004, p. 1 ("The word "sovereignty" is one of those powerful words which has its own existence as an active force within social consciousness. Through the cognitive process of the human mind, not only can language represent reality, but it may play a leading part in creating and transforming reality, including the activity of modelling the shared consciousness of society. Such a word is thus a *form of social power*.").

statunitense risale alla metà degli anni Novanta. La storia è nota e possiamo ripercorrerla per sommi capi. Dinanzi alle prime condanne subite dalle piattaforme digitali ad opera delle corti per i contenuti pubblicati dagli utenti, frutto dell'equiparazione con gli editori tradizionali[4], il Congresso americano diede vita ad una delle norme più note e discusse al mondo: la *Section* 230 del *Communications Decency Act* (1996), la quale stabilisce un'esenzione da responsabilità degli *interative computer services* per i contenuti generati dagli utenti.[5]

Il principale argomento a sostegno di una disciplina protettiva per le piattaforme digitali puntava sul loro carattere neutrale e non intrusivo: una caratteristica che le rendeva profondamente diverse dai media tradizionali, i quali tipicamente svolgono un ruolo attivo nella produzione e nella diffusione dei contenuti.[6] Un regime giuridico più favorevole per questi nuovi intermediari – si osservava - avrebbe scongiurato il pericolo di *chilling effect*, incoraggiandoli ad agire come "buoni samaritani" nel moderare i contenuti, proteggendo allo stesso tempo la libertà di parola e i rischi di *collateral censorship*.[7]

Richiamando la celebre opinione dissenziente del giudice Holmes in *Abrams*[8], la Corte Suprema degli Stati Uniti coniò la celebre metafora di Internet come "nuovo mercato libero delle idee"[9]: un luogo di libero scambio foriero di innovazioni benefiche che è meglio rimanga quanto più possibile libero da ingerenze governative. Senza timore di incorrere in responsabilità – è il

[4] *Stratton Oakmont v. Prodigy Services Co.*, Index No. 94-031063 (N.Y. Sup. Ct., Nassau County Dec. 11, 1995). In senso opposto, v. *Cubby v. CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991).

[5] 47 U.S.C. § 230 (1): 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider'; (2) 'No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (A)'.

[6] In giurisprudenza il richiamo è a *Reno v ACLU*, 521 U.S. 844 (1997), 869 ('the Internet is not as "invasive" as radio or television'). Il secondo argomento utilizzato si fonda sull'assenza di quella scarsità (delle frequenze), la quale tradizionalmente giustifica una normativa più severa per media come televisione o la radio le cui frequenze sono limitate.

[7] *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).

[8] *Abrams v. United States*, 250 U.S. 616 (1919) (Holmes, J, dissenting).

[9] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), at 885 ([a]s a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."). Sull'uso delle metafore nello spazio digitale si rinvia a A. Morelli, O. Pollicino, *Metaphors, Judicial Frames and Fundamental Rights in Cyberspace*, 68 *Am. J. Comp. L.* 616 (2020). Sul ruolo delle metafore nel ragionamento giuridico v. H. Bosmajian, *Metaphor and Reason in Judicial Opinions*, Carbondale, 1992.

ragionamento - si garantisce il libero scambio. Originariamente articolata in un'epoca segnata dal *laissez-faire*, la metafora del *marketplace* suggerisce che una regolazione pervasiva della sfera digitale possa scoraggiare questo libero scambio e compromettere l'innovazione[10].

Grazie alla sec. 230, e alla speciale copertura che il Primo Emendamento offre al *free speech*, prende forma un quadro normativo fortemente protettivo per le nascenti imprese che operano nella sfera digitale, e si realizza un'ampia delega del potere di autoregolamentazione ai privati. La nuova normativa sugli intermediari dell'informazione, infatti, non attribuisce loro semplicemente una speciale immunità da responsabilità, ma costituisce un potente argine ai tentativi di enti statali e locali di regolare le loro attività.[11] Nonostante le molte critiche, quelle "ventisei parole che crearono internet"[12], e la potente metafora del *new marketplace of ideas* che ne è alla base, sono rimaste il caposaldo del modello americano di governo della rete plasmando il modello di impresa e di mercato oggi dominante nel web.[13]

3. L'area europea

In opposizione al discorso nordamericano su competizione e mercato, l'Europa fonda la propria narrazione e la propria identità giuridica facendo appello al linguaggio dei diritti.[14] Una simile narrazione costituisce diretta espressione del progetto europeo sorto nel secondo dopoguerra e tradottosi a livello nazionale nelle costituzioni di paesi come Germania e Italia e, sul piano sovranazionale, nella Convenzione europea dei diritti dell'uomo, per poi trovare definitiva consacrazione nella Carta dei diritti fondamentali dell'UE.[15]

[10] Cf. 47 U.S.C. 230(b)(2) ("It is the policy of the United States (...) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.").

[11] Cf. 47 U.S.C. 230(e)(3) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.". Anche le piattaforme digitali per lo scambio di beni e servizi hanno iniziato a invocare la legge per contestare qualsiasi tentativo di regolare le proprie attività ed evitare responsabilità, enfatizzando l'elemento "espressivo" della propria attività. In questa prospettiva, qualsiasi regolamento – ad esempio un'ordinanza comunale che disciplina gli affitti a breve termine - è inquadrato come "content-based financial burden" che condiziona il "commercial speech" e che, in quanto tale, è soggetto a "strict scrutiny".

[12] J. Kosseff, *The Twenty-six Words that Created the Internet*, Itacha-Londra, 2019.

[13] Cf. A. Chander, *How Law Made Silicon Valley*, 63 *Emory L.J.* 639, 642 (2014) ("legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0.").

[14] Per un'analisi comparatistica si veda P.M. Schwartz, K.N. Peifer, *Transatlantic Data Privacy Law*, 106 *Geo. L.J.* 115 (2017), i quali parlano di "rights talk" per il modello europeo e di "marketplace discourse" per quello statunitense.

[15] Cf. *Carta dei diritti fondamentali dell'UE* - Articolo 8 (Protezione dei dati di carattere personale): 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; 2. Tali dati devono essere trattati secondo il principio di lealtà, per

Nasce in questo quadro una concezione dei dati personali e della loro tutela come diritti fondamentali della persona umana. La costituzionalizzazione del diritto alla protezione dei dati è, infatti, un elemento centrale nella creazione di un'identità europea nella sfera digitale. La dignità umana e l'autodeterminazione costituiscono la base del diritto alla riservatezza delle persone, in una prospettiva che, a differenza di quella nordamericana, trascende la dimensione di mercato per collocare la questione entro i diritti della personalità.[16]

A partire da queste premesse, l'Europa ha costruito una narrazione che descrive una sfera digitale basata sui valori comuni europei, che mette al centro le persone e i loro diritti e che ha l'obiettivo di plasmare una tecnologia "per la gente" ("Tech that works for people")[17], da realizzare attraverso una serie di interventi normativi fondati su alcuni principi cardine: solidarietà e inclusione, libertà di scelta, partecipazione, sicurezza in rete e sostenibilità.[18]

4. La Cina

Il modello cinese si distacca tanto dalla narrazione americana del *marketplace* quanto dal discorso europeo su diritti individuali e sulle tutele costituzionali per mettere al centro una precisa visione di società, da realizzare in linea con gli indirizzi del Partito e con i valori del socialismo. In questa visione, il ruolo del soggetto pubblico è fondamentale nel promuovere il mantenimento dell'ordine e della stabilità sociale, l'armonia, la cooperazione e la sicurezza, e per consolidare i valori del socialismo e del confucianesimo attraverso il controllo della società da parte del partito comunista.[19]

finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica; 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

[16] Per un confronto tra le due tradizioni, con particolare riferimento alla diversa estensione della libertà di espressione, si veda O. Pollicino, *Judicial Protection of Fundamental Rights in the Internet. A Road Towards Digital Constitutionalism?*, Oxford, 2021, spec. 39 ss.

[17] Si veda, ad esempio, la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale della Commissione europea*, 26.1.2022, COM(2022) 28 final, il cui primo capitolo si intitola significativamente "Mettere le persone al centro della trasformazione digitale" ("Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutti gli europei e metterli nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali.").

[18] A questi temi sono dedicati i diversi capitoli nei quali si divide la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale della Commissione europea* e la maggior parte dei documenti europei sul tema. A tal proposito, si veda anche il documento della Commissione europea, *Shaping Europe's digital future*, Publications Office, 2020, data.europa.eu/doi/10.2759/091014.

[19] Cf. *Xi Jinping gives speech at Cybersecurity and Informatization Work Conference*, in *China Copyright and Media*, 19.4.2016, chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-

DPCE online
ISSN: 2037-6677

È per questo che nella Repubblica popolare cinese, Internet, il web e le piattaforme digitali sono considerate infrastrutture tecniche che costituiscono parte integrante di una strategia nazionale unitaria. Questa visione strategica della sfera digitale si traduce in un sistema di governo basato su un *state-centric multilateralism*, che rivendica la centralità dello Stato nel definire le regole del gioco, in aperto contrasto con il *bottom-up multi-stakeholderism* occidentale che invece considera il settore privato e la società civile come gli attori chiave della sfera digitale.[20]

Negli ultimi anni questo progetto ha assunto lineamenti sempre più definiti, seguendo una traiettoria che si articola lungo due direttrici fondamentali. Per un verso, si stabilisce uno stretto controllo sulla libertà di espressione attraverso forme di censura e di selezione dei contenuti, il cui esercizio è spesso delegato alle stesse piattaforme. Per altro verso, si incoraggia uno sviluppo economico aperto e creativo, in cui i colossi del web diventano veicolo di nuove opportunità per l'intero Paese. È su questo secondo versante che la rivoluzione digitale incarna la promessa di rilancio nella competizione internazionale. E sono espressione di questa visione di una conquista collettiva della modernità una serie di leggi – tra l'altro, su concorrenza[21], sicurezza dei dati[22], protezione dei dati personali[23] e sistemi di raccomandazione algoritmica impiegati dalle piattaforme digitali[24] - che stanno contribuendo a definire le regole del gioco.

La centralità della tecnologia per le strategie complessive del paese spiega anche il riferimento insistito alla sicurezza tanto nelle politiche interne quanto nella proiezione internazionale.[25] Tale nozione di sicurezza, declinata

cybersecurity-and-informatization-work-conference/ ("We must (...) strengthen positive online propaganda, foster a positive, healthy, upward and benevolent online culture, use the Socialist core value view and the excellent civilizational achievements of humankind to nourish people's hearts and nourish society."). Per una rassegna di documenti ufficiali sul tema in lingua inglese, si vedano *Chinese government outlines AI ambitions through 2020*, in *New America Foundation*, 26.1.2018, www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/; *Chinese expert group offers 'governance principles' for 'responsible AI'*, in *New America Foundation*, 17.6.2019, www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/. In dottrina, si rinvia a R. Cremers, *China's conception of cyber sovereignty: rhetoric and realization*, in D.S. Broeders, B. van den Berg (eds.), *Digital Technologies and Global Politics*, Lanham, 2020, p. 129; H.S. Gao, *Data Regulation with Chinese Characteristics*, in M. Burri (ed.), *Big Data and Global Trade Law*, Cambridge, 2021, 251.

[20] Cf. A. Chander, H. Sun, *Sovereignty 2.0*, in *Georgetown Law Faculty Publications and Other Works*, p. 2404, 2021.

[21] www.samr.gov.cn/hd/zjdc/202011/t20201109_323234.html.

[22] www.gov.cn/xinwen/2021-06/11/content_5616919.htm.

[23] www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

[24] www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.

[25] Cf. Art. 1 *Cybersecurity Law* (2016) ("This law is formulated so as to ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social

in base agli interessi nazionali, è dilatata al punto da ricomprendere qualsiasi considerazione che riguardi la sovranità e lo sviluppo economico.[26]

5. Un banco di prova. I dati tra libera circolazione e protezione

La disciplina sui dati rappresenta la migliore cartina di tornasole del confronto tra questi modelli. Del resto, i dati non sono solamente il bene più prezioso dell'economia digitale, ma soprattutto la loro circolazione avviene necessariamente a livello planetario, essendo il loro flusso indispensabile per il commercio globale di beni, servizi e informazioni sul web.[27] È per questo che la disciplina dei dati è divenuta subito il terreno di scontro tra le diverse concezioni della sfera digitale ed il luogo nel quale l'espressione sovranità digitale ha fatto il proprio ingresso nel dibattitto pubblico.

a) Stati Uniti d'America. In coerenza con la retorica del *marketplace* e del *free speech*, negli Stati Uniti vige - almeno a livello declamatorio - un generale principio di libera circolazione dei dati, il quale si traduce in limiti stringenti alle ragioni che possano pregiudicarne o restringerne indebitamente la circolazione.[28] La protezione dei dati non assume rango costituzionale e manca una legge federale sulla privacy, la cui tutela è rimessa alle normative statali. Ove presenti, tali leggi sono comunque strumentali al corretto funzionamento del mercato.[29] Eventuali abusi nell'uso dei dati sono sanzionati solo se si siano tradotti in un pregiudizio concreto per il

informatization"), www.chinalawtranslate.com/en/2016-cybersecurity-law/. Sul piano internazionale si veda WTO, *Joint Statement on electronic commerce, Communication from China*, 23.4.2019, INF/ECOM/19 (4.3. "It's undeniable that trade-related aspects of data flow are of great importance to trade development. However, more importantly, the data flow should be subject to the precondition of security, which concerns each and every Member's core interests. To this end, it is necessary that the data flow orderly in compliance with Members' respective laws and regulations."), docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True.

[26] Cf. Art. 1 *Data Security Law* (2021) ("This Law is enacted for the purpose of regulating data processing, ensuring data security, promoting development and utilization of data, protecting the lawful rights and interests of individuals and organizations, and safeguarding the sovereignty, security, and development interests of the state."), www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.

[27] Le due misure principali attraverso le quali si esercita la sovranità digitale sono le restrizioni alla circolazione transfrontaliera dei dati e l'imposizione di requisiti connessi alla localizzazione obbligatoria dei dati. Tutti e tre i modelli esaminati adottano precise misure al riguardo.

[28] Il primo caso nel quale è stato affermato il principio della copertura costituzionale alla libera circolazione dei dati sotto forma di "free speech" è *Sorrell v. IMS Health Care*, 564 U.S. 552, 570 (2011) ("the creation and dissemination of information are speech within the meaning of the First Amendment.").

[29] Tale conclusione rimane valida anche in quei casi che all'apparenza si avvicinano di più al modello europeo, come nel caso del *California Online Privacy Protection Act* (CalOPPA), CAL. Bus. & Prof Code § 22575(a) (2017). Per un esame delle normative statali che impongono obblighi informativi a tutela della *privacy* del consumatore si rinvia a D. Solove, P.M. Schwarz, *Privacy Law Fundamentals*, Portsmouth, 2019, 205 ss.

DPCE online
ISSN: 2037-6677

consumatore e siano frutto di pratiche sleali o di difetto di informazione.[30] In coerenza con questo quadro, la tutela degli interessi lesi è rimessa all'autorità di regolazione del mercato.[31]

b) Europa. In modo opposto, in Europa la circolazione dei dati è condizionata alla tutela della privacy e alla protezione dei dati personali, considerati tratti essenziali della persona umana. A livello degli Stati Membri, il diritto alla privacy e alla protezione dei dati personali è riconosciuto in molte carte costituzionali. A livello europeo, il diritto alla riservatezza è affermato già con la Direttiva sul trattamento dei dati personali del 1995[32] e ha trovato definitiva consacrazione nel Regolamento europeo del 2016 (GDPR).[33] La violazione di tali diritti è sanzionabile indipendentemente dalla prova di un pregiudizio concreto subito, tanto nei confronti dell'autorità pubblica che dei privati, secondo il principio dell'efficacia orizzontale.[34] È in questo quadro che si spiega una tutela rimessa all'autorità giudiziaria, così come molte delle caratteristiche peculiari della disciplina europea sul trattamento dei dati: dall'esigenza di una valida base giuridica per il loro trattamento[35] al diritto

[30] In giurisprudenza si vedano *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1155 (2013); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016). Nella legislazione si vedano, ad esempio, *The Gramm-Leach-Bliley Act*, 15 U.S.C. § 6803 (1999); *Health Information Technology for Economic and Clinical Health Act*, 42 U.S.C. §§ 300jj-300jj-52 (2012). Circa la limitata capacità di offrire tutela di questo tipo di rimedi si veda, in chiave critica, O. Ben-Shahar, C.E. Schneider, *More Than You Wanted To Know: The Failure Of Mandated Disclosure*, Princeton, 2014.

[31] Per una riflessione sul tema si veda C.J. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge-UK, 2016.

[32] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, OJ L 281, 23.11.1995, 31.

[33] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), OJ L 119, 4.5.2016, p. 1 (d'ora in avanti, denominato GDPR). L'art. 1 del GDPR recita: 1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

[34] Per un confronto tra Europa e Stati Uniti sul tema si rinvia a D.J. Solove, *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*, in *GW Law*, 2023, ssrn.com/abstract=4322198.

[35] Cf. art. 6 GDPR (Liceità del trattamento): 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non

all'oblio.[36]

c) Cina. Anche la Cina ha sviluppato una peculiare visione della sfera digitale e, di riflesso, del trattamento dei dati e della loro circolazione. In opposizione tanto alla visione americana dei dati come *commodity* quanto a quella europea dei dati come diritti, la narrazione cinese si fonda su ragioni di sicurezza e, di riflesso, su una concezione dei dati come risorsa strategica.[37] È per questo che - a differenza dell'Europa dove sono i dati personali a ricevere una tutela più intensa - nel modello cinese, ancor prima di quella dei dati personali[38], la categoria fondante è quella dei dati di importanza nazionale sul piano strategico[39], a dimostrazione del fatto che al centro delle preoccupazioni

prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

[36] GDPR - Articolo 17 - Diritto alla cancellazione («diritto all'oblio»): 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. In giurisprudenza il riferimento è a C-131/12, *Google Spain SL and Google Inc v Agencia Española de Protectión de Datos (AEPD) and Mario Costeja Conzález.*

[37] NPC & Central Committee of the CPC, *Outline of the 13th Five-Year Plan for National Economic and Social Development of the People's Republic of China (2016-2020)*, 2016, en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf.

[38] Anche se la *Personal Information Protection Law* (2021) accoglie la nozione di dati personali (Art. 4 "Personal information" refers to various information related to an identified or identifiable natural person recorded electronically or by other means, but does not include anonymized information. Personal information processing includes personal information collection, storage, use, processing, transmission, provision, disclosure and deletion, among others."), le ragioni di sicurezza rimangono comunque centrali nell'impianto della legge (Art. 10 "No organization or individual shall illegally collect, use, process, or transmit the personal information of other persons, or illegally trade, provide or disclose the personal information of other persons, or engage in personal information processing activities that endanger national security or harm public interests."), en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm. Cf. anche Art. 37 PIPL. "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions."

[39] Cf. *Data Security Law* (Art. 21 "The state shall establish a categorized and classified system and carry out data protection based on the importance of the data in economic

DPCE online
ISSN: 2037-6677

cinesi ci sono esigenze di sicurezza nazionale, secondo una visione che si riflette nelle principali leggi sul tema.[40]

6. La contesa per la sovranità digitale e la circolazione dei modelli

Queste tre distinte narrazioni si scontrano nella contesa in corso per il dominio della sfera digitale. La posta in gioco è altissima e riguarda il controllo di dati e software, intelligenza artificiale, standard e protocolli (5G, nomi di dominio, ecc.), processi (come per i sistemi di *cloud computing*), hardware (server, computer, cellulari, tablet), servizi (social media, siti di e-commerce) e infrastrutture (cavi, satelliti fino a intere città, nel caso delle *smart cities*), per estendersi ai campi più diversi, all'interno così come al di fuori del web, dalla libertà di espressione alla tutela dei consumatori e del mercato.[41]

a) Stati Uniti d'America. Se la tendenza ad ampliare il raggio d'azione delle normative nazionali e della giurisdizione delle proprie corti costituisce da sempre un tratto distintivo del diritto nordamericano[42], tale propensione si fa ancora più marcata in tema di sovranità digitale.[43] La concorrenza tra ordinamenti è teorizzata e formalizzata in molti documenti ufficiali, i quali

and social development, as well as the extent of harm to national security, public interests, or the lawful rights and interests of individuals or organizations that will be caused once the data are altered, destroyed, leaked, or illegally obtained or used. The coordination mechanism for national data security shall coordinate the relevant departments to formulate a catalog of important data and strengthen protection of important data. Data concerning national security, lifelines of the national economy, important aspects of people's lives, major public interests, ect., are core data of the state, for which a stricter management system shall be implemented. All localities and departments shall, in accordance with the categorized and classified data protection system, prepare specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the data listed in the catalogs in terms of data protection."). Altre disposizioni significative sono contenute nella *Cyber Security Law* (artt. 21, 34, 37).

[40] V. *supra*, note 37, 38 e 39. Per una riflessione critica in dottrina si rinvia, tra gli altri, a S. Animashaun, *Tearing down the 'Walled Gardens' among China's Tech Giants*, University of Hong Kong Faculty of Law Research Paper No. 2022/35, 14.6.2022, ssrn.com/abstract=4135665; Y.C. Chin, Z. Jingwu, *Governing Cross-Border Data Flows: International Trade Agreements and Their Limits*, in 11(4) Laws 63 (2022); R. Creemers, *China's Long and Winding Road in Global Cyberspace. Great Power Relationships or Common Destiny?*, 31.1.2021, ssrn.com/abstract=3776814.

[41] L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 *Philosophy & Technology* 369, 2020, at 371 ("by "control" I mean here the ability to influence something (e.g. its occurrence, creation, or destruction) and its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence. In this sense, control comes in degrees and above all can be both pooled and transferred."). Sul punto si veda altresì A. Chander, H. Sun, *Sovereignty 2.0*, in *Georgetown Law Faculty Publications and Other Works* 2404 (2021), scholarship.law.georgetown.edu/facpub/2404.

[42] T.L. Putnam, *Courts without Borders: Law, Politics, and US Extraterritoriality*, Cambridge, 2016.

[43] Il provvedimento che, a giudizio degli osservatori, meglio esemplifica questa tendenza è il *Clarifying Lawful Overseas Use of Data Act* ("CLOUD Act") del 2018.

fanno esplicito riferimento agli equilibri geopolitici e competitivi e all'aspirazione degli Stati Uniti di porsi come leader globale della regolazione della sfera digitale.[44]

Fin dagli anni della sec. 230 gli USA hanno avviato una politica sul commercio internazionale per affermare a livello globale il principio della libera circolazione dei dati[45], secondo coordinate poi confluite in una serie di trattati bilaterali e regionali, i quali vietano restrizioni a tale circolazione.[46]

In coerenza con la metafora del *new marketplace*, gli Stati Uniti hanno tenuto politiche attive nel favorire la libera circolazione e considerato ogni forma di restrizione posta da paesi terzi come illegittima barriera al commercio.

L'esportazione del modello americano non è avvenuta solamente attraverso previsioni contenute nei trattati internazionali che stabiliscono la libera circolazione dei dati e il divieto di localizzazione dei dati quali barriere al

[44] Cf. J. Biden, *Remarks by President Biden At Signing of An Executive Order Promoting Competition in the American Economy.* The White House (9.7.2021), www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/09/remarks-by-president-biden-at-signing-of-an-executive-order-promoting-competition-in-the-american-economy/ ("In the competition against China (...) let's show that American democracy and the American people can truly outcompete anyone"); Office of Science and Technology Policy, *Accelerating America's Leadership in Artificial Intelligence* – The White House (11.2.2019), trumpwhitehouse.archives.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/, ove si sottolinea l'esigenza di proteggere i valori americani nei confronti di "strategic competitors and foreign adversaries". Definisce la competizione sull'intelligenza artificiale come una competizione sui valori la National Security Commission on Artificial Intelligence *Final Report* (2021). Anche la normativa proposta dal Congresso americano nel 2021 è esplicitamente definita in opposizione al modello cinese. Sul punto cf. E. Hine, L. Floridi, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*, cit.

[45] White House, *A Framework for Global Electronic Commerce*, 1 July 1997; U.S. Bipartisan Trade Promotion Authority Act of 2002.

[46] Cf. *Comprehensive and Progressive Agreement for Trans-Pacific Partnership - CPTPP*, art. 14.11 (Cross-Border Transfer of Information by Electronic Means); *United States–Mexico–Canada Agreement – USMCA*, art. 19.11 (Cross-Border Transfer of Information by Electronic Means) (1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person. 2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective."). Sul piano bilaterale, gli Stati Uniti hanno concluso accordi con Singapore (2003), Chile (2003), Australia (2004), Peru (2006), South Korea (2007), Panama (2012), Colombia (2012). L'art. 15.8 del *Free Trade Agreement between US and South Korea* ("recognizes the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders").Per una ricognizione sul tema si rinvia a Y.C. Chin, Z. Jingwu, *Governing Cross-Border Data Flows: International Trade Agreements and Their Limits*, cit., 4.

DPCE online
ISSN: 2037-6677

commercio[47], ma anche attraverso la promozione di accordi commerciali[48], strumenti di controllo sugli investimenti stranieri in imprese americane, soprattutto quando questi comportino l'acquisizione di dati sensibili[49], e interventi ad hoc per singole imprese.[50]

b) Europa. Nel tracciare la rotta per una via europea, la Commissione EU ha più volte sottolineato la necessità di disegnare una sfera digitale fondata su regole e valori tipicamente europei.[51]

Questa nozione europea di sovranità digitale si declina in due direzioni diverse e complementari. In primo luogo, l'Europa rivendica l'esigenza di definire in piena autonomia le proprie regole, riducendo al minimo la propria dipendenza da soluzioni create altrove. Allo stesso tempo - come emerge dalla lettura dei documenti ufficiali e delle dichiarazioni rese dalle principali istituzioni[52] - l'obiettivo di dar vita ad una sfera digitale basata sui valori europei procede di pari passo con l'ambizione di influenzare il modo in cui le soluzioni per la sfera digitale sono sviluppate a livello globale e di esportare il modello al di fuori del Vecchio Continente, promuovendo il ruolo di guida dell'Europa nel mondo.[53] Questa aspirazione ha trovato negli ultimi anni

[47] Si vedano, a titolo esemplificativo, le disposizioni contenute nel USMCA. Art. 19.11 ("no Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means"); Art. 19.12 ("no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory").

[48] WTO - Communication from the United States, *The economic benefits of cross-border data flows*, S/C/W/382, 17.6.2019, docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=255027,255028,254954,254931,254926,254888,254866,254874,254846,254826&CurrentCatalogueIdIndex=1&FullTextHash=237161575&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False.

[49] Cf. *Foreign Investment Risk Review Modernization Act* – FIRMA (2018). Sul punto si rimanda a C. Egan, X. Zhu, S. Rasay, *Scrutiny of Chinese investments in US tech to continue under Trump or Biden*, in *S&P Global*, 2020, www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/scrutiny-of-chinese-investments-in-us-tech-to-continue-under-trump-or-biden-60172055.

[50] V. *infra*, nota 85.

[51] Cf. R. Huw Roberts, J. Cowls, F. Casolari, J. Morley, M. Taddeo, L. Floridi, *Safeguarding European values with digital sovereignty: an analysis of statements and policies*, in 10(3) *Internet Policy Review* 1 (2021), policyreview.info/pdf/policyreview-2021-3-1575.pdf.

[52] Cf. *Digital sovereignty is central to European strategic autonomy* – Discorso del Presidente Charles Michel all'evento online "Masters of digital 2021" (We have unique and undeniable strengths. Our market of 450 million people. And with it, comes our regulatory power. The famous "Brussels effect" – that enables us to set the highest standards for our citizens, while projecting these standards across the world. This is especially true in the digital domain. Take our General Data Protection Regulation (GDPR) in 2016. And today's Digital Services Act and Digital Markets Act, proposed by the Commission. And we have another powerful tool: our competition policy. It has an effect beyond our borders. This ensures that consumers have more choice and fair prices in a fair market.").

[53] Cf. T. Madiega, *Digital sovereignty for Europe*, in *EPRS Ideas Paper*, 2020, www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf ("The notion of 'technological' or 'digital sovereignty' has recently

nuova linfa con il GDPR – divenuto una sorta di "gold standard" a livello globale della tutela della privacy[54] - il quale ha finito per rappresentare la dimostrazione più limpida della capacità di promuovere i valori europei nel mondo.

Se anche nel caso europeo i trattati internazionali hanno svolto un ruolo importantissimo, con clausole che riconoscono agli Stati contraenti il diritto di limitare la libera circolazione dei dati in nome del diritto alla privacy[55], l'estensione della portata delle norme eurounitarie al di fuori dello spazio dell'Unione si è caratterizzata soprattutto per il peculiare meccanismo stabilito dal GDPR[56], il quale subordina la libera circolazione dei dati ad una valutazione di "adeguatezza" del sistema di protezione dei dati personali nel paese terzo.[57] È

emerged as a means of promoting the notion of European leadership and strategic autonomy in the digital field (…) In this context, 'digital sovereignty' refers to Europe's ability to act independently in the digital world"). Cf. E. Fahey, *The European Union as a Digital Trade Actor: The Challenge of Being a Global Leader in Standard-Setting*, in 27(2) *International Trade Law and Regulation* 155 (2021).

[54] P.M. Schwartz, *Global Data Privacy: The EU Way*, 94 *N.Y.U. L. Rev.* 771 (2019) ("The cornerstone of EU law in this area, the General Data Protection Regulation (GDPR), is now widely regarded as a privacy law not just for the EU, but for the world."); A. Satariano, *GDPR a New Privacy Law, Makes Europe World's 8 Leading Tech Watchdog*, in *N.Y. Times*, 25.5.2018, www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

[55] In generale, sull'aumento e sulla maggiore latitudine delle eccezioni contenute nei trattati commerciali in tema di privacy si rinvia a S. Yakovleva, *EU's narratives and trade policy on data flows compared to US and China: towards a multilateral consensus, the end of multilateralism or eclipse of the 'Brussels effect'?*, ssrn.com/abstract=4028668 ("While the substantive obligations on data flows have hardened and deepened, the exceptions counterbalancing them became much broader than typical exceptions from international trade commitments").

[56] Cf. A. Chander, M.E. Kaminski, W. McGeveran, *Catalyzing Privacy Law*, cit., at 1765 ("The adequacy process can thus be characterized as a deliberate legal export strategy."); G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention*, in 2(2) *International Data Privacy Law* 68 (2012); J.M. Scott, L. Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, Politico, 31.1.2018, www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation.

[57] Tale requisito di adeguatezza è previsto sia nella Direttiva del 1995 (art. 56) che nel GDPR (art. 45). L'articolo 45, parr. 1-3, del Regolamento intitolato «Trasferimento sulla base di una decisione di adeguatezza», così prevede: «1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi: a) lo ⌈S⌋tato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso

DPCE online
ISSN: 2037-6677

importante notare, a questo riguardo, come il trapianto di norme che un simile dispositivo mette in atto – ossia la spinta nei confronti del paese terzo ad adottare un livello di protezione dei dati sostanzialmente equivalente a quello europee - vada ben oltre la portata immediata della norma. Sfruttando l'esigenza delle imprese di uniformazione nell'offerta di beni e servizi e di razionalizzazione delle politiche aziendali[58], si realizza un ampliamento di fatto della portata del GDPR, come mostra la decisione - assunta da Microsoft all'indomani dell'entrata in vigore del GDPR - di estendere le tutele previste dalle regole europee anche al di fuori dei suoi confini di applicazione.[59] Questo "Effetto Bruxelles"[60], frutto della spinta di mercato, finisce poi per riverberarsi anche sulle scelte degli altri legislatori, a causa delle pressioni di quelle imprese che, adottato lo standard europeo anche fuori dall'Europa, esercitino poi un'influenza sui legislatori dei paesi terzi per l'adozione di regole simili a quelle europee, così da godere di un vantaggio competitivo rispetto ai propri rivali.[61]

effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento; b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali."). Ad oggi la Commissione europea ha stabilito l'adeguatezza di Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israele, Isle of Man, Giappone, Jersey, New Zealand, Corea del Sud, Svizzera, United Kingdom e Uruguay, commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[58] Si vedano le interviste a dirigenti d'azienda riportate in K.A. Bamberger, D.K. Mulligan, *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*, Cambridge-US, 2015. In altri casi, la scelta delle imprese americane è stata quella di disabilitare l'accesso agli utenti europei. Cf. A. Hern, M. Belam, *LA Times among US-based news sites blocking EU users due to GDPR*, The Guardian, 25.5.2018, www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times.

[59] J. Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, Microsoft On Issues (21.5.2018), blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ ("That's why today we are announcing that we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide. Known as Data Subject Rights, they include the right to know what data we collect about you, to correct that data, to delete it and even to take it somewhere else.").

[60] Di "Brusseles Effect" parla A. Bradford, *The Brussels Effect*, 107 *Nw. U. L. Rev.* 1, 8 (2012) ("Unilateral regulatory globalization occurs when a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards.").

[61] Cf. A. Chander, M.E. Kaminski, W. McGeveran, *Catalyzing Privacy Law*, cit., 1789 ("The Brussels Effect on Microsoft may thus be driving it to push for state privacy legislation that more closely maps on to the GDPR and therefore does not raise regulatory costs for Microsoft-but may raise regulatory costs for non-GDPR-compliant local competitors.").

c) Cina. Anche la Cina ha rivendicato con forza la propria sovranità[62], in coerenza con il principio di sovranità territoriale e di mutua non interferenza negli affari interni che sono da sempre al centro della sua politica estera.[63] Nella sfera digitale questa rivendicazione si è tradotta in uno stretto controllo delle infrastrutture tecnologiche strategiche per il paese[64], secondo una traiettoria che ha riguardato inizialmente quelle fisiche per poi estendersi anche a software e contenuti.[65] Il famoso *Great Firewall*[66] e, in modo meno eclatante, le tante disposizioni che impongono una ferrea localizzazione dei dati, ne sono una chiara riprova.[67]

D'altra parte, parallelamente all'ambizione di trasformarsi da una "grande" (*wangluo daguo*) ad una "forte" potenza digitale (*wangluo qiangguo*)[68], si è modificata anche la politica cinese in tema di sovranità e, con essa, l'ambizione di esercitare la propria influenza a livello globale.[69] Nel

[62] Cf. Libro Bianco *The Internet in China*, www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm ("Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected."). Per una ricostruzione della vicenda v. A. Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 *Ohio St. Tech. L.J.* 395, 403 (2020).

[63] Una simile visione è riflessa nelle dichiarazioni ufficiali dei suoi leader. Cf. le dichiarazioni del Presidente Xi secondo cui il rispetto della sovranità digitale implica "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace — avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries." Per un resoconto si rinvia a F.S. Gady, *The Wuzhen Summit and the Battle over Internet Governance*, in *The Diplomat* (14.1.2016), thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/; A. Chander, *The Asian Century?*, 44 U.C. Davis L. Rev. 717, 727 (2011); A. Chander, H. Sun, *Sovereignty 2.0*, cit.

[64] W. Cong, *The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics* (2.9.2021), ssrn.com/abstract=4019797.

[65] Cf. H.S. Gao, *Data Regulation with Chinese Characteristics*, cit.

[66] A. Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 Ohio St. Tech. L.J. 395 (2020); J. Fallows, *The Connection Has Been Reset*, in Atlantic, 3/2008, www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/.

[67] Cf. Art. 37 *Cyber Security law* ("Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State network information departments and the relevant departments of the State Council to conduct a security assessment; but where laws and administrative regulations provide otherwise, follow those provisions.").

[68] Cf. R. Creemers, *China's Long and Winding Road in Global Cyberspace. Great Power Relationships or Common Destiny?* (31.1.2021), ssrn.com/abstract=3776814.

[69] Art. 2 *Data Security Law* (2021) ("This Law shall apply to data processing activities and security supervision and regulation of such activities within the territory of the People's Republic of China. Where data processing outside the territory of People's Republic of China harms the national security, public interests, or the lawful rights and interests of individuals or organizations of the People's Republic of China, legal liability shall be investigated in accordance with the law.").

DPCE online
ISSN: 2037-6677

disciplinare la circolazione transfrontaliera dei dati, anche l'ordinamento cinese attua meccanismi che favoriscono l'estensione della portata territoriale delle norme ai dati oggetto di trattamento al di fuori del territorio cinese, subordinando la circolazione dei dati ad una verifica sulla sicurezza non dissimile dall'*adequacy decision* europea.[70]

I trattati internazionali costituiscono la principale riprova di queste linee di tendenza. Mentre in una fase iniziale la circolazione dei dati non era neppure inclusa nei trattati sul commercio conclusi dalla Cina, negli ultimi anni questa posizione si è modificata notevolmente.[71] La *Global Initiative on Data Security* ha ottenuto il supporto, tra gli altri, di Russia, Pakistan, Cambogia, ASEAN e Lega Araba.[72] Allo stesso modo, la c.d. *Digital Silk Road* - la componente tecnologica della più ampia iniziativa che prende il nome di *Belt-Road Initiative*, con la quale la Cina fornisce aiuto tecnico e commerciale a diversi paesi della regione – svolge un ruolo centrale nell'espansione delle politiche cinesi in tema di digitale, esercitato in nome di una "comunità dal destino comune"[73], suscitando le decise reazioni del Dipartimento di Stato americano, che ha tacciato questa strategia come un'esportazione dell'autoritarismo cinese.[74] Infine, la Cina esercita uno stretto controllo sulle

[70] Cf. Art. 38 PIPL ("1.A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements: (1) passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law; (2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department; (3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and (4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department. 2. Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulates conditions for providing personal information for a party outside the territory of the People's Republic of China, such stipulations may be followed. 3. The personal information processor shall take necessary measures to ensure that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in this Law.").

[71] Con il *Regional Comprehensive Economomic Partenership* del 2020 (RCEP), concluso con altri quattordici paesi dell'area, la Cina si è impegnata a promuovere la libera circolazione dei dati, impedendo barriere commerciali alla loro circolazione e misure di localizzazione, rcepsec.org/legal-text/. Sul punto si rinvia a M. Burri, *Digital Trade Rulemaking in Free Trade Agreements*, in corso di pubblicazione in D. Collins, M. Geist (eds), *Handbook on Digital Trade*, Cheltenham, 2023, ssrn.com/abstract=4281650.

[72] Ministry of Foreign Affairs of China, *Global Initiative on Data Security*, 29.10.2020, www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/202010/t20201029_9869292.shtml.

[73] Cf. M.S. Erie, T. Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, 54 *New York University Journal of International Law and Politics* 1 (2021); R. Creemers, *China's Long and Winding Road in Global Cyberspace. Great Power Relationships or Common Destiny?*, cit.

[74] State Department, *The Elements of the China Challenge* 17 (2020) ("Beijing provides digital technology and physical infrastructure to advance the CCP's authoritarian objectives throughout the [Indo-Pacific] region"); White House, *National Security*

attività delle imprese cinesi all'estero, come mostra il caso dell'app cinese di *ride-hailing* Didi, rimossa dagli *app store* cinesi per ragioni di sicurezza, dopo la sua quotazione alla borsa di New York.[75]

7. Declamazioni teoriche e regole operazionali

A dispetto dell'apparente inconciliabilità di fondo delle tre narrazioni proposte, un'analisi per formanti disvela una contraddizione tra declamazioni teoriche e regole operazionali e una parziale convergenza di soluzioni.[76] Il peso di principi e valori solennemente proclamati – mercato, diritti e sicurezza - esce spesso ridimensionato da un'analisi di dettaglio delle regole giuridiche di ciascuna delle tradizioni in esame.[77]

a) Stati Uniti d'America. Sul piano declamatorio la narrazione tipica del modello nordamericano – incentrata su una visione della sfera digitale come luogo per il libero scambio di idee, beni e servizi - si riflette nei documenti ufficiali, i quali si caratterizzano per riferimenti costanti ai "valori

Strategy, 2017, 25 ("China gathers and exploits data on an unrivalled scale and spreads features of its authoritarian system, including corruption and the use of surveillance"), trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. Sul punto v. anche C. Cheney, *China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*, in *Pacific Forum. Issues & Insights. Working Paper*, vol. 19, 2019, pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf; S. Feldstein, *The Global Expansion of AI Surveillance*, in *Carnegie Endowment for International Peace*, 2019, carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf; J. Parkinson, N. Bariyo, J. Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, in *The Wall Street Journal*, 15.9.2015; L. Khalil, *Digital Authoritarianism, China and COVID*, Lowy Institutes, 2020, www.lowyinstitute.org/publications/digital-authoritarianism-china-covid; A. Polyakova, C. Meserole, *Exporting digital authoritarianism* 5-6 Brookings, 2019, www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf; M. Wang, *China's Techno-Authoritarianism Has Gone Global*, in *Foreign Affairs*, 8.4.2021.

[75] V. Liu, Y. Luo, *China Initiates Cybersecurity Review of Didi ChuXing and Three Other Chinese Mobile Applications*, Covington. Inside Privacy (6.7.2021), www.insideprivacy.com/international/china/china-initiates-cybersecurity-review-of-didi-chuxing-and-three-other-chinese-mobile-applications/; L. Qiaoyi, Z. Hongpei, *3 more internet firms scrutinized amid rising data security concern*, Global Times (China), 5.7.2021, www.globaltimes.cn/page/202107/1227899.shtml.

[76] La distinzione tra declamazioni teoriche e regole operazionali si deve a Rodolfo Sacco. Cf. R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law*, 39 *Am. J. Comp. L.* 1 - 343 (1991).

[77] Nella letteratura comparatistica la tesi della convergenza di regole operative è stata oggetto di aspre critiche, soprattutto nella sua nota formulazione in termini di presunzione (c.d. *praesumptio similitudins*) resa celebre da K. Zweigert, H. Kötz, *Introduction to Comparative Law*, Oxford, 1998, 3° ed. La riflessione successiva ha messo in luce come non ci siano conclusioni generale che possano trarsi in relazione ad una tendenza generale alla convergenza o divergenza tra declamazioni teoriche e regole operazionali. Sul punto ci si limita a rinviare alle riflessioni dello stesso R. Sacco, *Diversity and Uniformity in the Law*, in 49 *Am. J. Comp. L.* 171 (2001).

DPCE online
ISSN: 2037-6677

americani"[78], con una particolare enfasi su libero mercato e innovazione.[79]
Più che autentica espressione di scelte culturali e valoriali, secondo molti osservatori questa retorica avrebbe un carattere strategico. La confluenza di interessi pubblici e interessi privati, che si realizza sul suolo americano condizionando le scelte politiche, sarebbe alla base del peculiare regime giuridico. Patria di grandi imprese tecnologiche che detengono la maggior parte dei dati a livello globale, la visione americana della sfera digitale sarebbe funzionale a favorire i colossi americani del web attraverso la libera accumulazione di dati.[80]
La distanza tra declamazioni e regole tanto nelle politiche interne che, in modo più interessante, nelle sue proiezioni esterne disvelerebbero la natura strumentale dell'adesione a tali valori e principi. Sul piano interno, sono note le critiche ad un impianto normativo che non ostacola la concentrazione dei mercati[81] e favorisce un sistema di sorveglianza e di estrazione dei dati che spinge l'utente a delegare alle piattaforme le proprie scelte, con l'effetto di pregiudicare l'autonomia individuale[82]: una *de facto digital corporate sovereignty* così efficace da imporre all'interprete un ripensamento della

[78] A titolo di esempio, di vedano Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; Trump White House Archives, *Artificial Intelligence for the American People*, 2021, trumpwhitehouse.archives.gov/ai/.

[79] Così E. Hine, L. Floridi, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*, cit.

[80] Cf. A. Chander, H. Sun, *Sovereignty 2.0*, cit. ("This is because the United States is in the unique position of being home to many of the world's leading technology firms. This means that during the ordinary course of regulating its companies, the U.S. exercised data sovereignty from the start."); O. Pollicino, *Judicial Protection of Fundamental Rights in the Internet. A Road Towards Digital Constitutionalism?*, cit., 174 ("From this point of view, the US has in some way exported its paradigm of protection for fundamental rights through online platforms, the terms and conditions of which were heavily influenced, at least at least initially, by First Amendment lawyers.").

[81] La letteratura sul tema è amplissima. Per una prima ricognizione si rinvia a A. Ezrachi, M.E. Stucke, *Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy*, Cambridge-US, 2016; M. Patterson, *Antitrust Law in the New Economy. Google, Yelp, LIBOR, and the Control of Information*, Cambridge-US, 2017.

[82] Anche in questo caso la letteratura sul tema è amplissima. Per una prima ricognizione si rinvia in primo luogo ai lavori seminali di S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Londra, 2019; e D. Lyon, *The Culture of Surveillance*, 2018. Con specifico riferimento al diritto nordamericano si vedano, tra gli altri, R. Calo, *Digital Market Manipulation* 82(4) *Geo. Wash. L. Rev.* 995 (2014); R. Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986 (2008); J. Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 *J. Tech. L. & Pol'y* 123 (2010); F. Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, 17 *Theoretical Inquiries L.* 494 (2016); J.M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation* 51 *U.C.D. L. Rev.* 1149 (2018); K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech* 131 *Harv. L. Rev.* 1598 (2018); E. Goldman, *The Complicated Story of Fosta and Section 230* 17 *First Amend. L. Rev.* 279 (2019).

nozione stessa di sovranità.[83]

Sul piano esterno, le contraddizioni del modello americano emergerebbero innanzitutto dal diverso atteggiamento assunto nei confronti di imprese che hanno sede fuori dal proprio territorio ed i cui dati siano localizzati all'estero, specialmente se tali imprese siano in mani cinesi.[84] In tutti questi casi, il diritto americano è pronto ad invocare ragioni tanto di sicurezza quanto di tutela dei diritti individuali per limitare la circolazione dei dati[85], come mostrano i più recenti trattati sul commercio conclusi dagli Stati Uniti e molte scelte di politica industriale[86], che sembrano fare spazio sempre maggiore ad eccezioni basate sulla sicurezza.[87]

Il carattere strategico dell'invocazione di ragioni di sicurezza sembra ulteriormente confermato dalla latitudine con cui tale argomento è impiegato, al punto da ricomprendere l'autosufficienza dell'economia

[83] Così, L. Floridi, *The Fight for Digital Sovereignty* ("The real point is that, between companies and states, the former can determine the nature and speed of change, but the latter can control the direction of change.".) Di una vera e propria "Magna Carta dell'impunità aziendale" parla F. Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, cit.

[84] *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 474-75 (S.D.N.Y. 2014). Il culmine di quella che è stata definita la guerra fredda tecnologica tra Stati Uniti e Cina si è consumata con l'arresto della Chief Financial Officer e figlia del fondatore di Huawei, Meng Wanzhou. Per una ricostruzione della vicenda si rinvia a R. Creemers, *China's Long and Winding Road in Global Cyberspace. Great Power Relationships or Common Destiny?*, cit.

[85] *Executive Order on Addressing the Threat posed by TikTok*, Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (6.8.2020) ("Any person or with respect to any party, subject to the jurisdiction of the United States" would be prohibited from transacting with ByteDance Ltd., the Chinese owner of Tik Tok, or any of its subsidiaries); *Executive Order on Addressing the Threat posed by WeChat* Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (6.8.2020) (order prohibits "any transaction that is related to WeChat (…) with TenCent Holdings Ltd., Shenzhen, China, or any subsidiary of that entity"); Pres. Proc. No. 10,061, 84 Fed. Reg. 51, 295 (ordering ByteDance to divest all of its rights and interests in any assets or property used to enable or support the operation of TikTok in the United States, and "any data obtained or derived from TikTok or Music.ly application users in the United States" within 90 days.); Press Release, *U.S. Dep't of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States* (18.9.2020), 2017-2021.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.html; Press Release, *U.S. Dep't of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States* (18.9.2020), 2017-2021.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.html.

[86] Per una ricognizione sul tema cf. J. Benton Heath, *Trade and Security Among the Ruins*, 30 *Duke Journal of Comparative and International Law* 223, 228 (2020) ("domestic industrial policy—meaning the protection of emerging or declining industries —is increasingly taking on a national security cast, particularly in the United States under President Trump.").

[87] Cf. art. 29.2(b) Comprehensive and Progressive Agreement for Trans-Pacific Partnership - CPTPP (Security Exceptions); art. 32.2(1)(b) US–Mexico–Canada Agreement – USMCA (Essential Security); art. 4(b) US-Japan Digital Trade Agreement (Security Exceptions).

DPCE online
ISSN: 2037-6677

americana e la competitività delle sue imprese[88]: una "nuova" sicurezza nazionale – come è stata ribattezzata - più ampia ed elastica di quella tradizionale, funzionale ad attuare una sorta di protezionismo camuffato a danno della globalizzazione degli scambi.[89]

b) Europa. Anche per l'Europa si registra un contrasto tra le declamazioni teoriche e le regole operative, e anche in questo caso ad essere chiamate in cause sono scelte strategiche. In assenza di competenze in materia di sicurezza, riservate ai singoli Stati Membri[90], il linguaggio dei diritti e l'enfasi sulla tutela della persona e della privacy degli individui utilizzati dall'Unione europea divengono una scelta obbligata nella creazione di una narrazione unitaria. Simili richiami rispondono all'esigenza di affermare una competenza dell'Unione in tema di circolazione dei dati, fondata attraverso riferimenti alla Carta dell'UE e alla disciplina in tema di protezione dei dati personali.

A questa prima ragione istituzionale se ne aggiunge una seconda, che guarda alle caratteristiche e soprattutto alle debolezze dell'economia del Vecchio continente. L'assenza di grandi imprese tecnologiche sul suolo europeo spiegherebbe l'atteggiamento più restrittivo in tema di circolazione dei dati.[91] È per questo molti commentatori[92] e soprattutto le principali

[88] Lo sostengono, tra gli altri, Y.C. Chin, Z. Jingwu, *Governing Cross-Border Data Flows: International Trade Agreements and Their Limits*, cit., i quali rintracciano una simile tendenza in una serie di documenti governativi; White House, *National Security Strategy*, 2017, cit.; White House, *A Proclamation on Adjusting Imports of Steel into the United States*, 31.3.2022, www.whitehouse.gov/briefing-room/presidential-actions/2022/03/31/a-proclamation-on-adjusting-imports-of-steel-into-the-united-states-2/.

[89] Sulla centralità acquisita dalle questioni di sicurezza nazionale nel contesto del commercio globale si rinvia a J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 *Yale Law Journal* 1020, 1044 (2020); G. Vidigal, *WTO Adjudication and the Security Exception: Something Old, Something New, Something Borrowed – Something Blue?*, 46(3) *Legal Issues of Economic Integration* 203 (2019); H. Farrell, A.L. Newman, *Of Privacy and Power. The Transatlantic Struggle over Freedom and Security*, Princeton, 2019, p. 174; A. Roberts, H.C. Moraes, V. Ferguson, *Toward a Geoeconomic Order in International Trade and Investment*, 22 *Journal of International Economic Law* 655 (2019).

[90] Considerando 16 GDPR ("Il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.").

[91] Cf. I. Bremmer, *The Technopolar Moment: How Digital Powers Will Reshape the Global Order*, in *Foreign Affairs*, 1.11.2021 ("Nonstate actors are increasingly shaping geopolitics, with technology companies in the lead. And although Europe wants to play, its companies do not have the size or geopolitical influence to compete with their American and Chinese counterparts").

[92] Cf. F. Burwell, K. Propp, *The European Union and the search for digital sovereignty: Building 'Fortress Europe' or preparing for a new world?*, in *Atlantic Council*, 6/2020, www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/; H. Gao, *Data sovereignty and trade agreements: Three digital kingdoms*, 10/2021,

istituzioni statunitensi[93] hanno giudicato con scetticismo l'attenzione europea ai diritti, con l'accusa neppure troppo velata di limitare il libero flusso dei dati attraverso la creazione di misure protezionistiche mascherate.[94]

Ad essere contestato è, in particolare, il diverso bilanciamento tra libera circolazione dei dati e ragioni di sicurezza che opera per i paesi terzi e per gli Stati membri, i quali pure continuano a mantenere piena autonomia in materia di sicurezza.[95] Come emerge dalle decisioni Schrems I e Schrems II, l'Europa si mostra molto attenta a richiamare l'esigenza di un bilanciamento degli interessi in gioco nel fissare i limiti alla circolazione dei dati in ragione della tutela degli interessi individuali.[96] Allo stesso tempo, però, manca di esercitare

papers.ssrn.com/sol3/papers.cfm?abstract_id=3940508; K. Propp, *Waving the flag of digital sovereignty*, in *New Atlantist*, 11.12.2019, il quale individua nell'incapacità europea di far emergere grandi attori privati in ambito digitale la ragione di alcune misure. In particolare, secondo quanto riporta questo articolo, il 92 percento dei dati del mondo occidentale è archiviato negli Stati Uniti. Sei delle dieci aziende tecnologiche più grandi del mondo sono americane, nessuna è europea. Amazon Web Services (AWS), detenga un terzo del mercato globale di server esterni che ospitano dati aziendali. Microsoft e Google seguono a breve distanza, rispettivamente con il 16% e il 7,8% della quota di mercato.

[93] A proposito delle indagini delle autorità europee su Facebook e Google il Presidente americano Obama ha dichiarato: "[O]ftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests.". Per una riflessione sul tema si rinvia a K. Swisher, *White House. Red Chair Obama Meets Swisher*, Re/Code (15.2.2015), www.vox.com/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher. Vedi, inoltre, United States International Trade Commission, *Digital Trade in the U.S. and Global Economies. Part 2*, (2014), p. 14, www.usitc.gov/publications/332/pub4485.pdf; U.S. Trade Representative, *National Trade Estimate Report on Foreign Trade Barriers*, 2021, p. 216 (2021); M. Scott, *What's driving Europe's new aggressive stance on tech*, Politico, 28.10.2019, www.politico.com/news/2019/10/28/europe-technology-silicon-valley-059988. Sul punto si vedano le dichiarazioni rese dal Commissario europeo per il mercato interno e i servizi Thierry Breton, *Questions to the Commissioner-Designate Thierry Breton*, European Commission, 2019, ec.europa.eu/commission/commissioners/sites/default/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf.

[94] Sul punto si veda R. Creemers, *China's conception of cyber sovereignty: rhetoric and realization*, in D. Broeders, B.van den Berg (eds.), *Digital Technologies and Global Politics*, Lanham, 2020, 177; S. Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74(2) *University of Miami Law Review* 416 (2020).

[95] Cf. J.P. Meltzer, *The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security*, August 5, 2020, Brookings, www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

[96] Cf. C-131/12, *Google Spain SL and Google Inc v Agencia Española de Protectión de Datos (AEPD) and Mario Costeja Conzález*, § 81 ("Vista la gravità potenziale di tale ingerenza, è giocoforza constatare che quest'ultima non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati. Tuttavia, poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto

un'analoga valutazione rispetto alla circolazione interna all'Unione[97], pur in assenza di garanzie equivalenti a quelle richieste ai paesi terzi.[98]

In modo simile, si sottolinea la contraddizione insita in una narrazione fondata sulla protezione dei dati come diritto fondamentale dell'individuo che però pone limitazioni anche alla libera circolazione dei dati non personali.[99] Simili ostacoli – è facile concludere – non possono trovare fondamento nella retorica dei diritti e delle tutele della persona ma, più pragmaticamente, nella preoccupazione di favorire la nascita di campioni nazionali e di imprese europee finalmente in grado di competere con i colossi americani e cinesi.[100]

equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica.").

[97] Cf. Art. 1, co. 3, GDPR ("La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.").

[98] Così, J. Sanchez, TikTok, *Schrems II, and Cross- Border Data Flows*, in *Cato Institute – Cato at Liberty*, 6.7.2021, www.cato.org/blog/tiktok-schrems-ii-cross-border-data-flows. Da segnalare, a questo riguardo, anche la decisione della Commissione europea di imporre ai propri dipendenti di disinstallare TikTok dai propri cellulari per ragioni di sicurezza. Cf. M. Sweney, *European Commission bans staff using TikTok on work devices over security fears*, in *The Guardian*, 23.2.2023, theguardian.com/technology/2023/feb/23/european-commission-bans-staff-from-using-tiktok-on-work-devices.

[99] Il riferimento è al Regolamento (EU) 2022/868, 30.5.2022, *on European data governance and amending Regulation* (EU) 2018/1724 (*Data Governance Act*) PE/85/2021/REV/1, OJ L 152, 3.6.2022) e alla *Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data* (*Data Act*) COM/2022/68 final), oltre a che alla legislazione di settore, come ad esempio la *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, COM/2022/197 final. Sul punto si vedano le considerazioni di O. Moerel, P. Timmers, *Reflections on Digital Sovereignty*, in *EU Cyber Direct, Research in Focus series*, 2021, p. 4, ssrn.com/abstract=3772777; S. Yakovleva, *EU's narratives and trade policy on data flows compared to US and China: towards a multilateral consensus, the end of multilateralism or eclipse of the 'Brussels effect'?*, cit.; Id., *Editorial: On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows* (22.9.2022), in 49(4) *Legal Issues of Economic Integration* 339 (2022), *Amsterdam Law School Research Paper* No. 2023-03, Institute for Information Law Research Paper No. 2023-01, ssrn.com/abstract=4320767.

[100] Si vedano, ad esempio, le dichiarazioni riprese dalla stampa del Commissario europeo Thierry Breton ("European data will be used for European companies in priority, for us to create value in Europe."). Per un commento critico cf. F. Burwell, K. Propp, *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?*, in *Atlantic Council* 1, 6 (2020), www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf. Sul punto si veda anche Foo Yun Chee, *This is the EU's plan to compete with Silicon Valley*, in World Economic Forum, 2/2020, www.weforum.org/agenda/2020/02/eu-data-market-

c) Cina. Anche le posizioni cinesi in tema di dati sono spesso spiegate facendo ricorso a ragioni strategiche. In primo luogo, le rivendicazioni di sovranità da parte delle autorità cinesi - con il corredo di dichiarazioni sulle esigenze di sicurezza e sui rischi connessi alla dipendenza da infrastrutture tecnologiche in mano straniera[101] - farebbero da giustificazione ad un controllo pervasivo dei contenuti ed all'esercizio di censura, espressione di un modello di governo autoritario.

Ma non è solo questione di autoritarismo e censura. Accanto a queste preoccupazioni ci sarebbero, anche in questo caso, ragioni di mercato e di promozione degli interessi economici nazionali. La tendenza a trattare la materia della circolazione dei dati attraverso le ordinarie norme sul commercio internazionale, anziché con disposizioni specifiche sulla sfera digitale, chiama in causa le peculiari caratteristiche delle imprese locali, specializzate soprattutto nel settore della vendita di beni, anziché della fornitura di servizi come per le imprese americane. Allo stesso modo, la minor attenzione alla libera circolazione dei dati sarebbe frutto di una peculiarità dell'economia cinese, con la maggior parte dei grandi operatori del digitale che operano in via esclusiva o principale nel mercato interno, a differenza dei colossi del web americani la cui proiezione è quasi sempre globale.[102]

Anche in questo caso un'analisi del dato operativo sembra condurre a esiti più sfumati e talvolta in contrasto con le declamazioni di principio. In questi ultimi anni si è realizzata una significativa inversione di tendenza, frutto della presa d'atto degli effetti negativi per il commercio di simili politiche di localizzazione dei dati[103], che ha spinto a significative aperture tanto nella normativa interna[104]

technology-silicon-valley.

[101] Cf. il Discorso di Xi Jinping in occasione della Cybersecurity and Informatization Work Conference, China Copyright and Media (19.4.2016), chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ ("the fact that [the internet's] core technology is controlled by others is our greatest hidden danger"). Per una riflessione critica sul punto si rinvia a A. Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*; www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm.

[102] Così H. Gao, *Digital or trade? The contrasting approaches of China and US to digital trade*, 21(2) *Journal of International Economic Law*, 297 (2018).

[103] SICS Cyber Research Institute, *Study on Global Cross-border Data Flow and China's Strategy*, SICS Cyber Research Institute, 2019, www.sicsi.net/Upload/ueditor_file/ueditor/20200217/1581933527865681.pdf; S. Donnan, T. Mitchell, *Chinese laws prompt global business backlash*, in *Financial Times*, 11.8.2016, www.ft.com/content/8103baa0-5f9c-11e6-ae3f-77baadeb1c93. Sul punto si rinvia alle considerazioni di W. Cong, *The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics* cit.

[104] Cf. Data Security Law – Art. 7 ("The state shall protect the data-related rights and interests of individuals and organizations, encourage the lawful, reasonable, and effective use of data, ensure free flow of data in an orderly manner and in accordance with the law, and promote the development of a digital economy with data as the key factor."); Art. 11 ("The state shall actively carry out international exchanges and cooperation in fields such as data security governance and data development and

quanto nei trattati internazionali.[105] L'enfasi sul carattere securitario e autoritario cinese, fatto di localizzazione dei dati e fondato su una nozione ampia di sicurezza, non tiene nel debito conto le aperture alla circolazione transfrontaliera dei dati quando ciò sia funzionale alle esigenze del paese.[106] E la centralità delle ragioni di sicurezza cede il passo ad un'invocazione dei diritti individuali dei cittadini cinesi e perfino delle ragioni del mercato e della libera circolazione dei dati, in reazione a misure restrittive messe in atto dal governo nordamericano.[107]

8. Legislatori e corti

La scomposizione in formanti offre anche un'altra importante conclusione sulla presunta convergenza di soluzioni. Le decisioni della Commissione europea sull'adeguatezza del sistema nordamericano di protezione dei dati, le proposte di introdurre normative in tema di privacy da parte di molti Stati americani[108], l'inclusione in molti trattati sul commercio internazionale di eccezioni simili in tema di libera circolazione dei dati, l'introduzione nel nuovo codice civile cinese di un capitolo su protezione dei dati e privacy all'interno della sezione dedicata ai diritti della personalità (art. 1035) e le notevoli somiglianze tra GDPR e PIPL[109], sono tutti indici di un fitto

utilization, participate in the formulation of relevant international rules and standards for data security, and promote the safe and free flow of data across borders."). Questa inversione di tendenza è ancora più marcata nel Personal Information Protection Law. Cf. Art. 1 ("This Law is enacted in accordance with the Constitution for the purposes of protecting the rights and interests on personal information, regulating personal information processing activities, and promoting reasonable use of personal information.").

[105] Art. 12.15, Regional Comprehensive and Economic Partnership ("RCEP") 2020 ("Cross-border Transfer of Information by Electronic Means"). 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. 2. A Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person.3. Nothing in this Article shall prevent a Party from adopting or maintaining: (a) any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

[106] Così L. Zhang, P. Zhiyi, *The Influence of China's International Rules on Data Security Needs to Be Improved*, 3:27-32 *Information Security and Communication Privacy* (2022), www.cnki.com.cn/Article/CJFDTotal-TXBM202203003.htm.

[107] Cf. Reuters, *China says U.S. TikTok, WeChat bans break WTO rules*, 5.10.2020, www.reuters.com/article/us-usa-tiktok-ban-wto/china-says-u-s-tiktok-wechat-bans-break-wto-rules-idUSKBN26Q26O.

[108] Per una panoramica si rinvia a A. Chander, M.E. Kaminski, W. McGeveran, *Catalyzing Privacy Law*, cit., 1768 ("Since the advent of the GDPR and the CCPA, the United States seen an unprecedented volume of legislative proposals that would regulate data privacy at the state level.").

[109] N. Zhu, *What kind of Personal Information Protection Law Do We Need?*, in *Legal Daily*,

dialogo tra i legislatori che, a dispetto delle premesse, sembra trovare importanti punti di convergenza.[110]

La circolazione dei modelli avviene anche nel dialogo tra corti.[111] Allo stesso tempo, il formante giurisprudenziale sembra farsi portatore più intransigente del modello di cui è espressione. La celebre saga *Schrems*, nella quale la Corte di Giustizia UE ha smentito la Commissione europea in due distinte occasioni, mostra chiaramente questa diversità. Com'è noto, sia il primo (*Safe Harbour*)[112] che il secondo accordo (*Privacy Shield*)[113] sono stati invalidati dalla Corte di Giustizia per il mancato raggiungimento di un "adequate level of protection" dei diritti e delle libertà fondamentali dei cittadini europei. Distaccandosi dalle conclusioni della Commissione, nelle due decisioni la Corte ha sottolineato la radicale diversità tra modello americano ed europeo quanto a contemperamento degli interessi in gioco, ed i rischi insiti nel diritto americano di ingerenze nella sfera dei diritti

20.10.2020, www.legaldaily.com.cn/index/content/2020-10/20/content_8332111.htm; K. Xu, *Data Security Law: Location, Position and Institution Construction*, in 3 *Business and Economic Law Review*, 2019, 52; Y. Shi, *Network Borders of Sovereignty: From the Perspective of Regulating Cross-border Data Transmission*, in 37(9) *Journal of Intelligence* 160 (2018). In entrambi i casi la base per il trattamento dei dati è il consenso del singolo. D'altra parte, il principio del consenso al trattamento soffre di molte più eccezioni in Cina di quanto non accada in Europa Commentary, China's *Emerging Data Privacy System and GDPR*, Center for Strategic and International Studies, 9.3.2018, www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr. Secondo L. Lucas, *China's artificial intelligence ambitions hit hurdles*, in *Financial Times* (2018), www.ft.com/content/8620933a-e0c5-11e8-a6e5-792428919cee, queste novità hanno attribuito alla Cina il ruolo di guida asiatica in tema di tutela della riservatezza. D'altra parte, queste apparenti convergenze non possono far dimenticare le notevoli distanze di fondo tra i due modelli, a partire dal carattere non vincolante delle norme cinesi e del ruolo del tutto diverso delle autorità giudiziarie nell'attuazione delle disposizioni in parola. Sul punto si rinvia alle considerazioni di R. Huw, J. Cowls,·J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, 36 *AI & Society* 59 (2021).

[110] Per la tesi secondo cui il GDPR converga quanto ai suoi effetti pratici con la disciplina di altri ordinamenti, e in particolare, con il modello nordamericano, si vedano, tra gli altri, K.A. Bamberger, D.K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011); W. McGeveran, *Friending the Privacy Regulators*, 58 Ariz. L. Rev. 959 (2016). In senso opposto, A. Chander, M.E. Kaminski, W. McGeveran, *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733 (2021).

[111] Cf. K. Kowalik-Bańczyk, O. Pollicino, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, 17(3) *German Law Journal* 315, 2016.

[112] Commission Decision 2000/520/EC of July 26, 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the U.S. Department of Commerce, OJ L 215, 25.8.2000, p. 7-47. La decisione è stata invalidata dalla Corte di Giustizia in Case C-362/14, *Maximillian Schrems v Data Protection* Commissioner (Schrems I).

[113] Commission Implementing Decision (EU) 2016/1250 of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016, L 207, p. 1–112. La decisione è stata invalidata dalla Corte di Giustizia in Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (Schrems II).

DPCE online
ISSN: 2037-6677

fondamentali delle persone. In modo speculare, la posizione assunta dalle corti americane sulle decisioni presidenziali in tema di limitazione della circolazione dei dati per ragioni di sicurezza, invalidate in nome del *free speech* e dell'insufficienza delle ragioni di sicurezza addotte per limitare la libera circolazione dei dati e della mancata considerazione di alternative al divieto, mostrano un notevole rigore nella valutazione delle ragioni che possano legittimare un allontanamento dal generale principio di libera circolazione dei dati.[114]

9. Il dialogo tra ordinamenti e l'uso della comparazione

Questa costruzione delle identità nazionali o regionali nella sfera digitale si esprime spesso attraverso la contrapposizione tra le proprie scelte e quelle degli altri attori della competizione globale. I riferimenti ai diritti stranieri riguardano tanto l'uso obbligato o necessario quanto quello complementare o volontario della comparazione.[115] Con riferimento al primo, accanto ai

[114] *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 85 (D.D.C. 2020); *Maryland v. Trump*, 498 F. Supp. 3d 624, 642 (E.D. Pa. 2020). Cf. B. Allyn, *U.S. Judge Halts Trump's TikTok Ban, The 2nd Court To Fully Block The Action*, NPR 2020, www.npr.org/2020/12/07/944039053/u-s-judge-halts-trumps-tiktok-ban-the-2nd-court-to-fully-block-the-action?t=1609198010618&t=1611774870551.

[115] La letteratura in tema di uso della comparazione è molto ampia. Per una rassegna si rinvia a U. Drobnig, S. van Erp (eds.), *The Use of Comparative Law by Courts*, XIVth International Congress Of Comparative Law (Atene 1997), The Hague, 1999; A. Somma, *L'uso giurisprudenziale della comparazione nel diritto interno e comunitario*, Milano, 2001; AA.VV., *L'uso giurisprudenziale della comparazione*, in *Quaderni della Rivista trimestrale di diritto e procedura civile*, Milano, 2004; G. Alpa (ed.), *Il giudice e l'uso delle sentenze straniere*, Milano, 2005; B. Markesinis, J. Fedtke, *The Judge as Comparatist*, 80 *Tul. L. Rev.* 11 (2005); G. F. Ferrari, A. Gambaro, *Corti nazionali e comparazione giuridica*, Napoli, 2006; B. S. Markesinis, J. Fedtke, L. Ackermann, *Judicial Recourse to Foreign Law: A New Source of Inspiration?*, Londra, 2006; B. S. Markesinis, J. Fedtke, *Engaging with Foreign Law*, Londra, 2009; T. H. Bingham, *Widening Horizons: The Influence of Comparative Law and International Law on Domestic Law*, Cambridge, 2010; mi si consentito rinviare anche a G. Smorto, *L'uso giurisprudenziale della comparazione*, in *Europa e diritto privato* 223, 2010; V. Barsotti, V. Varano, *Il nuovo ruolo delle corti supreme nell'ordine politico e istituzionale. Dialogo di diritto comparato*, Napoli, 2012; M. Bobek, *Comparative Reasoning in European Supreme Courts*, Oxford, 2013; M. Gelter, M. M. Siems, *Language, Legal Origins, and Culture Before the Courts: Cross-Citations Between Supreme Courts in Europe*, 21 *Sup. Ct. Econ. Rev.* 215 (2013); T. Groppi, M-C. Ponthoreau (eds.), *The Use of Foreign Precedents by Constitutional Judges*, Londra, 2013; M. Gelter, M.M. Siems, *Citations to Foreign Courts—Illegitimate and Superfluous, or Unavoidable? Evidence from Europe*, 62 *Am. J. Comp. Law* 35 (2014); R. Hirschl, *Comparative Matters: The Renaissance of Comparative Constitutional Law*, Oxford, 2014; M. Andenas, D. Fairgrieve (eds.), *Courts and Comparative Law*, Oxford, 2015; D. S. Law, *Judicial Comparativism and Judicial Diplomacy*, 168 *U. of Pennsylvania L. Rev.* 927 (2015); R. Hirschl, *Judicial Review and the Politics of Comparative Citations: Theory, Evidence & Methodological Challenges*, in E.F. Delaney, R. Dixon (eds.), *Comparative Judicial Review*, Cheltenham, 2018; C. Lienen, *Judicial Constitutional Comparativism at the UK Supreme Court*, 39 *Leg. Stud.* 166 (2018); G. F. Ferrari (ed.), *Judicial Cosmopolitanism: The Use of Foreign Law in Contemporary Constitutional Systems*, Leiden, 2019; M. Graziadei, *The European Court of Justice at Work: Comparative Law on Stage and Behind the Scenes*, in 13

trattati internazionali e alle norme di conflitto – tipicamente considerati i casi per eccellenza di uso obbligato di un diritto extra-statuale - sono molti i meccanismi previsti a livello legislativo che impongono valutazioni di tipo comparatistico, come per la decisione di adeguatezza prevista dal GDPR.[116]
Ancor più interessante appare il ricorso alla comparazione quando non sia imposto da norme giuridiche. Una lettura dei documenti ufficiali e delle dichiarazioni delle più alte istituzioni dei tre attori globali mostra un assiduo e insistito richiamo ad ordinamenti stranieri in tutte e tre le tradizioni considerate.
Atteggiandosi a campioni del libero mercato, gli Stati Uniti criticano il modello europeo per il suo protezionismo[117] e soprattutto - a giudicare dalla frequenza con cui viene chiamato in causa nei documenti ufficiali - quello cinese per l'autoritarismo.[118]
Anche l'Europa fonda la propria narrazione su una contrapposizione con gli altri modelli. Se la Cina viene accusata di autoritarismo, censura e

J. Civ. L. Stud. 1 (2020); A.S. King, P.K. Bookman, *Travelling Judges*, 116 *Am. J. Int'l. L.* 477 (2022).

[116] Sulla dimensione comparatistica della decisione di adeguatezza e del sindacato operato dalla Corte di Giustizia si veda M. Graziadei, *The European Court of Justice at Work: Comparative Law on Stage and Behind the Scenes*, cit., 1. Sebbene a giudizio della Corte di Giustizia la valutazione di adeguatezza dell'ordinamento del paese terzo non implichi necessariamente che questo adotti un livello di protezione "identico" a quello garantito nell'ordinamento giuridico dell'UE, tale livello di protezione di libertà e diritti fondamentali deve però essere "sostanzialmente equivalente". Cf. Schrems II, par. 94 ("L'articolo 45, paragrafo 1, prima frase, del RGPD prevede che un trasferimento di dati personali verso un paese terzo può essere autorizzato mediante una decisione adottata dalla Commissione secondo la quale tale paese terzo, un territorio o uno o più settori specifici all'interno dello stesso garantiscono un livello di protezione adeguato. A tal riguardo, senza esigere che il paese terzo considerato garantisca un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, l'espressione «livello di protezione adeguato» deve essere intesa, come confermato dal considerando 104 dello stesso regolamento, nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza di tale regolamento, letto alla luce della Carta.").

[117] U.S. Trade Representative, *National Trade Estimate Report on Foreign Trade Barriers*, p. 216 (2021). Sul punto si veda S. A. Aaronson, *What are we talking about when we talk about digital protectionism?*, 18 *World Trade Review* 541 (2019).

[118] Office of the Secretary of State, *The Elements of the China Challenge* (2020), www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf; Office of the United States Trade Representative, *U.S. Statement on the Trade Policy Review of China* (2021), ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/us-statement-trade-policy-review-china. Cf. E. Hine, L. Floridi, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*, cit. ("Frequency analysis reveals that undergirding the American documents' emphasis on American technology and development is a competitive dynamic with China. While competition-related terms do not appear in the overall top focal words, China is mentioned in several of the documents" (…) China's documents, on the other hand, barely mention America").

DPCE online
ISSN: 2037-6677

repressione[119], anche gli Stati Uniti d'America suscitano diffidenza nell'osservatore europeo per la sua debole tutela della privacy e dei diritti della persona.[120] In questa conflitto tra le due opposte polarità, l'Europa viene presentata come terza via tra l'assenza di regole americana e l'autoritarismo cinese, ossia tra la violazione della privacy da parte del settore privato in nome del profitto e di una concezione dei dati come *commodity* e le derive autoritarie dello Stato in nome della sicurezza e di un controllo sui comportamenti individuali.[121]

Sebbene simili riferimenti siano presenti in misura minore nei documenti ufficiali, anche la Cina ha costruito la propria identità in tema di digitale attraverso il confronto con gli altri, frutto di una narrazione che enfatizza l'opportunità che l'innovazione tecnologica ha offerto a quei paesi che scontavano una forte arretratezza rispetto all'Occidente industrializzato, e che hanno avuto l'opportunità di saltare a piè pari la fase di sviluppo industriale e agganciare in un colpo solo i paesi più avanzati. La rivoluzione digitale è divenuta così un'opportunità irripetibile per la crescita di un sistema economico e per la modernizzazione di una società ancora legata all'agricoltura, in una competizione esplicita con le potenze occidentali, e in particolare con gli Stati Uniti, secondo la retorica del "catching up with the West".[122]

[119] Cf. Risoluzione del Parlamento europeo del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce (2019/2575(RSP)) (2021/C23/01), eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019IP0156&from=EL.

[120] Cf. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, 2 Dg Markt Doc. 5092/98, WP 15 (26.1.1999) ("the current patchwork of narrowly- focused sectoral laws and voluntary self-regulation cannot be relied upon to provide adequate protection").

[121] Cf. C. Michel, *Digital sovereignty is central to European strategic autonomy* – Discorso del Presidente Charles Michel, cit. ("In recent years, however, we have seen the abuse of personal data – the over-exploitation of data by companies in pursuit of profit. Or by states, like in China, for the purpose of controlling their citizens. We must use our new digital resources wisely to protect the "environment" of our fundamental values – democracy and individual freedoms. It is not only a political issue, it's also an economic one. We must ensure the sustainability of these resources. Citizens will not accept to be transformed into objects, to see their personal and consumption choices guided by secret algorithms." (…) "[b]etween an unregulated model and a state-controlled model we, Europeans, promote a human-centric, ethics-based approach, that serves our citizens."). Sulla via europea al digitale si veda anche U. Leyen, *Political guidelines for the next European Commission 2019-2024*. Opening statement in the European Parliament plenary session 16 July 2019. Speech in the European Parliament plenary session 27 November 2019, Publications Office of the European Union, 2020, data.europa.eu/doi/10.2775/101756.

[122] Cf. S. Lengen, *Digital Imaginaries and the Chinese Nation State*, in I. Ahmad, J., Kang (eds), *The Nation Form in the Global Age. Global Diversities*, Cham, 2022, at 207 ("Narratives of 'catching up with the West' discursively reinforce the unity of the nation state as a comparative unit (…) This drive to catch up with Western powers is an

10. Conclusioni

Un'indagine sull'uso della comparazione nella sfera digitale conduce a conclusioni che si pongono in linea di sostanziale continuità con la letteratura sul tema, pur se con importanti elementi di differenza.

In primo luogo, la centralità della comparazione nella sfera digitale conferma la tesi secondo cui i riferimenti a ordinamenti stranieri sono più frequenti in quelle materie che presentano elementi di novità e sulle quali non si siano ancora raggiunte soluzioni consolidate.[123] Sulla stessa linea, a rafforzare il dialogo tra ordinamenti contribuisce l'esigenza di un coordinamento tra le diverse soluzioni rispetto a materie che, per loro stessa natura, trascendono i confini nazionali.

Allo stesso tempo, l'uso della comparazione nella sfera digitale assume spesso tratti peculiari rispetto a quelli descritti in letteratura.

Tradizionalmente l'uso obbligatorio della comparazione riguarda le controversie in cui il riferimento al diritto straniero è imposto al giudice da fonti sopranazionali o da norme di conflitto. Nella sfera digitale, invece, l'uso obbligatorio della comparazione si distingue per la presenza di norme di diritto interno che impongono di effettuare un raffronto tra ordinamenti. Espressione paradigmatica di questo tipo di comparazione è la decisione di adeguatezza formulata dall'Unione europea come precondizione per la circolazione dei dati e il meccanismo analogo messo in piedi dal diritto cinese.

Anche sull'uso costruttivo o distruttivo della comparazione si registrano interessanti linee di discontinuità rispetto al passato. La letteratura comparatistica ha sempre concluso che, ove presente, il ricorso alla comparazione giuridica avvenga prevalentemente in chiave "costruttiva", allo scopo cioè di stabilire un'imitazione culturale tra modelli differenti.[124] In questo quadro, il richiamo ad esperienze giuridiche straniere serve a conferire legittimazione a scelte e interpretazioni diverse da quelle consuete

exercise in comparative nationalism "). Per una rassegna di esempi contenuti nelle dichiarazioni ufficiali delle massime autorità cinese si rinvia a R. Huw, J. Cowls,·J. Morley, M. Taddeo, V. Wang, L. Floridi, *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, cit., 63 ("The desire to leapfrog the US is echoed in statements from China's political and military leadership.").

[123] Sulla credenza di un diritto destinato fatalmente a dover riconcorrere l'evoluzione tecnologica Cf. Joshua A. T. Fairfield, *Runaway Technology can law keep up?*, Cambridge, 2021.

[124] Cf. A. Somma, *Le corti italiane e l'uso complementare dei modelli normativi extraterritoriali nel processo di armonizzazione del diritto in ambito comunitario*, in AAVV, *L'uso giurisprudenziale della comparazione giuridica*, cit., 25 ss., che distingue tra un uso "costruttivo" o "distruttivo" del modello alieno, a seconda che tale uso serva a incentivare l'evoluzione del diritto supportando soluzioni, anche contro il tenore letterale di alcune disposizioni o di alcuni orientamenti consolidati in dottrina e giurisprudenza, e con schemi usualmente ricondotti ad un testo normativo, promossi dalla letteratura o dalla prassi applicativa; ovvero a confermare le soluzioni già esistenti dichiarando l'estraneità di una certa soluzione rispetto all'esperienza giuridica di appartenenza.

DPCE online
ISSN: 2037-6677

attraverso un richiamo in senso adesivo a modelli stranieri, al fine di innovare l'ordinamento giuridico anche contro il tenore letterale di alcune disposizioni o di alcuni orientamenti consolidati. Mentre sono considerati decisamente rari gli impieghi del diritto straniero e comparato a fini distruttivi o di conservazione dei valori dell'ordinamento.[125] Come abbiamo visto in queste pagine, ciò che invece emerge nella sfera digitale è il netto prevalere di una comparazione di tipo "distruttivo".

Anche le ragioni di questa comparazione di tipo "distruttivo"si distaccano da quanto generalmente messo in luce in letteratura. Tipicamente alla base del rigetto del modello straniero sono quasi sempre le strettoie di carattere formale poste dal sistema delle fonti, espressione di un giuspositivismo statualistico che vede lo Stato come ordinamento esclusivo a validità territoriale entro il quale vale il principio *superiorem non recognoscentes*: un *horror alieni iuris* che spesso connota l'uso distruttivo della comparazione, frutto di una concezione statualistica e positivistica del diritto che porta a respingere la soluzione straniera come estranea all'ordinamento giuridico nazionale.

Al contrario, nella definizione delle politiche del digitale la presa di distanza dagli altri attori sembra svolgere una funzione diversa, finalizzata innanzitutto a tracciare le radici culturali del proprio modello. Come abbiamo visto, il richiamo al diritto straniero assume quasi sempre la funzione di marcare le differenze rispetto agli ordinamenti considerati ed è funzionale alla costruzione delle identità nazionali o regionali, spesso definite in contrapposizione alle scelte e alle preferenze espresse dagli altri. La comparazione giuridica diviene così uno strumento indispensabile per plasmare queste diverse identità.[126]

Infine, un'analisi per formanti ci offre strumenti di indagine utili per ricostruire il dialogo in atto tra ordinamenti nella sfera digitale. La rappresentazione a tinte nette delle scelte compiute nei tre diversi modelli passati in rassegna nasconde posizioni più sfumate e finisce per ammantare scelte in buona parte convergenti dietro ragioni e giustificazioni molto diverse. A dispetto della polarizzazione espressa a livello declamatorio, con giustificazioni che richiamano ragioni e principi differenti nel legittimare le proprie scelte, un'analisi delle regole operazionali rivela come ciascuno degli attori in campo operi un contemperamento di ragioni legate alla tutela dei

[125] Cf. A. Somma, *L'uso giurisprudenziale della comparazione nel diritto interno e comunitario*, cit., 287.

[126] Questo vale anche in quei rari casi in cui i riferimenti comparatistici sono volti a sottolineare la comunanza tra due modelli, finalizzati comunque a prendere le distanze da un terzo soggetto, come nel caso della pretesa convergenza europea e americana in tema di intelligenza artificiale rispetto al modello cinese. Cf. U.S.-EU Trade and Technology Council Inaugural Joint Statement. (29.9.2021), The White House, www.whitehouse.gov/briefing-room/statements-releases/2021/09/29/u-s-eu-trade-and-technology-council-inaugural-joint-statement/ ("our common democratic values and human rights (…) opposed to uses of AI that do not respect this requirement, such as rights-violating systems of social scoring").

diritti, alla difesa del libero mercato e alla sicurezza.
Le radici di questa distanza tra regole operative e declamazioni teoriche possono rintraciarsi tanto nelle ragioni strategiche analizzate in precedenza quanto in una sorta di *normative beautification* ad opera degli attori locali, ossia in una descrizione apologetica della propria tradizione culturale e giuridica, che non trova piena realizzazione nelle politiche effettivamente perseguite sul piano operativo.[127] Si spiegano in questa prospettiva la prevalenza nei documenti ufficiali di valutazioni di ordine emotivo rispetto a considerazioni di ordine strettamente tecnico.[128]

Le eccezioni contenute nei trattati internazionali - le quali attribuiscono, a dispetto delle diverse giustificazioni invocate[129], margini di manovra molto simili[130] - costituiscono la miglior riprova di questa confluenza di soluzioni, mostrando come sia soprattutto nella rivendicazione di un'autonomia nel controllo del flusso globale dei dati, e nella tendenza crescente ad ampliare la portata delle proprie norme oltre i confini territoriali di applicazione, che tale convergenza si realizza. In questo quadro, le diverse ragioni addotte dai diversi attori sembrano essere utilizzate per mantenere ampi margini di discrezionalità nel flusso transfrontaliero dei dati e per estendere il proprio raggio d'azione oltre i confini del territorio di riferimento, nella contesa oggi più che mai aperta per la sovranità digitale.

Guido Smorto
Dip.to di Giurisprudenza
Università degli Studi di Palermo
guido.smorto@unipa.com

[127] Sul punto cf. J.Q. Whitman, *The Neo-Romantic Turn*, in P. Legrand and R. Munday (eds), *Comparative Legal Studies: Traditions and Transitions*, Cambridge, 2003.
[128] Registrano questa tendenza E. Hine, L. Floridi, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*, cit., ai quali si rinvia per un'analisi terminologica basata sulla "sentiment analysis" dei testi normativi statunitensi e cinesi in tema di intelligenza artificiale.
[129] Un'analisi delle misure sulla circolazione dei dati contenute nei trattati sul commercio internazionale riflettono le differenze descritte, con gli Stati Uniti d'America promotori di un sistema di libera circolazione dei dati sul mercato, l'Europa maggiormente attenta alla tutela della privacy e dei diritti e la Cina che contempera queste due esigenze con quelle legate alla sicurezza. Cf. Y.C. Chin, Z. Jingwu, *Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. Laws*, cit.
[130] N. Cory, L. Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, ITIF, 19.7.2021, itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/. Oltre al richiamo alla sicurezza, è importante notare come considerazioni di sicurezza siano rimesse al giudizio insindacabile del Paese che le solleva. Sul punto si rinvia alle considerazioni di H. Gao, *Data sovereignty and trade agreements: Three digital kingdoms*, Hinrich Foundation, 2022, www.hinrichfoundation.com/research/article/digital/data-sovereignty-trade-agreements-digital-kingdoms/.