RIVISTA ITALIANA DI INFORMATICA E DIRITTO

PERIODICO INTERNAZIONALE DEL CNR-IGSG

diretta da Sebastiano Faro e Marina Pietrangelo

Anno III, n. 1/2021 • Periodicità semestrale • ISSN 2704-7318
Direzione e Redazione: Istituto di Informatica Giuridica e Sistemi Giudiziari • Via dei Barucci 20 - 50127 Firenze

1
2021

Consiglio Nazionale delle Ricerche

Rivista italiana di informatica e diritto
Periodico internazionale del CNR-IGSG
Anno III • n. 1/2021 • Periodicità semestrale

Direzione
Sebastiano Faro e Marina Pietrangelo

Comitato di direzione
Federigo Bambi, Davide Carnevali, Gian Luca Conti, Enrico Francesconi, Erik Longo
Elisabetta Marinai, Stefano Pietropaoli, Francesco Romano

Comitato scientifico nazionale
Laura Abba, Agata C. Amato Mangiameli, Andrea Cardone, Antonio Carcaterra, Paolo Caretti, Massimo Carli, Enrico Carloni, Adriana Ciancio, Renato Clarizia, Giuseppe Corasaniti, Pasquale Costanzo, Giovanna De Minico, Rosa Maria Di Giorgi, Elio Fameli Carla Faralli, Giusella Finocchiaro, Tommaso E. Frosini, Mario Jori, Donato A. Limone Aldo Loiodice, Luigi Lombardi Vallauri, Nicola Lupo, Nicoletta Maraschio, Paola Marsocci, Paolo Moro, Monica Palmirani, Ugo Pagallo, Giovanni Pascuzzi, Paolo Passaglia, Dianora Poletti, Oreste Pollicino, Giovanni Sartor, Andrea Simoncini, Carlo Sorrentino, Giancarlo Taddei Elmi, Lara Trucco, Stefano Trumpy, Alessandra Valastro Franco Vallocchia, Giovanni Ziccardi

Comitato scientifico dei corrispondenti stranieri
Y. Amoroso (C), T.J.M. Bench Capon (GB), D. Bourcier (F), W. Boyd (USA), V. De Mulder (NL), J. Dumortier (NL), F. Galindo (E), A. Gardner (USA), T. Gordon (D), G. Greenleaf (AUS), O.P. Hance (L), W. Kilian (D), F. Lachmayer (A), P. Leith (IRL), E. Mackaay (CAN) A. Maclntosh (GB), P. Maharg (GB), J. Mayor (USA), L.T. McCarty (USA), F. Novak (CZ) A. Paliwala (GB), A.E. Perez-Luño (E), R. Petrauskas (LT), L. Philipps (D), Y. Poullet (B) A. Saarempaa (FIN), E. Schweighofer (A), P. Seipel (S), R. Susskind (GB), W.R. Svoboda (A), H. Yoshino (J), T. Van Engers (NL), M.A. Wimmer (A), R. Winkels (NL), J. Zeleznikow (AUS)

Comitato dei revisori esperti per la valutazione
Fulvia Abbondante, Enrico Albanesi, Maria Romana Allegri, Marco Bassini, Raffaella Brighi, Elda Brogi, Simone Calzolaio, Giuseppe Cammarota, Gianluigi Ciacci, Sofia Ciuffoletti, Maria Vittoria Dell'Anna, Fabio Dell'Aversana, Rossana Ducato, Fernanda Faini, Paolo Galdieri, Riccardo Gualdo, Paolo Guarda, Antonio Iannuzzi, Alessandro Lovari, Daniele Marongiu, Letizia Materassi, Erica Palmerini, Saulle Panizza, Anna Papa, Viviana Patti, Giovanni Piccirilli, Benedetto Ponti, Cecilia Robustelli, Andrea Rossetti Simone Scagliarini, Caterina Sganga, Giuseppe Vaciago, Giulia Venturi

Redazione tecnica
Simona Binazzi (segreteria), Giuseppina Sabato (composizione dei testi), Elisabetta Marinai (sito web)

Direzione e Redazione
IGSG/CNR
Via dei Barucci, 20 • 50127 Firenze
telefono 055 43995 • fax 055 4399605 • RivistaRIID@igsg.cnr.it
www.rivistaitalianadiinformaticaediritto.it/index.php/RIID

Registrazione presso il Tribunale di Roma al n. 127/2019

Indice

Studi e Ricerche

Il diritto pubblico alla prova della conservazione e della circolazione dei dati nella società digitale

a cura di Simone Calzolaio

7 **Simone Calzolaio**
Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati

13 **Valentina Pagnanelli**
Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali

29 **Vanni Boncinelli**
Modelli tecnici e disciplina giuridica del c.d. cloud computing

49 **Stefano Torregiani**
La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa

69 **Yuan Li**
Cross-border Data Transfer Regulation in China

81 **Ciro D'Urso**
I profili informatici nella valutazione della responsabilità dell'Hosting Provider

91 **Alessandra Vernice**
Il letto di Procuste dei sistemi informativi via Web: un pluralismo falsato?

105 **Elena Montagnani**
La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia: quali prospettive future?

Note e Discussioni

141 **Laura Abba**
Carenze attuali e soluzioni future nei meccanismi per la cooperazione digitale

151 **Kelvin Peroli, Cíntia Rosa Pereira de Lima**
Democrazia come *Value-Sensitive Design*: un approccio sociotecnico allo sviluppo delle tecnologie basate su principi democratici

Recensioni

159 **Enrico Albanesi**
Roberto Zaccaria, Alessandra Valastro, Enrico Albanesi, *Diritto dell'informazione e della comunicazione*, XI edizione, Milano, Wolters Kluwer-Cedam, 2021

165 **Alessio Facciorusso**
Gianluigi Fioriglio, *Informatica medica e diritto. Un'introduzione*, Modena, Mucchi Editore, 2020

Il diritto pubblico alla prova della conservazione e della circolazione dei dati nella società digitale

a cura di Simone Calzolaio

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0035

Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati

Simone Calzolaio

La sezione della *Rivista italiana di informatica e diritto* ospita una serie di contributi in merito al regime giuridico della conservazione e della circolazione dei dati nella società digitale. Si intende introdurre sul piano metodologico il problema giuridico della localizzazione e disponibilità dei dati, come profilo attinente alla sovranità dello Stato contemporaneo.

Localizzazione dei dati – Sovranità digitale – Disponibilità dei dati – Dipendenza dai dati – Datificazione

Sommario: *1. Datificazione, Intelligenza artificiale,* data dependence – *2.* Ubi data, ibi imperium*: descrivere e individuare le questioni aperte, sotto il profilo giuridico – 3. Localizzazione dei dati, cognizione delle informazioni. Profili soggettivi della disponibilità di dati e informazioni – 4. Segue: profili oggettivi. La localizzazione e i suoi molteplici volti. L'ordinamento costituzionale al tempo della* data dependence.

1. Datificazione, intelligenza artificiale, *data dependence*

La realtà attuale rappresenta un contesto *data intensive*. Nel corso degli ultimi anni, ad avviso di chi scrive[1], la nozione che si presta meglio a descrivere la situazione attuale, anche per consentire una comprensione complessiva del fenomeno della cd. realtà digitale o altrimenti noto come *big data*, è quella di datificazione (*datification* o *datafication*).

La *datification* si compone di tre fattori essenziali: l'aumento esponenziale della quantità di dati prodotti nel mondo; la capacità di analisi dei dati e di estrazione di informazioni dai dati, svolta da parte di macchine a ciò addestrate; la possibilità e la capacità di prendere decisioni attraverso queste nuove informazioni, anche grazie alla cd. *alghoritmic decision making*.

Negli ultimi anni, la *datification* ha rappresentato un terreno fertile per lo sviluppo di tecnologie basate sull'intelligenza artificiale.

Le tecniche di *machine learning*, *deep learning*, *data mining* hanno bisogno di enormi quantità di dati, di buona qualità, per perfezionarsi, per riuscire a fornire a trarre informazioni dai dati e, di conseguenza, servizi sempre più raffinati e specifici.

L'insieme di questi fattori evidenzia che siamo in un contesto di *data driven innovation*; l'innovazione si realizza attraverso lo sfruttamento dei dati. In tutti i settori, e trasversalmente.

Ciò significa che anche la competizione e la concorrenza fra aziende, stati, continenti si gioca nella progressione della capacità di sfruttamento dei dati.

Questi aspetti lasciano capire perché il possesso e la disponibilità dei dati sono strategici, per le imprese, per gli stati, e per le imprese che operano nei diversi Stati.

Di più. Questo momento storico caratterizzato dalla pandemia rende evidente che l'avvento della *datification* e la *data-driven innovation* conducono ormai ad un contesto di data *dependence*[2]: non si tratta di sviluppare complessi ragionamenti, ma di

S. Calzolaio è professore associato di Diritto costituzionale presso il Dipartimento di Scienze politiche, della comunicazione e delle relazioni internazionali dell'Università degli Studi di Macerata.

arrendersi al fatto che il corso, il fluire, lo sviluppo della vita personale, sociale, economica, istituzionale dipende dal e segue il flusso dei dati. Siamo dipendenti dalla garanzia della continuità del flusso dei dati e delle informazioni per comunicare, esprimerci, operare, lavorare, vivere.

2. *Ubi data, ibi imperium*: descrivere e individuare le questioni aperte, sotto il profilo giuridico

Allo stato attuale, quindi, il contesto tecnologico, ma si potrebbe ben dire la realtà dei fatti, richiede al giurista uno sforzo non indifferente, che lambisce la domanda in ordine alla sua stessa identità e alle esigenze cognitive necessarie a consentire una comprensione dell'esistente e poi una regolazione giuridica orientata ai principi del costituzionalismo liberaldemocratico[3].

In qualche modo, in particolare sul versante del diritto pubblico, si sta sviluppando un vero e proprio diritto dei dati, che trae molte delle sue caratteristiche e dei suoi connotati dal modello europeo della protezione dei dati personali, ma che non coincide più e non si riduce più né alla protezione dei dati personali, né al diritto della proprietà intellettuale.

Il diritto pubblico è quella branca del diritto che si occupa – nel costituzionalismo occidentale – di regolare, e quindi di limitare, il potere dello Stato e di garantire la sovranità dello Stato e la tutela dei diritti delle persone (cittadini e non cittadini).

Il contesto tecnologico attuale, l'avvento della rete internet, del mondo digitale, della *datification* e dell'intelligenza artificiale, introduce un collegamento strutturale, e non temporaneo, fra disponibilità dei dati da parte degli Stati e *imperium*, cioè capacità di esercizio del potere sovrano. Con espressione sintetica: *ubi data, ibi imperium*.

L'espressione tuttavia va subito puntualizzata, senza pretesa alcuna di esaustività, sotto due profili.

Bisogna subito sottolineare che, in questo caso, perfino il termine "ubi" può e deve essere letto e declinato secondo le categorie del nuovo contesto tecnologico. Il luogo individuato dall'*ubi* può non essere uno spazio fisico, un territorio statale, un luogo unico e unitario. Affinché sia soddisfatta la formula (*ubi*... *ibi*...), non è affatto necessario pensare l'*ubi* come un luogo localizzato nel territorio dello Stato (su questo si veda il contributo di Valentina Pagnanelli).

Anche perché – ed ecco la seconda osservazione preliminare – affinché possa essere esercitato l'*imperium*, cioè il potere sui dati, quel che conta non è tanto la localizzazione dei dati, ma quella delle informazioni che se ne traggono e si riesce a trarne immediatamente e/o per correlazione con altri dati e altre informazioni (su entrambi questi aspetti – nei termini che di seguito si tenta di delineare – appare decisamente utile il contributo di Vanni Boncinelli).

Per queste ragioni, per il fatto di dover tener conto di un contesto tecnologico in cui il concetto di territorio si viene rimodulando, così come alcuni aspetti concernenti la distinzione fra popolo e popolazione, ed il correlativo concetto di monopolio del potere e della forza, si ritiene che il diritto pubblico sia chiamato ad una prova importante, forse epocale, come in realtà quasi tutti i settori della ricerca scientifica di fronte a questa quarta rivoluzione (secondo la lettura di Luciano Floridi[4]).

Quale metodo seguire per affrontare l'indagine scientifica della rivoluzione digitale in corso, anche solo rispetto al tema evocato, che tuttavia, come si intuirà, non è affatto facile anche solo da perimetrare?

Si ritiene, sommessamente, che il metodo debba necessariamente, in questa fase, essere descrittivo e interrogativo. Non ancora, o almeno non immediatamente, prescrittivo. Vi è infatti molto più da descrivere, da domandare e da capire, per il giurista (e non solo), di quanto si sia in grado di prescrivere con certezza o di certificare attraverso una prescrizione. Il primo passo di questa prova, pertanto, consiste nell'aprirsi non solo a nuovi temi, ma alle nuove categorie implicate dalla rivoluzione digitale: descrivere la fenomenologia, i nuovi istituti e concetti che emergono dall'esperienza, classificarli con timore e tremore, per avviarsi a comporre il nuovo mosaico del diritto pubblico dell'era digitale.

Qui non si sostiene affatto che mutino principi, diritti, criteri tipici e tradizionali del diritto pubblico. Non lo si può escludere apriori, ma è infantile trarre una conclusione del genere prima di descrivere analiticamente le fattispecie rilevanti e la loro intrinseca connessione. D'altra parte – come pure ancora il contributo di Vanni Boncinelli appare prospettare e fondare – non è affatto detto che un approccio tradizionale (localizzando i dati in un certo territorio statale si può garantire l'accesso illimitato alle informazioni portate da quei dati) sia in grado di raggiungere gli obiettivi prefissati (infatti, fra dato e informazione può collocarsi una capacità di criptografia dei dati che rende impossibile, allo Stato, l'accesso alle informazioni, pur essendo tutti i dati localizzati all'interno del territorio sovrano dello Stato). Pertanto, appunto, la questione prioritaria per il giurista è, in questo momento, riuscire a descrivere fattispecie che presentano un grado di novità

consistente. E questo è il tentativo che si sviluppa negli articoli di questa sezione.

3. Localizzazione dei dati, cognizione delle informazioni. Profili soggettivi della disponibilità di dati e informazioni

Di chi sono i dati? La domanda può apparire banale. In riferimento ai nostri dati personali tutti risponderemmo "i dati sono senz'altro miei!". Ovviamente non abbiamo letto le policies dei social network che utilizziamo!

Infatti, la domanda non è affatto banale. E la risposta non è affatto chiara o univoca.

I dati che circolano e sono prodotti in Italia, di chi sono? Cioè, a chi appartengono e chi può avervi accesso? Chi può analizzarli e di chi sono le informazioni che se ne ricavano?

Qui evidentemente non si possono affrontare e tantomeno risolvere questi quesiti.

Si può però osservare che un aspetto consistente dell'indagine scientifica dovrebbe necessariamente riguardare il rilievo pubblico e/o privato dei dati, e la relativa regolazione, pubblica e privata. In Cina – è sufficiente leggere l'articolo seguente di Yuan Li – hanno iniziato a porsi il problema, e con esiti interessanti sul piano del modello di disciplina (si pensi alla nozione di *important data* ed al relativo regime, che supera la ormai incompleta bipartizione europea dati personali/non personali).

In altri termini, è arrivato il momento che il diritto pubblico (altra questione in campo: il diritto pubblico italiano o europeo?) inizi a definire con una certa precisione quale è la situazione giuridica soggettiva che caratterizza il rapporto fra soggetto (privato e pubblico) e dato, e fra soggetto e informazione.

Cosa significa esattamente essere titolari dei dati? Cosa significa avere la disponibilità dei dati? Cosa significa aver diritto di accesso ai dati? Chi ha il diritto di utilizzare i dati? Questi diritti sono esclusivi? Il titolare dei dati è il proprietario? È il possessore? È il detentore? È una nuova figura giuridica che esula dagli istituti tradizionali del diritto "continentale" (*trust/trustee*)? E in che relazione è lo Stato con i dati e le informazioni, il cui insieme si rivela decisivo per garantire sicurezza, progresso, sovranità interna ed esterna dello Stato stesso?

Come è noto, almeno sotto il profilo del diritto della protezione dei dati personali, il GDPR offre una serie di risposte a questi quesiti. Ma si tratta ancora di risposte iniziali, parziali, nel senso che si riferiscono appunto ai dati personali, cioè a qualsiasi informazione concernente una persona fisica identificata o identificabile.

Il regolamento Europeo del 2018, concernente la libera circolazione dei dati non personali, non offre al momento risposte soddisfacenti o esaustive a queste domande (e su questo si veda il contributo di Stefano Torregiani).

Evidentemente, l'Unione europea si sta muovendo per edificare, progressivamente, un regime giuridico europeo dei dati, che si costruisce attraverso l'allargamento delle direttive esistenti in materia di comunicazioni elettroniche e di sistemi audiovisivi alle problematiche poste dai sistemi di messaggistica istantanea (Whatsapp) e dalle piattaforme audiovisive online (Netflix)[5].

Ma ancora più importante sarà il *digital service act*, cioè un vero e proprio diritto delle piattaforme online, e l'insieme di regolamenti, direttive e azioni che l'Unione europea – si badi quindi, non uno Stato, ma un ordinamento *sui generis* – sta mettendo in campo[6].

Tuttavia, quel che qui interessa è sottolineare – sulla scia di un recente convegno scientifico internazionale – quale sia il regime giuridico del *what people leave behind*, e quindi la descrizione progressiva di quale sia la relazione soggettiva fra persona, impresa, istituzioni e dato/informazione.

4. Segue: profili oggettivi. La localizzazione e i suoi molteplici volti. L'ordinamento costituzionale al tempo della *data dependence*

In questo contesto, ha ormai preso forma un problema più specifico, di cui si avviano ad occuparsi sotto profili diversi tutti i contributi che seguono.

Interi ordinamenti hanno iniziato a comprendere la rilevanza strategica della raccolta dei dati sul territorio nazionale ed i rischi implicati dal travolgente avvento del fenomeno del *cloud computing*.

Per questo, hanno iniziato a introdurre disposizioni volte a vincolare al territorio la raccolta e conservazione dei dati o a ostacolare il flusso verso l'esterno dei dati.

Il diritto dei dati, pertanto, ha iniziato a porre limiti ed a porsi in contrapposizioni ai caratteri genetici della rete internet, che consentono l'ubiquità dei dati e potenzialmente lo sfruttamento dei dati in modo simultaneo e intensivo.

Si sono affacciati nel contesto del dibattito scientifico i temi della localizzazione dei dati, della sovranità sui dati e della sovranità digitale dello Stato, il tema del regime del *trans-border data flow*, il

rischio del *data colonialism*, o all'inverso del *digital isolationism*, e infine la nuova tendenza al *data nationalism*.

Come ha puntualmente osservato Chander: «we define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms-including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data»[7].

Secondo la sua tesi, la localizzazione dei dati finisce per compromettere, invece che garantire, la sicurezza e la privacy di dati/informazioni e agevola il potere di sorveglianza degli Stati.

L'aspetto più interessante, per chi scrive, di questo contributo non consiste tanto nelle conclusioni cui perviene (che ciascuno verificherà se sono o meno condivisibili), ma specificamente nell'osservazione tecnologica del contesto in cui la localizzazione dei dati si colloca. Infatti, ad es., egli ritiene che vi sia un importante problema di sicurezza dei dati nel fatto che singoli Stati si occupino, con i loro limitati mezzi, della sicurezza di data set, in luogo dei grandi operatori del settore che, per definizione, hanno standard di sicurezza più elevati e aggiornati.

È una osservazione importante. Infatti, molti notano l'attivismo dell'Unione europea sul fronte della disciplina giuridica, sotto molteplici profili, dei dati, delle piattaforme, del commercio elettronico, ecc., e il connesso rischio di ipertrofia normativa.

Ma in pochi hanno notato l'iniziativa congiunta francese e tedesca per la costituzione di GAIA X, cioè di una "federated data infrastructure for Europe"[8].

Come viene esposto proprio nella presentazione del progetto – ormai già avviato – l'Europa sviluppa importanti investimenti in tecnologie digitali a modelli innovativi di business. Per questo: «we must ensure that those who drive innovations forward are also those who benefit in economic terms. This will help to secure value creation and employment in Europe. An open digital ecosystem is needed to enable European companies and business models to compete globally. This ecosystem should allow both the digital sovereignty of cloud services users and the scalability of European cloud providers. Within GAIA-X, we are developing the foundations for a federated, open data infrastructure based on European values. GAIA-X connects centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. The resulting federated form of data infrastructure strengthens the ability to both access and share data securely and confidently».

In altri termini, attraverso l'iniziativa francese e tedesca, l'Europa si sta dotando di una infrastruttura *cloud* tutta europea, dedicata a ospitare dati (importanti?) europei.

La questione della collocazione sicura, tecnologicamente all'avanguardia e conforme a standard di protezione dei dati personali (e non), appare tutt'altro che un problema o un tema astratto.

Ovviamente anche in Italia, con i tempi e i modi italiani, si sta ponendo il problema: il d.l. 21 settembre 2019, n. 105, convertito con modificazioni dalla l. 18 novembre 2019, n. 133, disciplina e determina, con ampi margini di approssimazione, il perimetro di sicurezza nazionale cibernetica[9].

Quel che qui interessa sottolineare, è che i temi indicati sono aspetti concreti del diritto dei dati che, non sempre in modo organico, sta nascendo e crescendo in Italia e in Europa.

Per poter giocare un ruolo in questo scenario, occorre partire da una prima, provvisoria, parziale descrizione degli aspetti che ne sono alla base, fra tecnologia e diritto.

Il problema della titolarità e della localizzazione dei dati, che è tutto da scrivere e da descrivere, si colloca sullo sfondo di due domande aperte. E in qualche modo contribuisce ad acuirle.

Quale regime di diritto pubblico di titolarità dei dati e di localizzazione dei dati è compatibile con (o ottimale in) una società liberal-democratica? Quale diritto costituzionale dei dati, nel progredire della *data dependence* della società contemporanea?

Ovviamente queste sono le domande del diritto costituzionale dell'era digitale e questo è il modo con cui anche per il diritto pubblico si inizia a porre il problema della cd. realtà aumentata.

Note

[1]Per questa impostazione e per più ampi riferimenti, sia consentito rinviare a S. Calzolaio, voce *Protezione dei dati personali*, in "Dig.disc.pubbl.", 2017, p. 594 ss.

[2]R.D. Taylor, *"Data localization": The internet in the balance*, in "Telecommunications Policy", vol. n. 44, 2020, n. 8.

[3]L. Lessig, *Code 2.0*, Basic Books, 2006.

[4]L. Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

[5]Interessantissimo, a questo riguardo, il recente aggiornamento del manuale E. Albanesi, R. Zaccaria, A. Valastro, *Diritto dell'informazione e della comunicazione*, Wolters Kluwer-Cedam, XI ed., 2021.

[6]Cfr. Commissione europea, *Strategia europea in materia di dati*.

[7]A. Chander, P.L. Uyen, *Data Nationalism*, in "Emory Law Journal", vol. n. 64, 2015, p. 677-740.

[8]Cfr. *GAIA-X: A Federated Data Infrastructure for Europe*.

[9]Cfr. B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in "Giornale di diritto amministrativo", 2020, n. 5, p. 629 ss.

* * *

Introduction. *Ubi data, ibi imperium*: public law facing data localization

Abstract: *The Rivista italiana di informatica e diritto* hosts a series of contributions on the legal regime of data storage and circulation in the digital society. The aim of this contribution is to introduce, on a methodological level, the legal problem of data localization and availability, as a profile pertaining to the sovereignty of the contemporary state.

Keywords: Data localization – Digital sovereignty – Data availability – Data dependance – Datification

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0022

Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali

Valentina Pagnanelli

Utilizzando le politiche di conservazione dei dati nel settore pubblico come paradigma, il contributo offre una riflessione sulle modalità con cui gli Stati stanno affermando o difendendo la loro sovranità digitale. L'articolo propone una ricostruzione del percorso di digitalizzazione della PA italiana, sul quale i *big data* hanno avuto un notevole impatto. La conservazione dei dati digitali ha imposto il passaggio dagli archivi cartacei ai *cloud*, un passaggio regolato dalla normativa nazionale ed europea ed in parte influenzato dalle strategie digitali delle grandi potenze mondiali. Il proliferare di obblighi e divieti di localizzazione conferma la complessità e la centralità di questi temi nella difesa della sovranità digitale. Il contributo si chiude con una analisi dei punti salienti della *European strategy for data* pubblicata dalla Commissione europea nel febbraio 2020, e con uno sguardo al progetto franco-tedesco di conservazione e condivisione dei dati denominato GAIA-X.

Conservazione dei dati – Sovranità digitale – Settore pubblico – Localizzazione dei dati

Sommario: *1. Introduzione – 2. Dalla digitalizzazione ai big data: il nuovo campo da gioco del settore pubblico – 3. La babele dei dati: fine delle classificazioni? – 4. Regole e ruoli per la conservazione dei dati nella PA – 5. L'individuazione delle infrastrutture: dall'archivio digitale al principio del cloud first – 6. Le regole di localizzazione: data storage pubblico e sovranità – 7. Riflessioni conclusive: la strategia digitale europea*

1. Introduzione

The Guardian il 24 aprile 2020 titolava *UK government told not to use Zoom because of China fears*[1]. Nell'articolo si dava conto della circostanza che «Government and parliament were told by the intelligence agencies last week not to use the videoconferencing service Zoom for confidential business, due to fears it could be vulnerable to Chinese surveillance».

Il *National Cyber Security Centre* avrebbe infatti sconsigliato ai membri del Governo e del Parlamento del Regno Unito l'utilizzo della piattaforma di videoconferenze Zoom[2], quantomeno per le riunioni classificate come "riservate"[3].

Il 29 ottobre 2019 durante l'annuale *Digital summit* tedesco[4] è stato presentato il progetto GAIA-X, una infrastruttura cloud interamente europea, interoperabile ed indipendente dai servizi forniti dai providers statunitensi e cinesi. La cancelliera Angela Merkel in quella occasione ha sottolineato l'importanza di trovare soluzioni europee per garantire la sovranità sui dati. Il progetto franco-tedesco[5] propone di implementare un sistema alternativo ai servizi offerti dai giganti del cloud, che assicuri il rispetto di elevati standard etici e di sicurezza e che sia basato sul principio della *data sovereignty by design*, al fine di creare uno spazio comune europeo per la conservazione dei dati[6].

V. Pagnanelli è dottoranda in Scienze giuridiche presso l'Università di Firenze, avvocato, consulente della protezione dati.

Il 7 aprile 2020, in sede di prime osservazioni sulla app di tracciamento dei contatti per il contenimento del Covid-19 all'esame del gruppo di lavoro istituito dal Governo c.d. *data-driven*[7], il Garante privacy italiano ha richiamato l'attenzione sulla necessità di una scelta oculata dei partner tecnologici, in ragione dell'elevato rischio connesso ai trattamenti di dati personali dei cittadini. Il Garante ha inoltre consigliato di privilegiare soggetti "situati in territorio italiano[8]". In una intervista rilasciata a *Cybersecurity trends* il 16 aprile 2020, il Presidente dell'Autorità garante è tornato sul tema, invocando la evidente necessità di un ripensamento della governance pubblica, per garantire la sovranità digitale dello Stato di fronte alle crescenti minacce globali all'indipendenza dei Paesi: *In uno spazio "defisicizzato" come la rete la sovranità va declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica [...]*[9]".

Territorio, sovranità e potere sono concetti assolutamente attuali nel diritto di internet, con cui bisogna fare i conti[10]. Eloquentemente Oreste Pollicino introduce così un commento a due sentenze della Corte di Giustizia dell'Unione europea[11] nelle quali i giudici di Lussemburgo sono stati chiamati a decidere sulla fissazione dei limiti territoriali all'applicazione del diritto europeo, giungendo peraltro a soluzioni apparentemente contrapposte[12].

Già questa breve e parziale rassegna evidenzia come le categorie costituzionali poc'anzi citate, pur necessitando di essere ripensate, rimangano necessarie per governare il contesto globale digitalizzato dei nostri giorni.

Utilizzando le politiche di conservazione e accesso ai dati del settore pubblico come paradigma, il presente contributo intende offrire una riflessione sulle modalità con cui gli Stati stanno affermando la loro sovranità digitale in una fase storica in cui, da una parte, il territorio diventa un riferimento sfuggente per individuare e proteggere i confini di una giurisdizione che è sempre meno materiale, e dall'altra, i sistemi democratici e le libertà e i diritti dei cittadini sono minacciati dal crescente e pervasivo ricorso all'intelligenza artificiale[13].

2. Dalla digitalizzazione ai big data: il nuovo campo da gioco del settore pubblico

Non ripercorreremo in questa sede le tappe dello sviluppo tecnologico che in alcuni anni, con progressione geometrica, ci ha portato dal cartaceo, al digitale, allo scenario attuale in cui i Big Data e in particolare la Big Data Analytics hanno cambiato di fatto la relazione dell'uomo con le informazioni[14].

Una componente di cruciale importanza all'interno di questa evoluzione è certamente costituita dalla progressiva digitalizzazione del patrimonio informativo delle pubbliche amministrazioni, che le ha portate a disporre di banche dati costantemente alimentate[15], contenenti quantità straordinarie di informazioni, siano esse dati personali, categorie particolari di dati, o dati non personali[16]. La Pubblica Amministrazione italiana, sulla quale la prima parte della trattazione sarà incentrata, non è naturalmente rimasta estranea a questo cambio di paradigma.

Invero a seguito del deciso impulso alla digitalizzazione impresso alle amministrazioni pubbliche in particolare con il d.l. n. 179/2012, che ha portato alla progressiva creazione tra gli altri dell'Anagrafe nazionale delle popolazione residente, del fascicolo elettronico dello studente, del fascicolo sanitario elettronico (istituito dalla Regioni e province autonome), la Pubblica Amministrazione italiana ha assunto *la responsabilità di gestire, trattare, condividere, elaborare, "archivi digitali" immensi, da cui possono essere tratte informazioni in grado di compromettere tanto gli interessi nazionali quanto i diritti individuali*[17].

Il progressivo sviluppo delle *Smart cities* ha contribuito ad incrementare esponenzialmente anche la quantità di dati non personali conservati dalla PA. Tale scenario ha di recente subito una ulteriore spinta in avanti con il Piano Triennale per l'Informatica 2019-2021, elaborato dall'Agenzia per l'Italia Digitale (AgID)[18].

L'introduzione del concetto di *Smart Landscape*[19] segna un importante cambiamento di quello che per lungo tempo è stato l'immaginario collettivo, che collegava la *smartness* ad un ventaglio certamente ampio di servizi e benefits per il cittadino, relegando le imprese e l'industria ai margini dei progetti di volta in volta ideati. Il modello di *Smart Landscape* prevede invece uno sviluppo dei servizi resi alle imprese, prime fra tutte quelle legate alla logistica per la circolazione delle merci.

Vale la pena di segnalare che il Piano Triennale prevede la progressiva implementazione di un modello predittivo (*Smart Landscape Engine*) che dovrà essere impiegato nella governance dello *Smart Landscape*. SLE sarà capace di elaborare scenari *what-if* in base alle informazioni inserite, e dovrà coadiuvare i processi decisionali legati allo sviluppo del *paesaggio intelligente*. La rilevanza di quanto appena descritto appare evidente: la realizzazione di un modello di intelligenza artificiale della PA segna infatti

un ulteriore avvicinamento[20] del settore pubblico a tecnologie (e pratiche) già ampiamente utilizzate nel settore privato.

Trasparenza amministrativa e *Open data* non costituiscono l'oggetto di questo contributo[21]. Basti solo qui ricordare che la governance dei dati del settore pubblico non può, in concreto, prescindere dal considerare anche gli obblighi di pubblicazione, oltre che le garanzie di accessibilità totale e riutilizzo delle informazioni[22]. Tali informazioni, a seguito di una costante ed ineliminabile opera di valutazione e bilanciamento rispetto al diritto alla protezione dei dati personali dei soggetti i cui dati sono di volta in volta coinvolti, contribuiscono in modo significativo ad accrescere l'insieme dei dati che possono essere correlati con altri dati e che rappresentano un fattore di *disclosure globale*[23] di informazioni, personali e non.

La digitalizzazione, lo sviluppo delle ICTs, il progredire dell'Intelligenza Artificiale hanno delle potenzialità eccezionali per il miglioramento della qualità dei servizi nel settore pubblico, oltre che in termini di semplificazione, riduzione dei costi, conoscibilità dell'azione amministrativa, esercizio dei diritti di cittadinanza, corretto svolgimento della vita democratica. I recenti accadimenti globali ne hanno dimostrato l'utilità anche per la gestione di situazioni complesse quali il contenimento di una epidemia (la possibilità di disporre di dati organizzati, unita all'interoperabilità di banche dati afferenti a differenti organismi, pubblici e privati, pare in alcuni casi aver fatto la differenza[24]).

Ma l'accentramento di una quantità incalcolabile di informazioni in una banca dati, unito alla possibilità di incrociare tali informazioni con quelle provenienti da altri database utilizzando algoritmi raffinatissimi, porta con sé altrettanti gravi rischi per i diritti e le libertà dei singoli, soprattutto rispetto a possibili discriminazioni, e per la tenuta dei sistemi democratici, ove le informazioni venissero utilizzate per interferire con la libera formazione dell'opinione pubblica[25] o con lo svolgimento dell'attività politica-economica-amministrativa di uno Stato sovrano[26].

A questo proposito si evidenzia come Garante per la protezione dei dati personali, AGCOM e AGCM, al termine di una analisi conoscitiva congiunta sul fenomeno dei Big Data[27], abbiano espresso preoccupazione in merito alla compatibilità con la normativa in materia di protezione dati di alcuni aspetti delle attività di analisi dei Big Data quali l'indeterminatezza delle finalità, i rischi legati alla possibilità di reidentificazione degli interessati, l'opacità delle logiche applicate dagli algoritmi.

Il report fa un esplicito riferimento alla creazione della Piattaforma Digitale Nazionale Dati, introdotta con l'art. 50 ter del Codice dell'Amministrazione Digitale (CAD). Le criticità della piattaforma andrebbero individuate principalmente nell'accentramento presso un unico soggetto di informazioni *anche sensibili e sensibilissime*, per finalità del tutto generiche, con evidente rischio di usi distorti. Secondo le tre Autorità indipendenti, date queste premesse, un trattamento fondato sui Big Data nel settore pubblico richiederà una base legale idonea *che assicuri ai cittadini, oltre alla trasparenza delle decisioni, la proporzionalità del ricorso ex lege a tale metodologia rispetto all'obiettivo di interesse pubblico perseguito e l'individuazione, nel rispetto del principio di privacy by design, di adeguate garanzie da integrare nel trattamento, dopo aver accuratamente valutato i rischi elevati per i diritti e le libertà degli interessati*[28].

3. La babele dei dati: fine delle classificazioni?

L'espansione del fenomeno della Big data Analytics sembra aver messo in luce i limiti del processo, divenuto ormai macchinoso, di separazione dei dati in categorie. Infatti molto spesso tale attività, seppure realizzabile in una fase di ricognizione ex ante dei dataset, diviene di poca utilità ex post, ovvero a seguito del trattamento degli stessi dati con strumenti di machine learning: com'è noto, infatti, grazie a raffinatissimi algoritmi, oggi possiamo estrarre informazioni personali su un individuo anche a partire da informazioni che personali non sono[29].

L'utilizzo di algoritmi applicati ad un volume immenso di dati consente di estrarre o anche di prevedere informazioni personali, a volte partendo da dataset di informazioni non personali, correlati con altri dataset di differente origine e contenuto[30]. In questo contesto la distinzione tra dato personale e dato non personale dunque è sempre meno realizzabile[31], e la possibilità di una applicazione di regimi giuridici differenti a tipologie diverse di dati, sempre meno probabile.

Una differenziazione che, qualora effettivamente possibile, comporterebbe comunque un aumento di spesa per adeguamenti tecnologici e probabili impegni regolamentari interni alle Pubbliche amministrazioni, che appaiono di difficile realizzazione nel breve periodo. Anche nel settore privato, un onere siffatto comporterebbe un sensibile aumento di costi e una riduzione del valore dei dati medesimi.

Il problema si pone oggi in concreto a seguito della entrata in vigore del Regolamento europeo c.d. FFD (*Free Flow Data*) sulla circolazione dei dati non personali, che introduce un regime differenziato per tutti i dati che non rientrino nella definizione[32] (e

nella disciplina) contenuta nel GDPR. Com'è noto, la possibile difficoltà nella separazione tra i due insiemi di dati è stata già prevista dal legislatore europeo, che all'art. 2 par. 2 del Regolamento n. 1807/2018 precisa che qualora i dati personali e non personali all'interno di un dataset siano indissolubilmente legati, resta impregiudicata l'applicazione del GDPR. A parere di chi scrive, tale inquadramento normativo costituirà un impedimento non di poco conto alla libera circolazione di una grandissima mole di dati non personali, inscindibilmente legati, tuttavia, a dati personali[33].

Proseguendo nella rassegna delle tipologie di dati, con specifico riferimento ai trattamenti posti in essere dalle amministrazioni pubbliche, vi è un ulteriore criterio di classificazione che nella prassi si rivela molto impattante. Si tratta della distinzione tra insiemi di dati contenuti in documenti cartacei e dataset che costituiscono i documenti digitali della PA. La citata distinzione non è meramente formale, ma come si vedrà tra un attimo è al contrario collegata ad aspetti assolutamente sostanziali.

Ancora una volta è il Regolamento FFD a fare da spartiacque, infatti in esso il *trattamento* viene definito come *qualsiasi operazione o insieme di operazioni compiute su dati o insiemi di dati in formato elettronico*[34]. Come poc'anzi ricordato, il Regolamento FFD pone regole volte ad agevolare la libera circolazione dei dati, che sono applicabili, appunto, solamente ai trattamenti di dati in formato elettronico.

I dati non personali contenuti in documenti cartacei, sono dunque de facto esclusi dalla disciplina che ne regola la libera circolazione nel territorio dell'Unione europea. Non considerare l'esistenza di questo "doppio binario" rischia di restituire una visione parziale della realtà; questa peculiarità invece potrebbe provocare limitazioni non secondarie alla applicazione della normativa, riducendone in ultima analisi l'efficacia.

4. Regole e ruoli per la conservazione dei dati nella PA

I riferimenti normativi generali in materia di conservazione degli atti della Pubblica Amministrazione e di gestione degli archivi sono contenuti nel D.P.R. n. 445/2000, in particolare nell'art. 68[35]. La medesima disposizione pone l'obbligo di applicazione della normativa in materia di privacy a tutte le attività di gestione e custodia dei documenti. Sarà dunque qui utile richiamare rapidamente le regole di *data storage* poste dal GDPR.

Il Regolamento UE n. 2016/679 impone al titolare del trattamento[36] di conservare i dati personali per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati, con due sole eccezioni: che i soggetti cui i dati personali si riferiscono non siano più identificabili; che i dati siano trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici (art. 5 par. 1 lett. e).

Il GDPR impone inoltre al titolare del trattamento di informare l'interessato rispetto al periodo di conservazione dei dati personali, o perlomeno di indicare i criteri utilizzati per determinare tale periodo (art. 13 par. 2 lett. a). Come si vedrà a breve, anche il responsabile del trattamento[37] deve cancellare o restituire i dati personali al titolare una volta terminata la prestazione (art. 28 par. 3 lett. g). Nel Registro dei trattamenti vanno indicati, quando possibile, i termini ultimi di cancellazione per ciascuna categoria di dati personali (art. 30 par. 1 lett. f).

A parere di chi scrive vi sono due aspetti della disciplina privacy sulla conservazione che incidono significativamente, e più di altri, nella governance dei dati del settore pubblico.

Il primo di essi è dato dalla applicazione dell'art. 25 del Regolamento 2016/679. La norma impone al titolare del trattamento di mettere in atto misure tecniche e organizzative atte a garantire la protezione dei dati e a tutelare in questo modo i diritti degli interessati. Tali misure dovranno essere individuate a seguito di una valutazione effettuata caso per caso, per ogni differente fattispecie di trattamento, *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche [...]*.

La conseguenza diretta della applicazione del principio di privacy by design appena descritto a quello che nel paragrafo precedente abbiamo chiamato "doppio binario" è evidente: l'attività di conservazione dei documenti amministrativi sarà soggetta ab origine a due differenti discipline, a seconda che i documenti siano cartacei o digitali[38].

La presenza di un doppio sistema di conservazione dei dati costituisce peraltro una componente non eliminabile nel breve periodo. Lo conferma la norma del CAD che prevede la predisposizione da parte delle PA di piani di sostituzione degli archivi cartacei con quelli informatici all'esito di una valutazione costi/benefici[39].

Un secondo aspetto, ancor più rilevante, della applicazione della disciplina privacy alla conservazione dei dati nel settore pubblico, è quello che attiene

alla individuazione e nomina dei citati responsabili esterni del trattamento, a norma dell'art. 28 del GDPR.

Il GDPR pone delle regole piuttosto precise per l'attribuzione della responsabilità rispetto al legittimo trattamento dei dati. Al titolare del trattamento spettano le decisioni in merito alle finalità e ai mezzi del trattamento. I responsabili sono invece soggetti che trattano i dati per conto del titolare e sono a tal fine "incaricati" con contratto o altro atto giuridico vincolante. Tale atto contiene la regolamentazione del rapporto tra titolare e responsabile[40], le istruzioni impartite dal primo e gli obblighi per il secondo rispetto al trattamento dei dati personali.

Nel contesto della Pubblica Amministrazione molte attività sono gestite da soggetti esterni incaricati a seguito di bando o tramite affidamento diretto. Ciò significa che in moltissimi settori, quantità consistenti di dati siano trattate esternamente.

In questa sede non è possibile neppure accennare al complesso organigramma dei "ruoli privacy" risultante dalla rete di rapporti che legano la PA ad altri soggetti pubblici e ad imprese e professionisti del settore privato. Sia consentito, tuttavia, rilevare come il rispetto della normativa sulla protezione dati abbia imposto alcuni adempimenti anche durante la pandemia di Covid-19. Il rispetto del GDPR e del Codice privacy ha infatti imposto alle autorità statali di elaborare rapidamente disposizioni normative che hanno consentito ai numerosi soggetti coinvolti nella gestione dell'emergenza di trattare legittimamente dati personali. Tale attività, seppure incontestabilmente necessaria, ed urgente, ha dato vita ad una rete complessa di ruoli e responsabilità che appare onestamente difficile da ricostruire a posteriori[41].

Terminata la digressione, è necessario a questo punto individuare i soggetti incaricati della conservazione dei dati nella Pubblica Amministrazione, che qualora esterni all'amministrazione medesima, dovranno essere contrattualizzati ex art. 28 del GDPR.

È l'articolo 34 del CAD ad offrire alle pubbliche amministrazioni l'alternativa tra la conservazione dei documenti informatici all'interno della propria struttura organizzativa e l'affidamento di tale attività a soggetti pubblici e privati accreditati presso AgID come conservatori. L'art. 44 impone poi al responsabile della conservazione che decida per l'esternalizzazione, di individuare soggetti che offrano *idonee garanzie organizzative e tecnologiche e di protezione dei dati personali.* Il rispetto di questo ultimo requisito dovrà essere garantito attraverso la predisposizione e sottoscrizione di contratti ex art. 28, che contengano la regolamentazione giuridica del rapporto tra *data controller* e *data processor*, oltre che istruzioni stringenti sulla sicurezza informatica dei dati trattati. La centralità e rilevanza di questo "adempimento privacy" sono state confermate di recente dall'Autorità garante.

Nel parere sullo schema di Linee guida sulla formazione, gestione e conservazione dei documenti informatici[42], reso il 13 febbraio scorso[43],il Garante per la protezione dati personali ha ribadito la necessità per le PA di rispondere ai requisiti richiesti dal GDPR, precisando che una chiara attribuzione dei compiti è il presupposto per una corretta attribuzione delle responsabilità, e che tale suddivisione deve essere contrattualizzata ed esplicitata in clausole che rispondano ai requisiti del Regolamento europeo, a maggior ragione nei casi in cui si preveda di esternalizzare servizi.

Merita evidenziare come il Garante non ponga dei limiti all'affidamento a privati di servizi che prevedano il trattamento di dati personali, ma insista piuttosto nella piena applicazione di tutte le garanzie individuate dal GDPR (contrattualizzazione dei responsabili esterni, rispetto degli obblighi di sicurezza, applicazione dei principi di privacy by design e by default, efficienti procedure di notifica in caso di data breach, adesione a codici di condotta).

Richiamate regole e ruoli del data storage pubblico, ci occuperemo ora del regime relativo alla collocazione materiale dei dati e documenti conservati. Nei prossimi paragrafi si darà conto di almeno due aspetti di rilievo: l'individuazione della tipologia di infrastrutture per l'archiviazione, e le regole di localizzazione dei dati.

5. L'individuazione delle infrastrutture: dall'archivio cartaceo al principio del cloud first

La conservazione dei dati della Pubblica Amministrazione avviene ormai solamente in formato digitale, in ossequio al principio *digital first.*

L'art. 40 del Codice dell'Amministrazione Digitale prevede che le PA formino gli originali dei propri documenti con mezzi informatici, e l'art. 43 chiarisce che gli obblighi di conservazione dei documenti si intendono soddisfatti a tutti gli effetti di legge con i documenti informatici, se conformi agli originali e alle linee guida.

Come ricordato nelle pagine precedenti, il CAD prevede la predisposizione di piani per la progressiva sostituzione degli archivi cartacei con quelli informatici. Di conseguenza ad oggi gli archivi cartacei sono sottoposti ad un regime che potremmo definire "ad

esaurimento". Ma a ben vedere, il citato articolo 42 del CAD collega tali determinazioni ad una valutazione sul rapporto tra costi e benefici e non indica un termine massimo per completare il passaggio dagli archivi cartacei a quelli digitali. Questa componente, lasciata alla valutazione discrezionale di ogni singola amministrazione ed unita alla mancanza del riferimento ad un termine ultimo per concludere lo *switch*, pare contribuire al rallentamento del processo di digitalizzazione della PA.

Svolta questa premessa, passiamo ora ad esaminare alcuni significativi interventi statali in tema di attuazione della Agenda digitale[44], che hanno inciso nella governance dei dati.

Una delle azioni trasversali della Strategia per la Crescita digitale del Paese prevede l'adozione progressiva del paradigma del *cloud computing*[45]. Il Piano Triennale per l'Informatica 2019-2021, in attuazione di questa scelta programmatica, contiene una decisa opzione per i servizi e le infrastrutture cloud. Tale opzione è stata consacrata con la enunciazione del principio *cloud first*[46].

Il PTI delinea un percorso di trasformazione dei sistemi informativi della PA, con l'obiettivo di passare dalla attuale frammentazione e disomogeneità ad una organizzazione evoluta ed efficiente.

Questa trasformazione dovrebbe poggiare su tre elementi-chiave: l'applicazione del già citato principio *cloud first* per la definizione di nuovi progetti e la programmazione di nuovi servizi delle PA; la progressiva migrazione delle infrastrutture e dei servizi esistenti verso il cloud (il c.d. *cloud enablement*); infine il potenziamento delle competenze mediante la creazione di Centri appositi, allo scopo di consolidare il *know-how* e l'esperienza relativa alla gestione dei servizi cloud nella PA.

Secondo quanto previsto nel PTI, tali Centri di competenza dovrebbero essere sorte di forum composti da tecnici, esperti e IT managers, *che discutano, propongano standard e regolamenti dei servizi digitali, condividano informazioni, soluzioni e competenze utili a mantenere, aggiornare, aumentare l'affidabilità dei sistemi*[47].

La strategia per l'adozione del *cloud computing* si sta realizzando anche attraverso vincoli alle spese per il settore ICT. Infatti, in attuazione del Piano Triennale 2019-2021, le PA non possono più effettuare investimenti su hardware e infrastrutture. Spese e investimenti potranno invece essere effettuati per progetti di virtualizzazione e per la migrazione dei servizi nelle infrastrutture del Cloud della PA.

Elemento non secondario, l'opzione per il *cloud computing* certamente risponde ad esigenze di riduzione dei costi per le infrastrutture informatiche[48], peraltro in aderenza a criteri di efficienza, efficacia ed economicità, richiamati anche nell'art. 12 del CAD[49].

Tale scelta a ben vedere, pare essere il fulcro di una più ampia strategia di razionalizzazione del patrimonio informativo della Pubblica Amministrazione[50]. Essa segna quindi una trasformazione culturale, prima che tecnica o giuridica, di non poco conto, se letta alla luce delle più volte richiamate dinamiche connesse alla digitalizzazione globale.

Su tale fronte, e prima di muovere verso la seconda questione relativa alla collocazione dei dati, ha un qualche rilievo citare il *Digital Economy and Society Index* (DESI), le cui risultanze sono state pubblicate l'11 giugno 2020[51]. Attraverso questo *Indice di digitalizzazione dell'economia e della società*, la Commissione Europea monitora il progresso digitale degli Stati membri dell'Unione.

Nel ranking complessivo viene indicata la sommatoria dei dati raccolti con riferimento a cinque aree tematiche: connettività, capitale umano, uso dei servizi internet, integrazione delle tecnologie digitali, servizi pubblici digitali. Il posizionamento dell'Italia al 25esimo posto su 28, nella sua eloquenza, stimola più di una riflessione[52].

Accanto a risultati soddisfacenti rispetto ad esempio alla connettività (in particolare alla "preparazione al 5G", ove l'Italia si colloca ben al di sopra della media europea), il DESI mette in luce carenze molto gravi per quanto riguarda il capitale umano, area nella quale l'Italia si colloca addirittura all'ultimo posto in Europa. Infatti solo il 42% degli individui di età compresa tra i 16 e i 74 anni possiede competenze digitali di base (rispetto alla media europea del 58%) e solo il 22% dispone di competenze digitali superiori a quelle di base (rispetto al 33% nell'Unione). L'uso modesto di internet, e la tipologia di contenuti oggetto delle ricerche online effettuate dagli utenti[53] sembrerebbero essere la diretta conseguenza delle scarse competenze digitali rilevate attraverso l'indagine europea.

Ciò nonostante, l'Indice europeo dà atto del crescente impegno dello Stato italiano per realizzare una efficiente digitalizzazione, impegno dimostrato tra l'altro attraverso l'istituzione del Ministero per l'innovazione tecnologica e la digitalizzazione, la presentazione della strategia *Italia 2025* e la predisposizione di un Piano Triennale per l'Informatica nella PA contenente un *elenco esaustivo di obiettivi per i prossimi anni.*

Tale impegno è comprovato dagli ottimi risultati conseguiti rispetto ai servizi pubblici online, ai servizi pubblici digitali per le imprese e all'open data, settori ove l'Italia supera persino il valore medio europeo. Tuttavia il dato, lungi dall'essere rassicurante,

è invece mortificante in quanto, nonostante i risultati appena citati, l'Italia si colloca al diciannovesimo posto nella classifica relativa ai servizi pubblici digitali. Il valore che inficia il risultato complessivo è quello relativo allo *scarso livello di interazione online tra le autorità pubbliche e il pubblico in generale. Solo il 32% degli utenti italiani online usufruisce attivamente dei servizi di e-government (rispetto alla media UE del 67%)*[54].

È appena il caso di sottolineare che un ritardo così grave non può che avere ripercussioni molto serie anche per la partecipazione del Paese al Mercato Unico Digitale. Tuttavia, la consapevolezza di queste gravi carenze, e soprattutto dello squilibrio tra lo sviluppo dei programmi di innovazione digitale delle PA e la scarsa attenzione ai diritti "digitali" di cittadini e imprese, così come garantiti dal CAD[55], potrebbe essere l'occasione per effettuare un investimento organico e strutturato sulla alfabetizzazione digitale[56]. Dunque il *digital divide*, se non affrontato in tempi rapidi, rischia di rivelarsi come l'ostacolo di gran lunga più difficile da rimuovere per la partecipazione dell'Italia al Digital Single Market[57].

Peraltro la diretta connessione tra *data literacy*, partecipazione alla economia digitale e sovranità tecnologica è un assunto della strategia digitale europea, confermato di recente nel White Paper sull'intelligenza artificiale[58].

6. Le regole di localizzazione: data storage pubblico e sovranità

Il secondo aspetto di rilievo in merito alla collocazione dei dati del settore pubblico riguarda la localizzazione fisica delle infrastrutture per la memorizzazione, in quanto talvolta la legge impone che determinati dataset siano conservati in server collocati sul territorio nazionale.

Anche in questo caso alcuni esempi saranno utili a chiarire i termini della questione.

La fattispecie più recente di imposizione di un obbligo di localizzazione in Italia può essere rinvenuta all'interno dell'art. 6 del d.l. n. 28 del 2020. Si tratta della norma sul *Sistema di allerta Covid-19*, che introduce una piattaforma per la gestione del sistema di tracciamento dei contagi ed impone che tale piattaforma sia localizzata sul territorio nazionale[59].

Come accennato nell'introduzione, il Garante per la protezione dei dati personali in fase di consultazioni aveva fatto una espressa raccomandazione in questo senso, richiamando il principio di precauzione in ragione della tipologia di dati oggetto di trattamento e quindi dei rischi elevati per i cittadini utenti della app di *contact tracing*[60].

Anche il Copasir, al termine di una attività di indagine e raccolta informazioni avviata in ragione di possibili rischi per la sicurezza nazionale, ha trasmesso al Parlamento una relazione sul sistema di allerta Covid-19[61]. Il Comitato, dopo aver richiamato l'esigenza che la conservazione dei dati avvenga sul territorio nazionale, esprime perplessità rispetto alla composizione della società proprietaria della app prescelta (Immuni). Infatti una quota minoritaria della Bending Spoons S.p.a. apparterrebbe ad un fondo riconducibile ad un uomo d'affari cinese. Le preoccupazioni espresse dal Copasir nascono in merito alla Cybersecurity law cinese, che *obbliga, in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità militari di pubblica sicurezza e alle agenzie di intelligence*[62].

Le conclusioni della Relazione divengono ancora più esplicite quando fanno espresso riferimento a rischi non trascurabili e non mitigabili sul piano geopolitico. Tali rischi sarebbero principalmente connessi alla necessaria e non fungibile presenza di partner privati non nazionali nella implementazione del sistema informatico di *contact tracing*; tali soggetti, ammonisce il Copasir, potrebbero manipolare i dati per finalità estranee da quella per la quale sono stati raccolti, di natura *politica, militare, sanitaria o commerciale*[63].

Un altro obbligo di localizzazione è contenuto nelle già richiamate Linee guida sulla formazione, gestione e conservazione dei documenti informatici, rilasciate dall'AgID in bozza per la consultazione. Nella sezione dedicata alle infrastrutture, vi è la prescrizione che i sistemi di conservazione delle PA e dei conservatori accreditati prevedano *la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale*, al fine di consentire all'Agenzia per l'Italia Digitale di svolgere le funzioni di vigilanza[64].

È utile ricordare che, secondo quanto precisato dal Consiglio di Stato, una volta adottate da AgID secondo la procedura indicata nell'art. 71 del CAD, le Linee guida acquisiranno carattere vincolante, assumeranno valenza erga omnes e saranno azionabili davanti al giudice amministrativo[65].

Proprio con riferimento alle regole di localizzazione dei dati, occorre qui mettere in evidenza una particolarità del sistema italiano. Infatti nella parte del Piano Triennale per l'Informatica nella PA dedicata al Cloud, più precisamente nella sezione delle domande frequenti, viene chiarito che vi è la possibilità per le PA di scegliere fornitori di servizi quali Google Cloud, Azure o altri providers, purché siano qualificati a norma della circolare Agid n. 3 del 9 aprile 2018, per la fruizione di servizi IaaS e PaaS[66].

I servizi di Cloud della tipologia *Infrastructure as a Service* possono fornire servizi di *computing*, *networking* e *storage* dei dati. La presenza nel Cloud Marketplace di AgID[67] di fornitori di servizi IaaS che non offrono all'utente la possibilità di scegliere la localizzazione dei siti ove verranno memorizzati e processati i dati, in controtendenza rispetto agli obblighi di localizzazione poc'anzi richiamati, sembra rivelare una lacuna nel coordinamento dei numerosi aspetti della complessa governance dei dati pubblici.

Accanto alle disposizioni normative e regolamentari appena richiamate, nei mesi scorsi il Garante per la protezione dei dati personali si è pronunciato ancora una volta in merito alla localizzazione dei dati personali, su impulso dell'Unione Camere Penali. Il riferimento è alla lettera inviata dal Presidente dell'Authority al Ministro della Giustizia Bonafede in merito ai software utilizzati per consentire lo svolgimento del processo penale da remoto[68]. Oggetto della richiesta di chiarimenti era la scelta, per la celebrazione delle udienze penali, di piattaforme fornite da un partner tecnologico (Microsoft) avente sede negli Stati Uniti, e per questa ragione soggetto all'applicazione del Cloud Act che *attribuisce alle autorità statunitensi un ampio potere acquisitivo di dati e informazioni.*

Gli obblighi di localizzazione imposti alle amministrazioni pubbliche italiane, unite ai richiami alle legislazioni cinese e statunitense, ci conducono al centro della questione.

Infatti come Vincenzo Zeno-Zencovich ha efficacemente sintetizzato commentando il Caso Schrems[69], *stabilire come i dati personali raccolti attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti ad altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto*[70].

Alcuni rapidi cenni alla normativa cinese sulla sicurezza cibernetica e a quella statunitense sul *cloud computing* permetteranno di mettere in luce le precise scelte strategiche volte a difendere la sovranità statale, entro (ed oltre) i limiti territoriali della propria giurisdizione.

Premettendo che l'articolatissimo sistema normativo e regolamentare della Repubblica Popolare Cinese in materia di privacy e sicurezza cibernetica[71], non è facilmente accessibile né decifrabile per uno studioso straniero, richiameremo nelle prossime righe solo alcuni tratti peculiari della governance cinese dei dati.

La *Cybersecurity law*[72], approvata nel novembre 2016, pone una serie di principi corredati in seguito da numerosissime integrazioni; si tratta di leggi, regolamenti, e standards che forniscono indicazioni tecniche per la implementazione del sistema nazionale di *cybersecurity*[73]. Questa legge, è importante sottolinearlo, non è incentrata sulla tutela dei dati personali (sebbene contenga delle norme a ciò dedicate), ma piuttosto sulla tutela della sovranità dello Stato, che viene assunta come la più alta priorità[74]. Il primo articolo elenca tra le finalità perseguite innanzitutto la salvaguardia della sicurezza cibernetica e della *cyberspace sovereignty*, per proseguire con la protezione dei diritti di cittadini e imprese e lo sviluppo della informatizzazione dell'economia e della società.

Gli operatori delle reti, principali destinatari delle regole previste dalla *Cybersecurity law*, debbono adeguare le loro infrastrutture ad una serie di requisiti tecnici finalizzati a garantire la sicurezza cibernetica. Gli obblighi saranno più o meno stringenti a seconda della tipologia di infrastruttura gestita[75]. Ai *network operators* è altresì esplicitamente fatto obbligo di collaborare con le autorità di pubblica sicurezza per la salvaguardia della sicurezza nazionale (art. 28).

Un interessante contributo di Aimin, Guosong e Wentong[76] articola il principio della sovranità cibernetica cinese in quattro diritti fondamentali: il diritto alla giurisdizione, cioè il diritto di gestire le reti informatiche presenti sul territorio nazionale; il diritto alla difesa contro gli attacchi informatici e le minacce esterne al Paese; il diritto alla indipendenza, ossia il diritto di usufruire dei servizi delle ICTs utilizzando esclusivamente network nazionali, indipendenti dal potere di altri Stati (il riferimento qui è al DNS statunitense); ultimo, il right of equality, che prevede per ogni Stato il diritto di avere giurisdizione sulle proprie reti informatiche[77].

Non a caso, uno degli strumenti normativi individuati dalla *Cybersecurity law* per affermare la propria sovranità cibernetica è l'imposizione agli operatori di *Critical Information Infrastructure*[78] dell'obbligo di localizzare i dati personali e gli *important data* da essi generati e raccolti, esclusivamente sul territorio nazionale[79].

Veniamo ora agli Stati Uniti, ove il Governo, dopo aver lanciato già nel 2011 la *Cloud First Strategy*, si appresta oggi a condurre una evoluzione dal paradigma *Cloud first* al *Cloud Smart*, basato su tre pilastri: *security*, *procurement*, e *workforce*[80]. Più rilevante rispetto all'oggetto del presente scritto è sicuramente la disciplina introdotta con il *Cloud Act*, relativa all'accesso da parte delle Autorità statunitensi a dati conservati al di fuori del territorio (e della giurisdizione) degli USA.

Infatti il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act*[81], approvato all'inizio del 2018, consente alle Autorità statunitensi di accedere alle in-

formazioni contenute nei server di *companies* statunitensi ovunque collocati nel mondo, al fine di garantire lo svolgimento di indagini e il perseguimento dei reati. Al contempo esso consente ai Governi stranieri di accedere, per le medesime finalità, a dati conservati sul territorio degli Stati Uniti. Il meccanismo si basa su un sistema di *executive agreements* negoziati bilateralmente con i singoli governi[82], che di fatto si sovrappone al modello, considerato inefficiente perché troppo lento e macchinoso, dei *Mutual Legal Assistance Treaties*[83].

Il fine dichiarato del Governo statunitense è quello di evitare conflitti di giurisdizione con altri Stati sovrani, e al contempo assicurare garanzie procedurali per tutti i casi di accesso ai dati personali.

Il risultato ottenuto, com'è noto, è molto controverso. Una parte dei commentatori ha sollevato dei dubbi sui rischi collegati ad una sensibile riduzione della protezione della privacy rispetto al precedente meccanismo dei MLATs. Altri sostengono invece che tale sistema sia completamente allineato con quello posto dal GDPR. Invero l'art. 48 del Regolamento europeo, disciplinando i trasferimenti non autorizzati di dati al di fuori dall'Unione europea nei casi in cui essi siano basati su una sentenza o una decisione amministrativa di uno Stato terzo, delinea una ipotesi di riconoscimento di tali atti proprio in presenza di un accordo internazionale, come un trattato di mutua assistenza giudiziaria[84].

A tale proposito è interessante notare come l'Unione europea si stia muovendo nella stessa direzione intrapresa dagli Stati Uniti per l'adozione di un Regolamento sull'accesso alle prove elettroniche, la cui proposta è attualmente in discussione in Consiglio[85], e la cui impostazione è in gran parte sovrapponibile al modello del Cloud Act.

Dalla sintetica analisi delle "strategie digitali" cinesi e statunitensi da ultimo proposta sembra di poter trarre una conferma del legame inscindibile tra data governance e affermazione della sovranità (digitale) dello Stato.

Basti ricordare che le scelte politiche cinesi e statunitensi di cui si è poc'anzi dato conto hanno avuto come conseguenza in primo luogo l'adozione, da parte degli altri Stati, di misure difensive del proprio patrimonio informativo; in secondo luogo, le grandi società fornitrici di servizi hanno dovuto adattarsi alle regole imposte per evitare di essere escluse da rilevantissime quote del mercato globale.

Non a caso, i big players hanno rapidamente provveduto a dotarsi di datacenters sul territorio della Repubblica Popolare cinese, e, sul fronte opposto, hanno elaborato soluzioni che, nel rispetto delle leggi, consentano di fatto ai loro clienti di sfuggire a possibili accessi indesiderati alle proprie informazioni da parte del Governo statunitense in forza del Cloud Act[86].

7. Riflessioni conclusive: la strategia digitale europea

La strategia europea si pone su un piano differente rispetto a tutto quanto sin qui descritto.

Infatti, a partire dal documento *A European Strategy for Data*[87] pubblicato il 19 febbraio 2020, viene presentata una visione dell'Unione europea nel contesto globale, che conferisce alla stessa una identità molto precisa, e la differenzia sensibilmente dagli altri attori mondiali.

Il documento, prese le mosse da una analisi dei ruoli degli USA e della Cina nella *data economy*, si prefigge di proporre/imporre una *European way*, che dovrebbe distinguersi per un bilanciamento, finora inedito, tra massimo utilizzo dei dati per lo sviluppo economico del Mercato Unico da una parte, e altissimi standard etici, di privacy, di safety and security dall'altra.

La grande novità proposta con la strategia europea è la creazione di *data spaces* tematici. Dalla possibilità di far circolare i dati ed estrarre da essi valore, innovazione, benefici per la collettività dipende l'espansione del Digital Single Market. La Commissione europea propone di realizzare questo effettivo cambio di marcia con un sistema di *pools* di dati, suddivisi in aree tematiche in modo che ogni settore possa trovare regole adeguate, e al contempo i singoli spaces possano comunicare tra di loro per massimizzare il flusso di dati, con il superamento dei limiti legati ai *data silos*.

L'Unione europea si appresta dunque a creare una grande area di localizzazione e scambio dei dati. Questa prospettiva introduce un ulteriore tema di tutt'altro che facile risoluzione: la governance dei flussi transfrontalieri di dati all'interno dell'Unione europea.

Come chiarito dal Considerando 5 del GDPR *L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. [...].*

Lo stesso dicasi per i flussi di dati non personali, ai quali è interamente dedicato il più volte citato Regolamento 2018/1807 FFD, il cui Considerando 10 recita eloquentemente: *A norma del regolamento*

(UE) 2016/679, gli Stati membri non possono limitare o vietare la libera circolazione dei dati personali all'interno dell'Unione per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento di dati personali. Il presente regolamento sancisce il medesimo principio di libera circolazione all'interno dell'Unione per i dati non personali [...]. Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati. [...][88].

Il combinato disposto dei due Regolamenti citati delinea dunque un modello di regolazione giuridica degli scambi di dati tra gli Stati membri, presupposto imprescindibile per lo sviluppo di una *data economy* dello spazio europeo.

La ritrosia degli Stati membri a considerare i servizi offerti e localizzati in altri Stati europei come facenti parte di un unico spazio giuridico, unita con un eccessivo protezionismo[89], ha portato ad una suddivisione delle banche dati nazionali in compartimenti stagni. Suddivisione che, come è evidente, ha sinora indebolito la posizione dell'Unione europea nell'economia globale.

Per contrastare questa tendenza l'Unione è impegnata nel rafforzamento di una visione comune che appare quanto mai necessaria alla tenuta e allo sviluppo del Mercato Unico Digitale. La scelta di contrastare le politiche nazionali di localizzazione, favorendo al contrario una apertura dei flussi tra Stati è condivisibile perché necessaria alla implementazione di una economia *data-driven*. Certamente il rafforzamento della fiducia rispetto alle modalità di trattamento dei dati e la chiara individuazione delle catene di responsabilità possono contribuire ad aumentare la fiducia e di conseguenza i flussi transfrontalieri di dati[90].

Tuttavia, sebbene il tema della fiducia sia di primaria importanza, vi è un dato strettamente giuridico che pare costituire la causa principale di questa disfunzione del sistema, ossia la frammentazione normativa che ancora differenzia sensibilmente le regole di trattamento dei dati. Questa realtà è stata bene messa in evidenza di recente nella relazione per i due anni di applicazione del GDPR[91]. In essa la Commissione denuncia quanto sia complesso sviluppare attività economiche/commerciali transfrontaliere, in particolare relative a tecnologie, innovazione e cybersecurity[92], a fronte di una ancora evidente differenziazione delle normative nazionali su aspetti di grande rilevanza pratica per le aziende, quali ad esempio il consenso dei minori in relazione ai servizi della società dell'informazione[93] e il regime di trattamento di particolari categorie di dati.

Peraltro la Commissione ha avuto l'occasione di richiamare gli Stati membri ad un "approccio paneuropeo", in stretto coordinamento per evitare la frammentazione, in sede di raccomandazioni per la gestione tecnologica della pandemia di Covid-19, con particolare riferimento alla gestione di situazioni di espansione transfrontaliera del contagio[94].

Tornando alla strategia dei *data spaces*, questa suddivisione per settori tematici dovrebbe contribuire a superare la descritta frammentazione, agevolando la condivisione di dati personali e non personali omogenei all'interno di aree regolamentate da norme comuni elaborate per quegli spazi. Nelle parole della Commissione: *Such spaces aim at overcoming legal and technical barriers to data sharing across organisations, by combining the necessary tools and infrastructures and addressing issues of trust, for example by way of common rules developed for the space*[95].

La Comunicazione, nella sua natura programmatica, non offre indicazioni specifiche sui passi che dovranno essere compiuti per la realizzazione di questo nuovo modello europeo di conservazione e condivisione dei dati. Significativamente però vengono annunciati, per il periodo 2021-2027, investimenti in un progetto ad alto impatto su spazi europei di dati e infrastrutture cloud federate.

Molto pragmaticamente la Commissione nel delineare i tratti principali della Strategia apre ad iniziative degli Stati membri per la realizzazione di infrastrutture comuni, annunciando la disponibilità ad elaborare protocolli d'intesa che favoriscano l'integrazione di tali iniziative nel progetto europeo[96].

Salta all'occhio, dato il tenore *high level* del documento, il riferimento esplicito al progetto franco-tedesco GAIA-X, che abbiamo citato nell'introduzione[97].

Occupiamoci brevemente di tratteggiare le caratteristiche distintive del progetto.

GAIA-X, nata da un'iniziativa del Governo tedesco, è divenuta ben presto oggetto di una partnership con la Francia, per poi essere presentata al resto dei Paesi dell'Unione europea con una conferenza di lancio che si è tenuta il 4 giugno 2020. Una volta realizzata, GAIA-X sarà una infrastruttura digitale *made in Europe*[98]. La sua ideazione ed il suo progressivo sviluppo sono il frutto della collaborazione di più di trecento partner pubblici e privati[99].

Da quanto è dato sapere, leggendo i documenti pubblicati in occasione del lancio del progetto, GAIA-X sarà un modulo di collegamento tra le infrastrutture di *cloud* ed *edge computing* nazionali. Così come per le infrastrutture, anche per quanto riguarda l'architettura giuridica è previsto che GAIA-X sia

disciplinata sulla base di principi, regole e standard già applicati nell'Unione europea[100].

L'infrastruttura sarà aperta alla partecipazione di attori pubblici e privati che rispettino quello che potremmo definire l'*acquis* di GAIA-X, ovvero l'insieme di principi e norme giuridiche e regole tecniche "europee" che l'iniziativa ha fatto proprie e che conta di arricchire con la progressiva elaborazione nuove policy e nuovi standard.

Di questo *acquis* fanno parte la protezione dati, la trasparenza, la fiducia, la sovranità sui dati, l'interoperabilità[101].

È bene a tal proposito evidenziare che all'interno di GAIA-X vengono utilizzati sia il termine *data sovereignty* che *digital sovereignty*[102]. Mentre la sovranità digitale viene definita come il potere di decidere *about how digital processes, infrastructures and the movement of data are structured, built and managed*, la *data sovreignty* viene presentata come un particolare aspetto della sovranità digitale, consistente nel pieno controllo del *data owner* rispetto alla collocazione e all'uso dei dati. La sovranità sui dati sarebbe dunque il primo passo per assicurare una sovranità digitale piena.

La finalità più volte richiamata nella documentazione rilasciata in occasione del lancio del progetto è di creare un ecosistema europeo per lo sviluppo della *data economy*[103]. GAIA-X si pone infatti come facilitatore dello sviluppo del mercato europeo dei dati[104]: nell'ecosistema di GAIA-X le imprese e le pubbliche amministrazioni dovrebbero sfruttare al massimo il potenziale dei dati, traendone servizi sempre migliori per la cittadinanza e sviluppo per il business delle imprese. Il tutto, entro i limiti della giurisdizione di almeno un Paese europeo.

GAIA-X sembra poter offrire una valida alternativa, seppure in gran parte ancora da costruire, alla dipendenza dell'Unione europea dai giganti tecnologici globali. Un ecosistema siffatto potrebbe rispondere alla richiesta di tutela dei diritti dei cittadini/utenti, favorire lo sviluppo della *data economy* a livelli davvero competitivi, e infine potrebbe garantire la sovranità digitale degli Stati membri dell'Unione europea. Alcuni punti però dovranno certamente essere chiariti nelle fasi di implementazione.

Ad esempio, vale la pena di precisare che ogni provider che entrerà a far parte dell'infrastruttura, resterà responsabile per il servizio da esso prestato[105]: *GAIA-X is a federated system of autonomous providers [. . .]. In accordance to the shared responsibility model each GAIA-X Partecipant is responsible for the service and data which is controlled by him.* Nei documenti pubblicati si legge anche che legittimamente un Consumer potrebbe richiedere una prova della reale localizzazione dei propri dati, rispetto a quanto garantito dal provider.

Dunque, privata dell'enfasi del lancio del progetto e dell'entusiasmo legato alla totale adesione alla strategia europea, GAIA-X si presenta come un sistema di collegamento tra server nazionali situati nel territorio dell'Unione. Una rete di *mutual agreements* consentirà di avere la certezza giuridica che tutti i partecipanti al progetto GAIA-X rispondano agli stessi requisiti tecnici e valoriali. Per la verifica della compliance al GDPR viene proposto l'utilizzo di certificazioni e codici di condotta a norma degli artt. 40 e 42 del Regolamento europeo[106].

Tale riferimento appare particolarmente adeguato e strategico, nell'ottica dell'efficienza del sistema e ancor di più nell'ottica dello sviluppo e rafforzamento dello spazio digitale europeo. Nella sistematica del GDPR l'elaborazione di codici di condotta dovrebbe contribuire alla corretta applicazione del Regolamento medesimo in settori specifici[107], mentre le certificazioni, i sigilli e i marchi dovrebbero servire a dimostrare la conformità al GDPR dei trattamenti svolti nella fornitura di prodotti e servizi[108].

L'articolo 40, relativo ai codici di condotta, prevede che il progetto di codice debba essere presentato dalle associazioni o altri organismi di rappresentanza di titolari e responsabili alla Autorità di controllo competente, ovvero quella dello Stato ove i richiedenti abbiano la sede legale. Se le attività si svolgono interamente nel territorio dello Stato di cui si trova l'associazione, l'Autorità competente potrà autonomamente procedere alla approvazione del codice di condotta.

Ma ciò che davvero rileva, rispetto all'argomento che ci occupa, è la procedura prevista dai paragrafi 7 e seguenti del medesimo articolo, relativa alle ipotesi di flussi transfrontalieri di dati. Infatti quando il progetto di codice di condotta si riferisce ad attività di trattamento che interessano diversi Stati membri, l'Autorità di controllo compente è tenuta, in ossequio al meccanismo di coerenza, a sottoporre il progetto al Comitato europeo per la protezione dei dati personali (EDPB). Il Comitato formulerà un parere che sarà poi trasmesso (in caso di valutazione positiva sulla conformità al GDPR) alla Commissione. Quest'ultima poi con un atto di esecuzione conferirà al codice di condotta validità generale su tutto il territorio dell'Unione.

Certificazioni, marchi e sigilli, possono essere rilasciati, a norma dell'art. 42, dalle Autorità di controllo, da organismi di certificazione o dal Comitato europeo (EDPB). Quest'ultimo ha il potere di approvare dei criteri di certificazione che consentano poi a titolari e responsabili del trattamento di otte-

nere un sigillo europeo. Anche in questo caso sono le Autorità di controllo ad individuare i criteri per la certificazione. La Commissione ha il potere, a norma dell'art. 43, di precisare i requisiti di cui tener conto delle certificazioni, oltre che di stabilire norme tecniche riguardanti tali meccanismi e la promozione degli stessi.

Dunque, come è stato autorevolmente evidenziato[109], nella produzione di codici di condotta e certificazioni le Autorità di controllo nazionali svolgono una funzione di primaria importanza. Non solo, in alcuni settori specifici, il GDPR prevede un intervento dell'European Data Protection Board per il controllo e il coordinamento delle Autorità nazionali coinvolte.

Posto l'ecosistema di riferimento, gli organi investiti dei poteri di regolazione e controllo, coordinati grazie ai meccanismi di cooperazione e coerenza, potranno contribuire alla creazione di regole condivise (tra cui i codici di condotta europei) che gradualmente condurranno alla realizzazione di uno spazio giuridico sicuro dal punto di vista delle tutele dei diritti fondamentali e funzionale allo sviluppo della *data economy*[110].

A sostegno di questa tesi deve essere ricordato, inoltre, che l'art. 64 par. 2 prevede che il Comitato europeo si pronunci su questioni di applicazione generale o relative a più Stati membri. Questo ruolo appare di importanza strategica per il progressivo consolidamento della *data governance* europea. Non a caso l'articolo 70 del GDPR individua nella garanzia dell'applicazione coerente del Regolamento la prima determinante funzione dell'EDPB.

Il ruolo appena tratteggiato delle Autorità di controllo, della Commissione e del European Data Protection Board nel consolidamento del Mercato Unico assume ancora più rilievo alla luce della possibilità offerta dal Regolamento a titolari e responsabili non soggetti al GDPR di aderire a codici di condotta e certificazioni nel quadro di trasferimenti di dati personali presso paesi terzi o organizzazioni internazionali.

A ben vedere la progressiva edificazione di un apparato regolamentare agile ed efficiente potrebbe essere la cifra distintiva della *(big) data governance* del settore pubblico attraverso la quale l'Unione potrà riaffermare (e tutelare) la sovranità europea sui dati nello scacchiere digitale globale.

Note

[1]The Guardian, *UK government told not to use Zoom because of China fears*, 24 April 2020.

[2]Divenuta popolarissima a seguito delle misure di isolamento e distanziamento sociale dovute al contenimento della pandemia di Covid-19. Il tema principale della presente ricerca non è strettamente connesso alla pandemia. Tuttavia, nello scritto si farà più volte riferimento ad atti, documenti, decisioni che sono correlati alla pandemia medesima, assumendo che il contesto della emergenza sanitaria globale dichiarata dall'Organizzazione Mondiale della Sanità il 30 gennaio 2020 sia noto ai lettori.

[3]Già da inizio aprile 2020 infatti un centro studi dell'Università di Toronto aveva evidenziato le debolezze del sistema di crittografia utilizzato dalla piattaforma e i rischi derivanti dal fatto che le chiavi di sicurezza fornite ai partecipanti agli Zoom meetings venissero inviate da server collocati in Cina: «An app with easily-identifiable limitations in cryptography, security issues, and offshore servers located in China which handle meeting keys presents a clear target to reasonably well-resourced nation state attackers, including the People's Republic of China». Cfr. B. Markzar, J. Scott-Railton, Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings, The citizen lab, University of Toronto, 3 aprile 2020.

[4]Cfr. *German government's digital summit*, 29 October 2019.

[5]Cfr. la posizione comune del 18 febbraio 2020.

[6]La presentazione ufficiale del progetto è avvenuta il 4 giugno 2020 con un evento promosso dal *German Federal Ministry for Economic Affairs and Energy*.

[7]Garante per la protezione dei dati personali, *Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro datadriven per l'emergenza COVID-19*, 7 aprile 2020.

[8]Richiesta peraltro esaudita, come risulta dal d.l. n. 28/2020 in cui all'art. 6, relativo al sistema di tracciamento, si specifica che la piattaforma unica nazionale di gestione del sistema di allerta costituenda sarà realizzata "esclusivamente con infrastrutture localizzate sul territorio nazionale".

[9]Cfr. il testo completo dell'intervista.

[10]O. Pollicino, *L'"autunno caldo" della corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in "Federalismi.it", 16 ottobre 2019.

[11]Si tratta delle decisioni: Corte di giustizia dell'Unione europea, sentenza C-507/17, *Google LLC contro Commission nationale de l'informatique et des libertés (CNIL)*, 24 settembre 2019; Corte di giustizia dell'Unione europea, sentenza C-18/18, *Eva Glawischnig-Piesczek contro Facebook Ireland Limited*, 3 ottobre 2019.

[12]Per l'analisi dei due casi si rinvia a O. Pollicino, *op. cit.*

[13]«Se ci terremo ad una tradizione [...] per cui il diritto è fatto, il fatto della volontà di chi ha la forza, e continueremo a fondarlo sulla sovranità, avremo un bel da fare a comprendere e governare un presente in cui la sovranità riesce sconfitta (per non fare che un esempio) da un giovanotto intelligente e pratico di computer. [...] Siamo stati abituati a pensare per duecento anni che la sovranità fosse la base del diritto. Proviamo ora a pensare che il diritto sia la base della sovranità», A. Gentili, *La sovranità nei sistemi giuridici aperti*, in "Politica del diritto", giugno 2011, n. 2, p. 205.

[14]Per una descrizione efficace dei rischi e delle potenzialità legati alla Big data analytics si veda S. Calzolaio, voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017, p. 594 ss.; su Big Data e machine learning, A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019, n. 1, pp. 87-106.

[15]Basti scorrere l'elenco delle Basi di dati di interesse nazionale, all'art. 60 del Codice dell'Amministrazione Digitale (CAD), d.lgs. n. 82/2005.

[16]Le definizioni di queste categorie sono contenute negli artt. 4 e 9 del Regolamento europeo sulla protezione dei dati personali (UE) 2016/679 (*General Data Protection Regulation*) e nell'art. 3 del Regolamento europeo sulla libera circolazione dei dati non personali (UE) 2018/1807 (*Free Flow Data Regulation*).

[17]S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in "Giornale di storia costituzionale", 2016, n. 31, p. 198.

[18]AGID, *Piano Triennale per l'Informatica 2019-2021.*

[19]Nel Piano Triennale 2019-2021 i limiti del paradigma Smart city, che hanno portato alla evoluzione nel modello Smart landscape sono descritti così: «Le iniziative finora condotte sul tema, in particolare da alcune città metropolitane, per quanto apprezzabili, sono però accomunate da un approccio limitato al contesto urbano di riferimento e quasi tutte prendono in maggior considerazione gli aspetti correlati al "cittadino" tralasciando quelli che hanno un forte impatto sulle imprese, quali, ad esempio, il movimento delle merci e le opportunità derivanti dalle integrazioni con altri sottosistemi (Port Communities, Cargo communities, nodi logistici territoriali, imprese di distribuzione. . .). [...] La logistica rappresenta un settore strategico per l'economia nazionale da considerare strumento di politica industriale, per valorizzare le eccellenze del sistema produttivo e per promuovere lo sviluppo del trasporto ecosostenibile e la tutela dell'ambiente. La declinazione del paradigma "Internet of Things" applicato alle merci implica l'integrazione dei servizi resi da differenti attori pubblici/privati che si può ottenere grazie ad una completa digitalizzazione della catena logistica. Soluzioni intelligenti, "smart", basate sull'utilizzo di corridoi e nodi logistici interconnessi, consentono di dominare la complessità in questo settore - legata anche al carattere multimodale del trasporto e alla pluralità di attori coinvolti – e di recuperare notevoli spazi di efficienza, ottimizzando i tempi ed i costi di spostamento delle merci, garantendo safety e security. L'attenzione va quindi rivolta ad un sistema ampio e complesso, che comprende anche una pluralità di "nodi logistici "(porti, aeroporti, retroporti, interporti, piattaforme logistiche territoriali, centri e aziende di distribuzione . . .) e dai collegamenti intermodali tra essi, necessari a rendere funzionale l'ambito logistico nel complesso, da tutti i nodi logistici e dalle città, perseguendo, attraverso un approccio sinergico, coordinato e integrato, un'ottica di ottimizzazione degli investimenti e di efficienza e lo sviluppo di sinergie di sistema, attuando una "logistica sostenibile" (sostenibilità economica, ambientale, sociale). [. . .] I programmi nazionali attivati e in via di attivazione dovrebbero essere quindi sinergicamente inquadrati in un'ottica più ampia per rendere interoperabili le soluzioni verticali sviluppate al fine di pervenire ad una gestione intelligente e sicura della mobilità, delle persone e delle merci, favorendo lo sviluppo di servizi basati sulle esigenze dei cittadini e delle imprese». Appare dunque evidente la spinta verso un modello integrato di servizi alla persona e servizi all'impresa/logistica.

[20]L'art. 50 del CAD prevede già la possibilità per le PA, nell'ambito delle proprie funzioni istituzionali, di procedere all'analisi dei dati, anche in combinazione con quelli detenuti da altre PA, da gestori di servizi pubblici e da società a controllo pubblico, escluse quelle quotate che non gestiscano servizi pubblici.

[21]Su questo tema sia consentito rinviare a V. Pagnanelli, *Accesso, accessibilità, Open data. Il modello italiano di Open data pubblico nel contesto europeo*, in "Giornale di storia costituzionale", 2016, n. 31, p. 205 ss.

[22]Si veda in proposito F. Sciacchitano, *Disciplina e utilizzo degli Open Data in Italia*, in "Medialaws", 2018, n. 1, p. 281 ss.

[23]S. Calzolaio, voce *Protezione dei dati personali*, cit., p. 601.

[24]Il modello di gestione della pandemia della Regione Veneto, pur nella complessità delle questioni giuridiche che ha sollevato e che non possono essere trattate in questa sede, pare essere stato, almeno in una prima fase, un esempio di utilizzo efficace delle banche dati nel contenimento dell'emergenza sanitaria.

[25]A titolo di esempio, sull'utilizzo delle tecniche di *Deep fake* si veda F. Bertoni, *Deepfake, ovvero Manipula et impera. Un'analisi sulle cause, gli effetti e gli strumenti per la sicurezza nazionale, nell'ambito dell'utilizzo malevolo dell'intelligenza artificiale ai fini di disinformazione e propaganda*, in "Ciberspazio e diritto", 2019, n. 1-2, pp. 11-28.

[26]Sulle potenzialità ed i rischi dell'utilizzo dei *Big Data* nel settore pubblico si veda G.M. Ruotolo, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in Studi sull'integrazione europea, 2018, n. 3, p.105 ss.; più in generale, su opportunità e rischi della democrazia al "tempo del digitale", P. Costanzo, *La democrazia digitale (precauzioni per l'uso)*, in "Diritto pubblico", 2019, n. 1.

[27]Autorità garante della Concorrenza e del Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, documento finale, 10 febbraio 2020.

[28]*Ivi*, pp. 68-69.

[29]Per tutti, G. D'Acquisto, M. Naldi, *Big data e privacy by design*, Giappichelli, 2017, in particolare Cap. 1, *Big Data e protezione dei dati personali.*

[30]Autorità per le Garanzie nelle Comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 14.

[31]Cfr. *Ibidem*, *Executive Summary*, p. 7.

[32]L'articolo 3 n. 1 del Reg. n. 2018/1807 definisce i dati come «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del Regolamento (UE) n. 2016/679».

[33]L'art. 8 dello stesso articolato, che prevede la elaborazione da parte della Commissione, entro il 29 novembre 2022, di una relazione sull'attuazione del Regolamento e in particolare sugli insiemi misti di dati personali e non personali in ragione dei futuri progressi tecnologici non prevedibili, sembra confermare le perplessità.

[34]Regolamento n. 2018/1807, art. 3 n. 2.

[35]Le regole contenute nei massimari di conservazione e scarto ed il vaglio della Sovraintendenza archivistica definiscono ulteriormente il quadro di gestione degli archivi pubblici.

[36]Il titolare del trattamento è la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che determina finalità e mezzi del trattamento dei dati personali (GDPR, art. 4 n. 7).

[37]Cioè la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare (GDPR, art. 4 n. 8).

[38]A solo titolo di esempio, l'esito dell'attività di scarto nell'archivio cartaceo comporterà la distruzione materiale dei documenti attraverso invio al macero, da affidarsi a imprese specializzate in tale senso; la medesima attività si svolgerà con modalità ovviamente differenti presso gli archivi digitali.

[39]Cfr. d.lgs. n. 82/2005, art. 42.

[40]«[...] la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del trattamento», GDPR, art. 28 par. 3.

[41]Il riferimento è all'art. 17 bis del decreto c.d. "Cura Italia" (d.l. 17 marzo 2020, n. 18 conv. con legge 24 aprile 2020, n. 27) in cui viene elencata una lunga serie di soggetti che al fine di poter gestire e contenere l'emergenza sanitaria da Covid-19

sono autorizzati a trattare dati anche relativi agli articoli 9 e 10 del GDPR e a farne oggetto di comunicazione.

[42]Cfr. la bozza delle Linee guida.

[43]Garante per la protezione dei dati personali, *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, 13 febbraio 2020.

[44]«Lo scopo dell'Agenda Digitale è fare leva sul potenziale delle tecnologie ICT per favorire innovazione, progresso e crescita economica, avendo come obiettivo principale lo sviluppo del mercato unico digitale. Nel quadro dell'Agenda Digitale Europea, l'Italia ha sviluppato l'Agenda Digitale Italiana, una strategia nazionale per raggiungere gli obiettivi indicati dall'Agenda Europea». Cfr. l'Agenda Digitale.

[45]Presidenza del Consiglio dei Ministri, *Strategia per la crescita digitale 2014-2020*, 21 giugno 2016, p. 61.

[46]«In base al principio Cloud First, le PA in fase di definizione di un nuovo progetto, e/o sviluppo di nuovi servizi, devono, in via prioritaria, adottare il paradigma cloud in particolare i servizi SaaS, prima di qualsiasi altra opzione tecnologica». Cfr. *Il cloud enablement*.

[47]*Ibidem*.

[48]«Le applicazioni cloud (SaaS) si pagano generalmente in base al consumo, consentono di gestire la crescita di un servizio in maniera dinamica e richiedono investimenti iniziali estremamente limitati. [...] Il ridotto investimento iniziale implica una riduzione del rischio, è così possibile sviluppare e testare, su scala ridotta, soluzioni che possono essere valutate velocemente per poi essere adottate, modificate radicalmente o abbandonate, con costi minimi». Cfr. *Perché usare il cloud*.

[49]«Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione [...]». Si veda in proposito A. Masucci, *Digitalizzazione dell'amministrazione e servizi pubblici online. Lineamenti del disegno normativo*, in Diritto Pubblico, 2019, n. 1, p. 140 ss.

[50]Razionalizzazione significativamente basata sul coordinamento informatico a livello centrale. A norma dell'art. 14 del CAD «L'AgID assicura il coordinamento informatico dell'amministrazione statale, regionale e locale [...]». Sul punto M. Di Francesco Torregrossa, *La competenza statale nel processo di digitalizzazione delle pubbliche amministrazioni*, in Consulta online, 2019, n. 1, p. 64 ss.

[51]Cfr. *Le performance digitali di tutti i Paesi dell'UE*.

[52]Cfr. *Lo scoreboard italiano*.

[53]Il 79% degli utenti utilizza internet per fruire di musica, video e giochi.

[54]V. *supra* nota 49, p. 14.

[55]L'art. 3 riconosce a chiunque il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti previsti dal CAD nei rapporti con le amministrazioni pubbliche.

[56]Come prescritto dall'art. 8 del CAD.

[57]Sul ruolo-chiave della *digital literacy* per lo sviluppo del Mercato Unico Digitale cfr. V. Pagnanelli, *op. cit.*, p. 212: «L'evoluzione rapida e irreversibile verso l'amministrazione digitale pone tra le priorità assolute il superamento del *digital divide*, e di conseguenza i passi da compiere in quella direzione. Tra di essi un serio investimento sulla *digital literacy* appare ormai necessario».

[58]«Lo sfruttamento della capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione nonché nelle competenze digitali, come l'alfabetizzazione ai dati (data literacy), accrescerà la sovranità tecnologica dell'Europa nell'ambito delle tecnologie e infrastrutture abilitanti fondamentali per l'economia dei dati». Commissione europea, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, 19 febbraio 2020, p. 4.

[59]A norma dell'art. 6, la piattaforma unica nazionale per la gestione del sistema di allerta «è di titolarità pubblica ed è realizzata [. . .] esclusivamente con infrastrutture localizzate sul territorio nazionale».

[60]Cfr. *supra* nota 5.

[61]Comitato parlamentare per la sicurezza della Repubblica (COPASIR), *Relazione sui profili di sicurezza del sistema di allerta Covid-19 previsto dall'articolo 6 del decreto-legge n. 28 del 30 aprile 2020*, 13 maggio 2020.

[62]*Ivi*, p. 11.

[63]*Ivi*, p. 13.

[64]Garante per la protezione dei dati personali, *Parere sullo schema di "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici"*, cit.

[65]*Ivi*, Capitolo 1.10.

[66]Vedi la *Circolare qualificazione cloud service provider*; per una analisi dei modelli Cloud e delle diverse tipologie di servizi forniti si rimanda interamente al contributo di Vanni Boncinelli, in questo fascicolo.

[67]Vedi *AGID Cloud Marketplace*.

[68]Garante per la protezione dei dati personali, *Processo penale da remoto: lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro della Giustizia, Alfonso Bonafede*, 16 aprile 2020.

[69]La notissima sentenza con cui la Corte di Giustizia UE ha dichiarato l'invalidità della decisione della Commissione UE n. 2000/252/CE sull'accordo denominato Safe Harbour relativo al trasferimento dei dati personali di cittadini europei verso gli USA. Sul caso Schrems si vedano, *ex plurimis* G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai «Safe Harbour Principles» al «Privacy Shield»", Tre Press, 2016, pp. 23-48; M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in "Rivista AIC", 2016, n. 3; V. Fiorillo, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in "Federalismi.it", 26 luglio 2017. Un nuovo capitolo della vicenda è stato scritto di recente con la pubblicazione il 16 luglio 2020 della sentenza nella causa C-311/18 *Data Protection Commissioner / Maximilian Schrems e Facebook Ireland*, con la quale la Corte di Giustizia UE ha dichiarato l'invalidità della decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del c.d. Privacy Shield EU-US per il trasferimento di dati personali verso gli Stati Uniti (sentenza pubblicata quanto il presente articolo era già in bozze e quindi citata solo nei riferimenti essenziali).

[70]V. Zeno Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta, V. Zeno Zencovich (a cura di), "op. cit.", p. 11.

[71]Per una contestualizzazione G. Greenleaf, *Asian data privacy law. Trade and Human rights perspectives*, Oxford University Press, 2014, p. 192 ss.; J.R. Lindsay, T.M. Cheung, D.S. Reveron, *China and cybersecurity espionage, strategy and politics in the digital domain*, Oxford University Press, 2015, in particolare, Cap. 10; G. Austin, *Cybersecurity in China. The next wave*, Springer, 2018.

[72]Per una analisi del contenuto della *Cybersecurity Law* si vedano L. Huang, D. Ilan, K. Mooney Carrol, Z. Zhou, *Understanding the impact of China's far-reaching new Cybersecurity law*, in "Intellectual Property & Technology Law Jour-

nal", 2018, n. 2, p. 15 ss.; Q. Aimin, S. Guosong, Z. Wentong, *Assessing China's cybersecurity law*, in "Computer Law & Security Review", 2018, n. 34, p. 1342 ss.

[73] *National standards* e *technical guidances* sono ulteriormente suddivisi per tipologia in *mandatory standards* (GB Standards), *voluntary standards* (GB/T Standards) *and technical guidance* (GB/Z guidance).

[74] Cfr. Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*, p. 1344. L'Italia si è dotata della propria *cybersecurity law* con il d.l. 21 settembre 2019 n. 105, conv. con l. 18 novembre 2019 n. 133, che ha istituito il perimetro di sicurezza nazionale cibernetica.

[75] La legge cinese prevede una disciplina "aggravata" per gli operatori di *Critical Information Infrastructure*, definite come «infrastructure that is used in public communications and information services, energy, transportation, water conservancy, finance, public services or electronic governance or that, if it were destroyed, malfunctioned or leaked data, could seriously endanger national security, national welfare and the people's livelihood, or the public interest»; cfr. L. Huang, D. Ilan, K. Mooney Carrol, Z. Zhou, *op. cit.*, p. 17 ss.

[76] Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*

[77] *Ivi*, pp. 1345-1346.

[78] Cfr. *supra* nota 73.

[79] «Specifically, the data required to be stored locally in accordance with other laws or regulations include: population and Health data (Section 10 of the Provisional Measures on Population health Information Management), credit information (Section 24 of the Rules on Credit Industry Administration), personal financial information (Article 6 of the People's Bank of China Notice on the Protection of Personal Financial Information), map data (Section 34 of the Rules on Map Management), online publication data (Article 8 of the Regulations on the Administration of Online Publishing Services); data related to online car-hailing business (Article 27 of the Provisional Measures on Online Car-hailing Operation Service Management)»; cfr. Q. Aimin, S. Guosong, Z. Wentong, *op. cit.*, p. 1351.

[80] Cfr. la *Federal Cloud Computing Strategy*.

[81] Cfr. il testo del *Cloud Act*; il *White paper* pubblicato dal U.S. Department of Justice nell'aprile 2019 ne descrive *background*, caratteristiche e finalità.

[82] Cfr. *Cloud Act*, Sec. 105. *Executive agreements on access to data by foreign governments*, nella quale sono elencati i requisiti che il Governo straniero deve possedere per poter sottoscrivere un accordo bilaterale.

[83] «A long-established way for the U.S. government to access private information held abroad is through Mutual Legal Assistance Treaties. These agreements permit a public authority seeking data to ask for the assistance of the country in which the data is held and require that country to cooperate in processing such requests under its domestic law. MLATs establish legal mechanisms for cooperation between signatory nations in criminal matters and proceedings, including the exchange of evidence and information during criminal proceedings», P.M. Schwarts, *Legal access to the global cloud*, in Columbia Law Review, 2018, n. 6, p. 1720.

[84] Sulle criticità del meccanismo introdotto dal *Cloud Act* si veda H.H. Abraha, *How compatible il the US "Cloud Act" with cloud computing? A brief analysis*, in International Data Privacy Law, 2019, n. 3, p. 207 ss.; *contra* M.W. Brennan, W. Maxwell, A.A. Sura, *Demistifying the Cloud Act: assessing the law's compatibility with international norms and the GDPR*, Hogan Lovells, January 2019, i quali sostengono che le garanzie introdotte dal *Cloud Act* siano adeguate agli standard internazionali in materia di protezione dati, compreso il GDPR.

[85] Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale* - COM/2018/225 final 2018/0108 (COD).

[86] Il *Data Trustee model* elaborato da Microsoft per il mercato tedesco costituisce un esempio di tali soluzioni. In proposito cfr. H.H. Abraha, *op. cit.*, p. 208: «This arrangement [the Data trustee model, N.d.A.] could create a situation where personal data concerning a US person and required for US domestic crime investigation purpose is neither located in the USA nor effectively controlled by a US company». Il modello *Data trustee* elaborato da Microsoft consente alla *company* di mantenere la responsabilità sul servizio dal punto di vista tecnico, rispettando allo stesso tempo la esigenza di localizzazione dei dati sul territorio tedesco, in modo che gli stessi siano esclusivamente sottoposti alla legislazione tedesca. Il *trustee* tedesco e l'interessato potranno accedere ai dati, mentre Microsoft potrà farlo solo in limitati casi previsti dal contratto.

[87] *European Commission*, *Communication from the Commission to the European Parliament, The Council, The European economic and social Committee and the Committee of the Regions. "A European strategy for data"* - COM(2020) 66 final, 19 febbraio 2020.

[88] L'articolo 4 del Regolamento FFD vieta agli Stati di imporre obblighi di localizzazione che impongano di effettuare il trattamento sul territorio dello Stato o ostacolino il trattamento in un altro Stato membro. Per una disamina approfondita delle regole sulla circolazione dei dati nell'ordinamento europeo si rimanda al contributo di Stefano Torregiani, in questo fascicolo.

[89] Il Copasir, nell'esprimere preoccupazione rispetto ad usi malevoli dei dati conservati al di fuori del territorio italiano, ha fatto esplicito riferimento ad "attori europei ed internazionali" che possano a vario titolo essere interessati alle informazioni raccolte, lasciando trasparire la mancanza di una visione in tema di spazio comune europeo dei dati.

[90] Il Considerando 7 del GDPR fa riferimento all'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. Franco Pizzetti lo definisce «principio di fiducia, che deve essere assunto come criterio interpretativo di base e come l'obiettivo ultimo che giustifica anche la stretta connessione fatta dall'art. 1 GDPR tra l'attuazione del diritto fondamentale alla tutela dei dati e la necessità di garantirne la libera circolazione»; cfr. F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 170.

[91] European Commission, *Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation* - COM(2020) 264 final, 24 giugno 2020.

[92] Cfr. *Ivi*, p. 7.

[93] Il GDPR lascia agli Stati la possibilità di stabilire un'età inferiore a sedici anni (opportunità colta per esempio dall'Italia, che con l'art. 2 *quinquies* del Codice della Privacy novellato ha abbassato la soglia a quattordici anni).

[94] European Commission, *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*.

[95] European Commission, *Communication from the Commission to the European Parliament, The Council, The European economic and social Committee and the Committee of the Regions. "A European strategy for data"*, cit., p. 16.

[96] *Ivi*, p. 18.

[97] *Supra* par. 1.

[98] *GAIA-X: The European project kicks off the next phase*, June, 2020, p. 2.

[99] Tra di essi anche Google Germany GmbH.

[100] Su portabilità, interoperabilità, interconnessione tra infrastrutture, applicazioni, dati.

[101] Il documento *GAIA-X: Policy Rules and Architecture of Standards*, June 2020, richiamando la posizione Franco-tedesca li individua in: «1. European data protection 2. Open-ness, reversibility, and transparency 3. Authenticity and trust 4. Digital sovereignty and self-determination 5. Free market access and European value creation 6. Modularity and interoperability 7. Federation of infrastructure».

[102] GAIA-X: Technical Architecture, June 2020, p. 3.

[103] «GAIA-X combines the technological and industrial strengths of EU industry, academia and the public sector to develop an ecosystem of data and infrastructure providers and a regulatory framework based on fundamental European values and standards. The initiative supports the target of the EU to be-come a global leader in innovation in the data economy and its data-driven applications as set out in the European data strategy»; *GAIA-X: Driver of digital innovation in Europe*, May 2020, p. 25

[104] *Ivi*, p. 39.

[105] *GAIA-X: Technical Architecture*, cit., p. 30.

[106] *Ivi*, p. 32.

[107] Il Considerando 99 del GDPR specifica che i codici di condotta dovrebbero facilitare l'applicazione del regolamento «tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese».

[108] Cfr. Considerando 100 del GDPR, secondo cui certificazioni, sigilli e marchi dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati offerto da tali prodotti e servizi.

[109] F. Pizzetti, *op. cit.*, p. 175 ss.

[110] In particolare le certificazioni, strumenti chiaramente elaborati per essere impiegati a livello europeo, potranno essere utilizzati dalle Autorità nazionali, dall'EDBD e dalla Commissione per agevolare la circolazione dei dati nello spazio digitale dell'Unione. Pizzetti sottolinea le differenze di formulazione degli articoli 40 e 42, che lungi dall'esser solo formali, evidenziano una spiccata opzione per le certificazioni di validità europea. Cfr. F. Pizzetti, *op. cit.*, p. 157 e p. 160.

* * *

Data storage and digital sovereignty: The public (big) data governance facing the new global challenges

Abstract: By using data retention policies in the public sector as a paradigm, the paper reflects on how States are asserting or defending their digital sovereignty. The article recalls the digitization path of the Italian PA, on which big data has had a significant impact. The digital data storage has imposed the transition from paper archives to the cloud, a transition regulated by national and European legislation and partly influenced by the digital strategies of the great world powers. The proliferation of localization obligations and prohibitions confirms the complexity and centrality of these issues in the protection of digital sovereignty. The paper ends with an analysis of the key points of the *European strategy for data* published by the European Commission in February 2020, and with a look at the Franco-German data storage and data sharing project called GAIA-X.

Keywords: Data storage – Digital sovereignty – Public sector – Data localization

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0023

Modelli tecnici e disciplina giuridica del c.d. cloud computing

Vanni Boncinelli

Il mercato dei servizi di *cloud computing* ha registrato negli ultimi anni uno tasso di crescita esponenziale, che la recente emergenza sanitaria mondiale finirà per rafforzare ulteriormente. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione "sinergica" di fattori, nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha portato a nuove modalità di utilizzo dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, i quali non potrebbero esistere (o quasi) senza le risorse computazionali, applicative e di *storage* messe a disposizione da fornitori di *cloud computing*. Dal punto di vista giuridico, tuttavia, il *cloud computing* lascia sul tappeto enormi interrogativi ancora in gran parte irrisolti. Come proteggere i diritti degli interessati quando i loro dati possono essere spostati, spacchettati, ricomposti e replicati in qualsiasi nodo della rete globale con un semplice click? Come regolare un caleidoscopio di servizi così diversi tra loro e ripartire obblighi e responsabilità tra i vari soggetti che compongono la "filiera" *cloud*? Per molti versi, l'approccio seguito da Stati Uniti e Unione europea non potrebbe essere più diverso, ma entrambi scontano la pretesa di voler regolare in modo unilaterale un fenomeno – il *cloud computing* e, più in generale, Internet – nel quale "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Cloud computing – Cloud Act – e-Evidence Regulation

Sommario: *1. Introduzione – 2. Un* cloud*, mille* cloud*. Genesi, evoluzione e caratteristiche del* cloud computing *– 3. I principali modelli di servizio – 4. I modelli di distribuzione del* cloud computing *– 5. Una classificazione alternativa dei servizi* cloud*:* Data Shard*,* Data Localization*,* Data Trust *– 6. L'approccio al* cloud *al di là dell'oceano: i casi* Microsoft Ireland *e* Google Pennsylvania *– 7. Alcune osservazioni sul* Cloud Act *– 8. L'accesso ai dati conservati sul* cloud*: la proposta di Regolamento* e-Evidence *– 9. Riflessioni conclusive*

1. Introduzione

Nel giro di poco più di dieci anni, il *cloud computing* ha conosciuto uno sviluppo esponenziale che non accenna a rallentare[1]. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione sinergica di fattori tecnologici (la sovrabbondanza di risorse non utilizzate, lo sviluppo della virtualizzazione, ecc.), nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha imposto nuovi modelli di fruizione dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, resi possibili dalle risorse computazionali, applicative e di *storage* messe a disposizione dagli operatori di *cloud computing*.

Questo sviluppo travolgente si è tuttavia accompagnato a crescenti difficoltà nel trovare un punto di equilibrio tra esigenze diverse e spesso contrapposte, che vanno dalle preoccupazioni per la privacy e la sicurezza informatica, alla lotta all'evasione fiscale, dal perseguimento dei reati allo spionaggio industriale.

V. Boncinelli è dottore di ricerca in "Teoria del diritto e della politica" presso l'Università degli Studi di Macerata (2005) e svolge la propria attività di consulente informatico specializzato in soluzioni *cloud* e architetture distribuite.

Molto spesso si è finito per concentrarsi su un unico aspetto, trascurando le concrete modalità di funzionamento del *cloud computing* e, più in generale, della rete Internet. Si è così assistito alla proliferazione di obblighi più o meno generalizzati di localizzazione dei dati (*data residency*). Queste misure di localizzazione, per quanto possano assumere le forme più variegate e rispondere ai fini più disparati, sono accomunate dal fatto di porre intenzionalmente ostacoli al flusso di dati attraverso i confini nazionali, ad esempio imponendo di conservare i dati all'interno di server ubicati nel territorio dello Stato, ovvero subordinando il trasferimento dei dati al previo consenso dell'interessato. Il numero di Paesi che hanno introdotto obblighi di questo tipo è in continuo aumento[2]. Uno degli ultimi esempi di questo tipo è rappresentato dall'art. 6, co. 5, del D.L. 30 aprile 2020, n. 28, che nel dettare le linee guida per lo sviluppo della nota piattaforma per la prevenzione e il tracciamento dei casi di Covid-19 ("Immuni"), ha previsto che debba essere "realizzata con infrastrutture localizzate sul territorio nazionale"[3].

Quali che siano le motivazioni dietro all'introduzione di tali misure, è indubbio che stiamo assistendo a un'inversione di tendenza nell'atteggiamento nei confronti dei flussi di dati: se in passato la preoccupazione principale di molti Paesi era quella di mantenere alcune informazioni "al di fuori" dei confini nazionali (si pensi ai sistemi di censura e alla protezione della proprietà intellettuale), oggi gli sforzi maggiori sembrano esser rivolti nel senso opposto, ovvero quello di tenere le informazioni relative ai propri cittadini all'"interno"[4].

Contemporaneamente, però, si assiste anche al fenomeno inverso: quando si tratta di garantire l'interesse pubblico all'accertamento dei reati e all'acquisizione delle prove digitali che si trovano conservate al di fuori del territorio nazionale, anziché guardare al luogo di conservazione dei dati (che costringerebbe le autorità nazionali ad avviare le complesse procedure previste dai trattati di mutua assistenza giudiziaria) si preferisce agire sui soggetti, *in primis* i fornitori di servizi *cloud*, che su tali dati esercitano una qualche forma di controllo, affinché producano le informazioni richieste. In questa direzione si muovono, solo per fare alcuni esempi, tanto il contestatissimo *Cloud Act* del 2018, quanto la proposta di regolamento della Commissione europea relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*), entrambi trattati nelle pagine che seguono.

Si crea così un perverso circolo vizioso, nel quale il proliferare degli obblighi di localizzazione viene assunto come giustificazione delle norme che mirano a "estendere" la giurisdizione degli Stati nazionali al di fuori del loro territorio, con ciò alimentando timori e diffidenze che si traducono nell'adozione di nuovi e più penetranti obblighi di localizzazione. Il problema è che, come accade ogniqualvolta si tenti di regolare in modo settoriale e locale un fenomeno di portata globale, si rischia non solo di non raggiungere il risultato sperato ma, anzi, di moltiplicare e amplificare gli effetti negativi sui diritti dei singoli, sulla sicurezza informatica e la privacy, la libertà di concorrenza e gli investimenti[5].

Scopo di questo contributo non è quello di fornire un'esaustiva ricognizione dei tanti, tantissimi punti critici che si accompagnano ai recenti tentativi di regolazione del fenomeno, né tantomeno di proporre soluzioni generali buone per tutte le stagioni. L'obiettivo, assai più limitato e circoscritto, è quello di evidenziare come, al di là delle definizioni astratte, quando si parla di *cloud computing* si fa in realtà riferimento a un complesso e variegato "ecosistema" di servizi, applicazioni, metodologie e pratiche che presentano tante differenze e peculiarità quanto sono i caratteri in comune. Il problema, ovviamente, non è solo di natura "tassonomica", poiché alla base di qualsiasi tentativo di regolazione del *cloud*, come del resto dell'intera Internet, vi dovrebbe essere la consapevolezza che gli interessi in gioco sono inevitabilmente confliggenti. Ragione in più per evitare tanto un approccio di tipo *one size fits all*, quanto la sua eccessiva "parcellizzazione" in tante legislazioni nazionali e di settore.

2. Un *cloud*, mille *cloud*. Genesi, evoluzione e caratteristiche del *cloud computing*

La storia del *cloud* è disseminata di piccole e grandi innovazioni, la più importante delle quali è stata certamente la nascita e l'inarrestabile diffusione di Internet, che oggi conta 4.5 miliardi di utilizzatori attivi, pari al 59% della popolazione mondiale[6]. Nel ricostruire la genesi del *cloud computing* si è soliti partire dalla tecnologia del *mainframe computing* sviluppata a partire dalla fine degli anni '50 del secolo scorso[7]. Questi costosissimi e ingombranti elaboratori venivano utilizzati per processare dati ed effettuare calcoli che oggi potrebbero essere svolti senza fatica anche dal più economico *smartphone* disponibile sul mercato. Se confrontati con gli standard odierni, questi sistemi erano estremamente difficili da usare, privi com'erano di un'interfaccia umana, o persino di una tastiera, e programmati mediante schede perforate o nastri magnetici.

Considerato che un'università o un'azienda normalmente potevano permettersi al massimo uno o due *mainframe*, era necessario ottimizzare al massimo l'utilizzo delle risorse computazionali. L'idea alla base della condivisione delle risorse nasceva da una semplice constatazione: l'inserimento di un programma all'interno dell'elaboratore richiedeva un tempo considerevole, durante il quale le capacità computazionali rimanevano in larga parte inutilizzate. Al contrario, un ampio gruppo di utenti che lavoravano contemporaneamente avrebbe permesso di utilizzare le pause di un utente intento a inserire dati per destinare il tempo di elaborazione a vantaggio degli altri. Di qui l'elaborazione di metodi di *time-sharing* in grado di consentire a più utenti di condividere le risorse del *mainframe*, utilizzando dei terminali privi di una propria capacità di elaborazione (e per questo definiti anche *dumb terminal* o, con un'espressione tornata recentemente alla ribalta proprio in connessione con lo sviluppo del *cloud computing*, *thin client*).

Un'altra importante innovazione fu rappresentata dalla "virtualizzazione". A cavallo degli anni '60 e '70 furono rilasciati i primi sistemi operativi in grado di supportare la possibilità di condividere un insieme di risorse hardware (dischi rigidi, processori, ecc.) tra più sistemi operativi "virtuali" che "convivono" sullo stesso computer fisico. Questi sistemi operativi virtuali sono completamente isolati gli uni dagli altri, e possono utilizzare soltanto le risorse di tipo "logico" (capacità computazionale, di *storage*, di connettività, ecc.) messe a disposizione dal sistema di virtualizzazione, e da questo dinamicamente allocate tra le varie macchine virtuali a seconda delle esigenze (*pooling*).

Sebbene i concetti fondamentali del *cloud computing* risalgano dunque agli albori dell'informatica, l'uso del termine *cloud* per indicare un nuovo modo di accedere al software, potenza di calcolo e capacità di archiviazione dei dati attraverso il web è invece relativamente recente. Contrariamente a quanto si potrebbe pensare, l'espressione *cloud computing* non è nata nell'ambiente *hi-tech*, ma è stata coniata durante una (si presume fumosa) riunione dei responsabili del *marketing* tenutasi nel 1996 negli uffici di Houston della Compaq Computer. L'espressione non indicava tanto un insieme specifico di tecnologie, quanto piuttosto un diverso modello di consumo dei servizi informatici tramite Internet[8].

Le origini del termine spiegano forse il perché il concetto di *cloud*, con i suoi contorni indefiniti ed evanescenti, abbia sin da subito creato difficoltà, equivoci e incomprensioni (che continuano a tutt'oggi) non solo tra gli addetti ai lavori, ma anche per i governi che a più riprese sono intervenuti nel tentativo di regolare il fenomeno, i quali si sono trovati nella necessità di definire cosa rientri nel concetto di *cloud computing* e cosa no. Non a caso, una delle prime pubblicazioni dedicata al *cloud computing* da parte del *National Institute for Standards and Technology* (NIST), a cui si deve peraltro la più citata definizione di *cloud*, si apre con l'affermazione per cui «Cloud computing can and does mean different things to different people»[9]. In altre parole, non esiste un solo *cloud*. Come vedremo nelle prossime pagine, una parte consistente dei problemi che nascono sul piano della regolazione del fenomeno possono essere affrontati solo se si tengono in debito conto le peculiarità dei diversi modelli di *cloud*.

Dunque, di *cloud computing* esistono svariate definizioni, che pongono l'accento ora su alcuni caratteri, ora su altri[10]. Tuttavia, un aspetto generale su cui le varie formulazioni convergono è l'idea per cui il *cloud* abbia rappresentato un completo mutamento di paradigma rispetto alle forme tradizionali di utilizzo dei servizi informatici[11].

Volendo partire da una definizione comunemente accettata, possiamo prendere a prestito quella offerta proprio dal NIST: «Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction»[12].

Proviamo a specificare meglio la definizione sopra riportata, evidenziando alcune caratteristiche essenziali. Per prima cosa, il *cloud* introduce (o consiste di) una serie di livelli di "astrazione" che permettono di utilizzare determinate risorse senza doversi preoccupare della loro gestione, configurazione, manutenzione, messa in sicurezza, ecc. Sebbene la ripartizione delle responsabilità tra fornitore del servizio e utilizzatore vari in base al "modello di servizio" (su cui torneremo più avanti), l'elemento comune è che le risorse utilizzate dall'utente hanno, come si è accennato parlando di virtualizzazione, un carattere prettamente logico, anziché "fisico".

Tali risorse sono messe in comune per servire molteplici utenti mediante un modello condiviso (c.d. *multi-tenant*), assegnate e riassegnate dinamicamente in base alla domanda (*resource pooling*). Possono essere accedute, create, gestite o dismesse direttamente dall'utente, con poca o nessuna interazione con il fornitore e tramite meccanismi standard, accessibili via Internet da piattaforme eterogenee (*broad network access*), e utilizzate in piena autonomia, secondo le proprie necessità (*on-demand*

self-service). Le risorse possono essere inoltre acquisite e rilasciate in modo elastico, in alcuni casi anche automaticamente, per scalare[13] rapidamente le capacità del sistema in relazione alla domanda (*rapid elasticity*). Infine, i sistemi *cloud* monitorano e ottimizzano costantemente l'uso delle risorse (*measured service*), facendo leva sulla capacità di misurazione ad un livello di astrazione appropriato per il tipo di servizio (ad esempio memoria, elaborazione, larghezza di banda e utenti attivi) e, in genere, con costi legati all'utilizzo delle risorse[14].

3. I principali modelli di servizio

Sulla base della definizione sopra riportata, il NIST individua tre specifici "modelli di servizio", distinti in base al tipo di risorsa messa a disposizione e al ruolo riservato all'utente che acquista il servizio: si parla così di *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS), e *Software-as-a-Service* (SaaS).

In un servizio di tipo IaaS, il fornitore del servizio *cloud* mette a disposizione i componenti necessari a realizzare una propria infrastruttura informatica virtuale. Rispetto a una tradizionale infrastruttura locale, costituita da server, dischi rigidi e sistemi di rete che devono essere acquistati o noleggiati, gestiti per tutto il loro ciclo di vita e sostituiti in caso di problemi, un'infrastruttura *cloud* si basa sul carattere puramente "virtuale" delle risorse. Questo significa, tra le altre cose, che gli utenti non devono preoccuparsi dell'installazione, della configurazione e della manutenzione dell'hardware e dei sistemi infrastrutturali, che è a totale carico del fornitore *cloud*. Gli utenti rimangono invece responsabili della configurazione dei sistemi che vengono eseguiti sull'infrastruttura virtuale (come i sistemi operativi e le applicazioni che ci girano sopra). I più diffusi servizi IaaS sono rappresentati da macchine virtuali, servizi di *storage* dei dati e servizi di rete virtuali (*virtual networking*).

In un servizio di tipo PaaS, invece, la piattaforma mette a disposizione dell'utente l'ambiente di esecuzione di un'applicazione (quale ad esempio un sito web), a mantenerlo in esecuzione anche in caso di problemi nei livelli sottostanti dell'infrastruttura (grazie a sofisticati meccanismi di *fault-tolerance* e di replica geografica dei dati), garantendo inoltre alti livelli di performance e di scalabilità del servizio. In un servizio PaaS, il fruitore non si deve preoccupare dell'infrastruttura, della connettività, della configurazione del sistema operativo o di altri aspetti legati all'ambiente di esecuzione. Tutti questi dettagli sono a carico del fornitore *cloud* e all'utente resta la sola responsabilità di gestire l'applicazione[15].

Infine, le soluzioni SaaS liberano gli utenti sia dalla gestione del sistema operativo, che dalla supervisione dell'applicazione: tutto ricade nelle mani del fornitore del servizio. Tutto quello che l'utente deve fare è usare l'applicazione messa a disposizione dal fornitore senza doversi preoccupare di altro. Tipicamente, i servizi SaaS sono usufruiti tramite un *web browser*, e tanto i dati applicativi quanto il carico di lavoro sono trasferiti sull'infrastruttura dell'operatore *cloud*, il che rende possibile sfruttare un'ampia gamma di funzionalità direttamente dallo schermo del proprio *smartphone* o da qualunque altro dispositivo connesso a Internet. A essere interessati da questa trasformazione non sono soltanto gli utenti finali, ma anche le aziende e le pubbliche amministrazioni. Gran parte del lavoro che prima veniva svolto sfruttando applicazioni e servizi installati in locale (sui server aziendali o direttamente sulle postazioni lavorative), si avvale oggi del web per numerose funzioni (dall'archiviazione dei dati alle analisi di *business intelligence*, dai filtri *antispam* alla lotta al *malware*).

Con il tempo, accanto a questi tre modelli tradizionali se ne sono aggiunti di nuovi. Nel tentativo di dare specifico risalto alle peculiarità dei nuovi servizi lanciati a un ritmo quasi giornaliero, e forse anche per venderli meglio, sono stati elaborati un gran numero di acronimi (es. *Database-as-a-Service*, *Storage-as-a-Service*, *Disaster Recovery-as-a-Service*, *Workplace-as-a-Service*, *Desktop-as-a-service*, ecc.)[16]. Di recente, vista l'impossibilità di arginarne la proliferazione, è stata proposta anche un'ulteriore tipologia, definita "XaaS" (o *X-as-a-Service*), dove la "X" sta a indicare non tanto uno specifico modello di servizio, quanto piuttosto una sorta di categoria residuale entro cui ricondurre tutti quei servizi *cloud* che non si lasciano facilmente incasellare in una delle tre categorie tradizionali, vuoi perché se ne differenziano sotto aspetti rilevanti, vuoi perché presentano elementi di tutte e tre le classificazioni precedenti.

Questo tipo di classificazione ha ovviamente un valore puramente esemplificativo e non ha alcuna pretesa di esaustività delle differenze e delle particolarità dei numerosi servizi *cloud* oggi disponibili sul mercato. Quando, poco più di dieci anni fa, questa classificazione si è affermata tra gli addetti ai lavori, i servizi offerti erano relativamente pochi (macchine virtuali, servizi di rete, applicazioni web, ecc.). In quel contesto, la distinzione tra IaaS, PaaS e SaaS era sufficiente a descrivere, se non tutti, la gran parte dei servizi offerti. Negli ultimi anni si è assistito al proliferare di decine e decine di nuovi servizi,

sempre più sofisticati ed evoluti. Oggi si contano centinaia di servizi *cloud* diversi, che sono andati ad arricchire l'offerta accanto a quelli più "tradizionali": servizi di intelligenza artificiale e *machine learning*, analisi dei dati, *Internet of Things* (IoT), *blockchain* e cripto-valute, *streaming* di contenuti multimediali, realtà aumentata (*augmented reality*), sicurezza informatica, servizi per dispositivi mobili, ecc.

Anche con tutti questi limiti, tuttavia, la distinzione tra IaaS, PaaS e SaaS ha una sua rilevanza. Come abbiamo visto, nel caso di servizi IaaS e PaaS l'utente ha un controllo molto più accentuato sui dati, potendo innanzitutto scegliere dove tali dati devono essere conservati, partizionati o replicati. Nel caso di servizi SaaS, invece, l'utente non ha in genere alcun controllo su dove i dati sono conservati o sulle misure di sicurezza applicate. Tra queste ultime, una menzione particolare va alla cifratura dei dati conservati o in transito sull'infrastruttura. Nei servizi SaaS, la scelta di cifrare o meno i dati di cui è "titolare" l'utente del servizio (ad esempio le fatture dei clienti, le e-mail, i messaggi scambiati in software, i dati di produzione, ecc.) ricade sul fornitore del servizio software, che decide anche le modalità di gestione delle relative chiavi. Nei servizi di tipo IaaS e PaaS, la gestione di questi aspetti è lasciata per lo più all'utente, e dipende in buona sostanza dal livello di sicurezza che quest'ultimo mira a implementare[17]. Queste differenze nel grado di libertà lasciato all'utilizzatore del servizio discendono dal fatto che, mentre questi ultimi due modelli sono rivolti principalmente a organizzazioni, pubbliche o private, dotate delle necessarie competenze tecnologiche e professionali, i servizi SaaS, nella misura in cui sollevano l'utente da qualunque responsabilità in merito alla loro gestione, possono essere utilizzati da chiunque, sia esso un utente finale o un'organizzazione (si potrebbe dire, sotto questo profilo, che sono servizi "chiavi in mano").

In altri termini, i servizi infrastrutturali (così come la maggior parte di quelli PaaS, in cui la "piattaforma" può essere vista come una sorta di "ponte" tra l'infrastruttura e il servizio applicativo finale), oltre a rappresentare un modello alternativo alla gestione in proprio di risorse informatiche (con tutti i benefici che ne derivano in termini di risparmio e flessibilità), possono essere visti anche come una "borsa degli attrezzi" a cui attingere per "confezionare" servizi applicativi ad alto valore aggiunto (come ad esempio sistemi per la gestione e la fidelizzazione dei clienti, per la pianificazione delle risorse aziendali, ovvero per facilitare lo *smart-working* e la collaborazione da remoto, ecc.) destinati ad essere rivenduti a clienti finali (altre organizzazioni o persone fisiche).

Questo rilievo mette in luce un aspetto spesso sottovalutato quando si tratta di elaborare le regole da applicare al *cloud computing*. Sempre più spesso, infatti, la realizzazione di una soluzione *cloud* comporta la combinazione di molteplici servizi, di natura anche assai diversa e con l'intervento di fornitori terzi. Tale complessità è in genere "trasparente"[18] dal punto di vista dell'utente finale, il quale si limita a utilizzare il servizio senza rendersi conto della sottostante complessità. Ad esempio, se dalla prospettiva di un utente, il servizio di archiviazione *cloud* di Dropbox può apparire come un classico SaaS, dietro le quinte il servizio ha utilizzato per molti anni l'infrastruttura messa a disposizione da un altro fornitore (in questo caso Amazon AWS)[19]. Dropbox era dunque al tempo stesso un utilizzatore di servizi di tipo IaaS (forniti da Amazon) e, dal punto di vista dei suoi utenti, un fornitore di servizi di tipo SaaS.

La struttura naturalmente aperta e "partecipativa" del *cloud* pone non pochi interrogativi quando si tratta, ad esempio, di definire formalmente i ruoli dei vari soggetti coinvolti nel trattamento di dati personali. Come vedremo meglio nelle prossime pagine, tutte queste differenze giocano un ruolo importante anche sul piano degli effetti della regolazione. Lo stesso vale, seppur sotto altri profili, per i diversi modelli di distribuzione dei servizi *cloud* oggi presenti sul mercato, che si distinguono principalmente in base ai loro destinatari.

4. I modelli di distribuzione del *cloud computing*

Accanto ai tre modelli di servizio, il NIST individua infatti anche quattro modelli di distribuzione, distinguendo tra *cloud* pubblici, privati, "comunitari" (*community cloud*) e ibridi.

In un *cloud* pubblico, la modalità di distribuzione di gran lunga più comune e diffusa, l'infrastruttura è predisposta per essere utilizzata dalla generalità degli utenti. Le risorse sono di proprietà del fornitore e vengono distribuite tramite Internet a chiunque ne faccia richiesta (esempi di *cloud* pubblici sono Amazon Web Services, Microsoft Azure e Google Cloud). Nel *cloud* pubblico le risorse hardware sono condivise dai vari utenti (o *tenant*) e allocate secondo logiche che ne massimizzano l'efficienza.

In un *cloud* privato, invece, l'infrastruttura tecnologica è predisposta per essere utilizzata in via esclusiva da una singola organizzazione. In questo caso, a consumare le risorse condivise sono in genere le diverse unità che compongono l'organizzazione (dipartimenti, direzioni, uffici, ecc.). Tanto l'ubicazione fisica quanto la proprietà dell'infrastruttura è

irrilevante: può essere gestita direttamente dall'organizzazione o affidata, in tutto o in parte, a fornitori terzi, così come può comprendere un solo *data center* situato all'interno dei locali dell'organizzazione, ovvero più *data center* distribuiti in località diverse. Quello che conta è che nell'infrastruttura, anche se gestita da un terzo, tutte le risorse sono dedicate a uno specifico cliente. Molto spesso le organizzazioni di una certa dimensione optano per un *cloud* privato (magari riconvertendo l'infrastruttura tradizionale già esistente) per motivi legati alla sicurezza dei dati (dal momento che questi rimangono all'interno del perimetro dell'organizzazione), ovvero per soddisfare particolari requisiti di localizzazione previsti da normative di settore, o ancora per il tipo particolare di applicazioni utilizzate dall'azienda.

Il *cloud* comunitario, nonostante il nome, è assimilabile *in toto* a quello privato, con la sola differenza che in questo caso l'infrastruttura è messa a esclusiva disposizione di più organizzazioni che hanno obiettivi o necessità (es. di sicurezza, normativi, ecc.) condivise. Come un qualsiasi *cloud* privato, può essere gestito da una o più organizzazioni della comunità o affidato, in tutto o in parte, a un fornitore terzo (che può consistere, ad esempio, in un raggruppamento temporaneo di imprese).

Nel *cloud* ibrido, infine, *cloud* pubblici e privati sono integrati per svolgere funzioni distinte all'interno della stessa organizzazione. Negli ultimi anni questa forma di *cloud* ha conosciuto una notevole diffusione, acquisendo sempre maggiori quote di mercato rispetto agli altri modelli di distribuzione[20], grazie ai vantaggi che presenta per le organizzazioni, che possono sia usufruire delle risorse illimitate (e poco costose) messe a disposizione dal *cloud* pubblico, sia soddisfare particolari esigenze di sicurezza o di *compliance* normativa garantite dal *cloud* privato.

Ciascun modello di distribuzione porta con sé vantaggi e svantaggi. In generale, tanto i *cloud* pubblici che quelli privati sono caratterizzati da un'alta efficienza grazie alla virtualizzazione e alla condivisione delle risorse, consentendo così un migliore bilanciamento del carico di lavoro; da un'elevata disponibilità, che minimizza i tempi di inattività e migliora la continuità aziendale; nonché da una scalabilità elastica (che nel caso di *cloud* privati incontra tuttavia un limite nelle risorse fisiche non infinite a disposizione di un'organizzazione, mentre in quello pubblico sono virtualmente illimitate).

Alcuni vantaggi, invece, sono specifici del *cloud* pubblico, quali bassi costi iniziali (mentre in quello privato sono particolarmente elevati); elevate economie di scala in termini di potere di acquisto delle apparecchiature che di efficienza nella gestione; semplicità di gestione, in quanto l'infrastruttura è gestita, configurata e mantenuta dal fornitore (mentre in quello privato sono richieste competenze tecniche specifiche, oltre che capacità organizzative e disponibilità economiche al di fuori della portata di molte organizzazioni).

Di contro, il *cloud* privato consente, come si è detto, di avere un maggiore controllo in tema di sicurezza e conformità normativa, nonché di garantire una maggiore qualità del servizio, poiché l'infrastruttura può essere configurata e ottimizzata per venire incontro alle specifiche esigenze di un'organizzazione[21].

Sulla base di questa classificazione, un'eventuale infrastruttura *cloud* gestita da o per conto di soggetti che svolgono compiti e funzioni di natura pubblica si configurerebbe comunque come *cloud* privato (o comunitario, qualora condiviso da più soggetti), indipendentemente dal fatto che a fornire (e a gestire) l'infrastruttura sia o meno un soggetto pubblico. L'unico elemento rilevante, in questo schema, è infatti il carattere esclusivo delle risorse *cloud* usufruibili, e non la "natura" del soggetto (o dei soggetti) che, a seconda dei casi, forniscono o utilizzano detti servizi[22].

5. Una classificazione alternativa di *cloud computing*: *Data Shard*, *Data Localization*, *Data Trust*

Le tradizionali classificazioni dei servizi *cloud* sin qui sommariamente illustrate dovrebbero aver già lasciato intuire la complessità dei modelli che stanno dietro l'erogazione di servizi apparentemente semplici, se considerati dal punto di vista dell'utente finale. A queste classificazioni, però, se ne affianca un'altra che riveste un'importanza assolutamente centrale quando si affrontano le tematiche relative alla localizzazione dei dati, perché basata sulla diversa modalità di gestione dell'infrastruttura, o meglio dei dati che su tale infrastruttura circolano: *Data Shard*, *Data Localization* e *Data Trust*[23].

Nel modello definito *Data Shard*, l'informazione è divisa, o meglio "partizionata", in molteplici "frammenti" (*shard*) dispersi in vari nodi della rete. Tramite il partizionamento, un archivio di grandi dimensioni viene suddiviso in "componenti" più piccoli, più efficienti e "maneggevoli" rispetto all'originale[24]. Alle strategie di partizionamento si ricorre in genere per migliorare le performance delle operazioni che coinvolgono grandi volumi di dati, ovvero per "avvicinare" i dati agli utenti sulla base della loro ubicazione geografica, in modo da ridurre i tempi di latenza e

migliorare le prestazioni complessive[25]. Le ragioni che stanno dietro questo tipo di strategie sono dunque di natura eminentemente tecnica: «The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world»[26].

Nel modello denominato *Data Localization*, il fornitore dei servizi *cloud* conserva i dati all'interno di un certo ambito geografico che, a seconda dei casi, può avere estensioni assai diverse, e che solo occasionalmente coincide con i confini di uno Stato. Nell'individuazione dei diversi ambiti geografici in cui suddividere l'infrastruttura concorrono molteplici ragioni, di natura economica, tecnica e, non ultima, legale, come l'esistenza di obblighi positivi di localizzazione dei dati (es. Francia e Germania).

Solitamente, l'infrastruttura globale dei grandi operatori di servizi *cloud* comprende più aree geografiche o regioni più o meno estese (ad esempio Europa centrale, Stati Uniti occidentali, ecc.). Ciascuna di queste aree è, a livello infrastrutturale, completamente autonoma e indipendente dalle altre, così da garantire la massima stabilità e tolleranza ai guasti. Ogni area o regione è a sua volta suddivisa in più zone di disponibilità. Queste zone, che comprendono uno o più *data center* muniti di impianti indipendenti per l'energia, il raffreddamento e la rete, sono fisicamente isolate le une dalle altre, ma connesse tramite collegamenti dedicati a bassa latenza. Mediante la suddivisione di un'area in zone più circoscritte si cerca di garantire la costante disponibilità dei servizi all'interno di quell'area, mediante la replica delle risorse in diverse zone geografiche, di modo che queste siano sempre accessibili anche quando, ad esempio a seguito di una calamità naturale, si verificano dei problemi in uno o più *data center*[27].

Il modello di *Data Trust* è senz'altro quello più interessante ai fini della nostra discussione, se non altro perché non nasce per soddisfare esigenze tecniche, quanto piuttosto come tentativo, da parte dei fornitori di servizi *cloud* (in questo caso Microsoft), di trovare una via d'uscita da una situazione sempre più insostenibile. Come vedremo meglio nelle prossime pagine, infatti, l'approvazione del *Cloud Act* da parte del Congresso USA e la conseguente pretesa di poter accedere ai dati degli utenti custoditi dai fornitori *cloud* americani indipendentemente dal luogo in cui sono conservati, ha gettato ulteriore benzina sui timori di indesiderate interferenze da parte degli Stati Uniti sui dati dei cittadini di altri Paesi[28]. Di fronte al moltiplicarsi degli obblighi di localizzazione dei dati, spaventati dalla possibilità di perdere rilevanti quote di mercato a favore di concorrenti più piccoli, ma fuori dalla portata del governo americano, alcune aziende d'oltreoceano hanno finito per elaborare un approccio assolutamente originale, che combina elementi legali, organizzativi e tecnici per separare nettamente la gestione dell'infrastruttura dall'accesso ai dati che su tale infrastruttura insistono.

Nel modello di *Data Trust*, elaborato a partire da concetti e istituti giuridici di origine anglosassone, il fornitore di servizi *cloud* si avvale infatti di un soggetto esterno, detto *data trustee*, per la gestione di tutto ciò che esula dalla stretta manutenzione operativa dell'infrastruttura. L'elemento giuridico essenziale è dato dal ricorso alla figura negoziale del *trust*[29], mediante il quale il fornitore si spoglia completamente della facoltà giuridica di accedere ai dati che transitano sull'infrastruttura per affidarli a una terza parte (nel caso in questione, una sussidiaria della tedesca Deutsche Telekom). Qualsiasi attività operativa svolta dal fornitore dell'infrastruttura che potrebbe potenzialmente consentire l'accesso ai dati dei clienti (come ad esempio la gestione degli incidenti, l'aggiornamento del software, ecc.) è soggetta a controlli tecnici che richiedono l'approvazione e la supervisione esplicite del fiduciario dei dati. L'accesso ai sistemi è inoltre consentito solo nell'ambito di un servizio specifico, per uno scopo definito, e solo per il tempo strettamente necessario allo svolgimento delle attività tecniche, che sono strettamente registrate e monitorate.

Sul piano tecnico, la separazione dei profili relativi alla gestione dell'infrastruttura da quelli dell'accesso ai dati viene garantita, oltre che dalla segregazione fisica e logica di reti e sistemi, principalmente da meccanismi di cifratura dei dati, le cui chiavi sono conservate in via esclusiva dal fiduciario. Tutte le richieste di accesso ai dati, dunque, devono essere indirizzate al *trustee* (l'unico in possesso delle chiavi di cifratura), il quale sarà tenuto a valutarle esclusivamente sulla base del diritto nazionale. Proprio l'elaborazione del principio di separazione tra la gestione dell'infrastruttura e l'accesso ai dati che su di essa insistono rappresenta uno degli elementi maggiormente innovativi e, possibilmente, più dirompenti dell'attuale panorama dei servizi di *cloud computing*.

È opportuno precisare, prima di continuare oltre, che questi diversi modelli non si escludono necessariamente l'un l'altro, ma – entro certi limiti – possono combinarsi variamente all'interno di una stessa soluzione. Il modello di *Data Trust* tedesco, ad esempio, prevede che i dati siano conservati all'interno dei confini nazionali (*Data Localization*), anche se – dal punto di vista teorico – questo non sembra essere un requisito necessario per raggiungere le finalità che tale modello persegue (prima fra tutte quella di evi-

tare l'insorgere di conflitti di giurisdizione), poiché le modalità tecniche, organizzative e legali adottate sono di per sé sufficienti a escludere qualunque accesso esterno ai dati stessi (anche qualora, in ipotesi, fossero localizzati in *data center* collocati in altri Paesi europei). Né l'eventuale presenza di obblighi di localizzazione esclude, di per sé, il ricorso alle tecniche di partizionamento dei dati (*Data Shard*), anche se queste avranno una portata assai più limitata, potendo riguardare unicamente *data center* collocati entro i confini nazionali (con ciò sacrificando in misura significativa l'efficacia complessiva del sistema).

Nei prossimi paragrafi ci soffermeremo su alcuni dei passaggi salienti che hanno caratterizzato l'accidentato percorso seguito dalla giurisprudenza e dal legislatore USA in tema di accesso ai dati custoditi su *cloud* da parte delle pubbliche autorità. In questo breve *excursus* non si può non partire dalla celebre decisione della corte d'appello nel caso *Microsoft Ireland*, che, dando prevalenza all'ubicazione geografica dei dati, ha riconosciuto il diritto del fornitore a non ottemperare all'ordine delle autorità federali di comunicare il contenuto di e-mail conservate nel territorio irlandese. Vedremo anche come tale decisione, al netto delle questioni ermeneutiche di diritto interno, sia stata di fatto resa possibile dal particolare modello di servizio utilizzato dall'operatore *cloud* (di tipo *Data Localization*). Vedremo anche come siano state sempre le effettive modalità di gestione del servizio *cloud* a rendere impossibile l'applicazione dello stesso principio in un caso apparentemente identico (*Google Pennsylvania*), perché espressione di un diverso modello di *cloud* (*Data Shard*). Infine, accenneremo agli aspetti salienti del *Cloud Act*, approvato dal Congresso USA proprio per disinnescare le potenziali conseguenze della decisione del caso *Microsoft Ireland*, ma che ha finito per ottenere il risultato opposto rispetto a quello perseguito, a dimostrazione di come la complessità e la varietà dei modelli *cloud* siano state, ancora una volta, sostanzialmente ignorate.

6. L'approccio al *cloud* al di là dell'oceano: i casi *Microsoft Ireland* e *Google Pennsylvania*

Il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* è stato adottato dal Congresso USA nel marzo del 2018 come risposta alla decisione della corte d'appello nel caso *United States v. Microsoft Corp.*[30]. In quell'occasione, Microsoft si era opposta a un ordine (*warrant*) emesso dalle autorità federali americane sulla base delle disposizioni dello *Stored Communication Act* (SCA) del 1986, di produrre, tra le altre cose, il contenuto di e-mail riconducibili a un determinato *account* di posta elettronica[31].

Microsoft, che pure aveva fornito alle autorità i dati custoditi sui server in territorio americano, si era rifiutata di dare accesso ai contenuti delle e-mail perché conservate nei suoi *data center* di Dublino, dunque al di fuori del territorio statunitense, con ciò suggerendo l'idea della prevalenza dell'ubicazione "fisica" dei dati nella determinazione della giurisdizione. Nell'accogliere il ricorso di Microsoft e ribaltare la decisione di primo grado, il giudice d'appello muove infatti dal rilievo secondo cui Microsoft archivia i dati associati al contenuto della posta elettronica dei propri utenti su oltre cento *data center* sparsi per il mondo. Quando viene creato un *account*, l'utente seleziona automaticamente un "codice Paese" e Microsoft archivia il contenuto delle e-mail associate a quell'*account* (nonché tutta una serie di contenuti ulteriori, quali documenti, calendari, ecc.) nel *data center* più vicino al Paese identificato dall'utente[32]. L'ubicazione fisica dei dati è, per la corte, l'elemento oggettivo da cui partire per decidere dell'applicabilità extra-territoriale delle disposizioni dello SCA: «Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States»[33].

Quando, nel 1986, il Congresso approvò lo SCA come parte del più ampio *Electronic Communications Privacy Act*, l'obiettivo era quello di proteggere la privacy degli utenti nel contesto dei nuovi mezzi tecnologici che richiedono l'interazione di un utente con un fornitore di servizi, anche perché "trent'anni fa, i confini internazionali non venivano attraversati così regolarmente come lo sono oggi", grazie a reti e infrastrutture hardware sparse in tutto il mondo per soddisfare le richieste degli utenti. Né esplicitamente, né implicitamente, lo SCA prende in considerazione l'applicazione delle sue disposizioni al di fuori del territorio americano. E questa – conclude la corte – è esattamente la vera questione del giudizio: «It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. (...) It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in

which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our border»[34].

La decisione ha sorpreso molti commentatori perché, nell'offrire una lettura molto più restrittiva delle norme dello SCA (e in particolare dell'istituto del *warrant*), ha messo in discussione il tradizionale test in base al quale l'elemento critico nel determinare se l'ordine di produrre la documentazione richiesta sia o meno eseguibile è dato dal fatto che il destinatario abbia o meno "il controllo, la custodia o il possesso" della stessa, indipendentemente dal luogo in cui tali informazioni sono conservate al momento della richiesta[35]. Il timore che la decisione del caso *Microsoft Ireland* potesse porre, ove confermata dalla Corte Suprema davanti alla quale la questione era stata sollevata, un ostacolo alle indagini aventi ad oggetto dati collocati al di fuori del territorio statunitense ha spinto il Congresso ad approvare rapidamente il *Cloud Act*.

Il carattere "eccezionale" del caso *Microsoft Ireland* è stato spesso ricondotto alla diversa lettura offerta dalla corte d'appello circa l'estensione dello SCA al di fuori del territorio americano. A riprova di tale carattere viene solitamente citato il caso *Google Pennsylvania*, di poco successivo al primo, nel quale il giudice ribalta il principio espresso nel caso Microsoft e impone al fornitore *cloud* di ottemperare all'ordine emesso dalle autorità federali[36]. Solo pochi commentatori hanno invece evidenziato come l'opposto risultato raggiunto nei due casi dipenda in larga parte dal diverso modello di *cloud* al centro della contesa[37].

Nel caso *Google Pennsylvania*[38], infatti, a essere coinvolti erano una serie di servizi i cui dati sono suddivisi in componenti che la sottostante infrastruttura provvede a smistare tra vari nodi della sua rete globale, spostandoli automaticamente da un nodo all'altro sulla base di logiche di natura prettamente tecniche, legate alla complessiva efficienza e affidabilità del sistema. Si trattava insomma di un caso di *Data Shard*, secondo la classificazione esposta nella prima parte del contributo.

Il caso riguardava due *search warrant* emessi per dati associati ad altrettanti *account* di utenti di Google. Quest'ultimo, da parte sua, aveva parzialmente ottemperato alla richiesta fornendo informazioni archiviate in *data center* situati negli Stati Uniti. Al tempo stesso, basandosi sul precedente Microsoft, si era rifiutata di fornire i dati che, in base a logiche interne di partizionamento, si trovavano su server collocati all'estero. Uno dei passaggi fondamentali seguiti dalla corte nell'arrivare alla conclusione positiva circa l'obbligo di Google di fornire per intero le informazioni richieste muove proprio dalla questione relativa a come i dati siano stati partizionati e dove si trovino i vari *shard*[39]: «Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process. (...) Google's architecture not only divides user data among data centers located in different countries, but also partitions user data into shards. Furthermore, the data automatically moves data from one location on Google's network to another as frequently as needed, to optimize for performance, reliability, and other efficiencies. Because of the structure of this system, Google cannot say with any certainty which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process»[40].

Secondo la Corte, piuttosto che a mere *possibilities and legal abstractions*, occorre guardare alla realtà dei fatti. In questo caso, la realtà era che Google avrebbe potuto accedere a tutte le informazioni direttamente dalla sede centrale in territorio americano, a nulla rilevando l'ubicazione fisica dei dati, che in questo caso è così frammentaria da considerarsi evanescente. Il ricorso al criterio del "possesso, custodia o controllo" è dunque una strada resa necessaria dalla natura stessa del servizio *cloud*. L'opposto orientamento mostrato dalla corte d'appello nel caso Microsoft nasce dalla diversa configurazione del servizio *cloud* al centro della contesa, nel quale tutti i dati rilevanti erano conservati "in via esclusiva e in modo stabile" nel suo *data center* irlandese. Nel caso *Google*, invece, il giudice muove dalla constatazione secondo cui non sussiste alcuna prova circa l'esatta ubicazione dei server su cui sono ospitate le informazioni richieste dalle autorità federali.

«Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a "seizure" because there is no meaningful interference with the account holder's possessory interest in the user data. Indeed, (...) Google regularly transfers user data from one data center to another without the customer's knowledge. Such transfers do not interfere with the customer's access or possessory interest in the user data. Even if the transfer interferes with the account owner's

control over his information, this interference is de minimis and temporary».

Il fatto che l'operatore *cloud* ricorra a tecniche di partizionamento per massimizzare l'efficienza dell'infrastruttura, in modo del tutto invisibile e trasparente per l'utente finale (che anzi non ha alcuna idea circa l'ubicazione dei propri dati, né tantomeno delle sottostanti logiche di partizionamento) implicherebbe, secondo la corte, che non si possa parlare di interferenza con il possesso dei dati da parte dell'utente. Se, per effetto di queste logiche interne, i dati si trovano partizionati in *data center* collocati all'estero, questo rappresenta un elemento del tutto accidentale, perché in fondo neppure il fornitore saprebbe indicare con precisione dove e in quali server sono presenti questi frammenti[41]. L'unico elemento rilevante è, per la Corte, la possibilità di accedere ai dati, nella loro forma "ricomposta", dalla sede centrale del fornitore, situata in territorio USA e come tale soggetta all'osservanza delle norme federali.

Nel confermare l'obbligo di Google di adempiere a quanto richiesto dalle autorità USA, il giudice esclude però che questo comporti un'applicazione extraterritoriale alle disposizioni dello SCA. L'argomento principale sembra essere dunque di natura prettamente contingente, relativo al particolare modello di servizio *cloud* al centro della questione: «No one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified»[42].

Mettendo a confronto il caso *Microsoft Ireland* con il caso *Google Pennsylvania*, è facile notare come le due decisioni abbiano ad oggetto modelli di servizio e di gestione del *cloud* assai diversi[43]. La prevalenza al criterio dell'ubicazione fisica dei dati nel primo, così come la prevalenza del criterio del controllo sui dati, nel secondo, dipendono in ultima analisi dal tipo di servizio al centro della discussione. Nel caso Microsoft, l'applicazione del criterio del luogo di residenza dei dati è resa possibile dal particolare modello di gestione dell'infrastruttura, in cui l'informazione si trova stabilmente ubicata all'interno di confini definiti (*Data Localization*). Questa caratteristica tecnica del servizio, frutto di scelte più o meno arbitrarie dell'operatore *cloud*, rappresenta l'elemento che abilita, sul piano pratico, la discussione sull'eventuale efficacia extraterritoriale delle norme che ne prevedono la confisca o il sequestro, alla pari di qualunque altro oggetto fisico.

Anche nel caso Google sono i caratteri contingenti del servizio a indirizzare e condizionare l'inquadramento legale del caso. Qui, le modalità tecniche scelte dal fornitore per ottimizzare la complessiva infrastruttura (*Data Shard*) rendono virtualmente impossibile ricorrere al criterio della ubicazione dei dati, sia dal punto di vista concettuale che da quello pratico. Questi vengono infatti spostati e riallocati continuamente da un nodo della rete ad un altro sulla base di logiche interne, largamente automatizzate, che rendono difficilmente percorribili i tradizionali canali della cooperazione giudiziaria internazionale. La vera questione, secondo il giudice, non è tanto l'applicabilità extraterritoriale delle disposizioni dello SCA, quanto piuttosto il rischio, concretissimo, di rendere eccessivamente difficoltoso, o addirittura impossibile, l'accesso alle informazioni da parte delle forze di polizia e dell'autorità giudiziaria: il timore del c.d. *going dark*.

7. Alcune osservazioni sul *Cloud Act*

Se è vero che esistono sostanziali differenze tra Stati Uniti e Unione europea in merito agli standard di protezione dei dati personali, che il *Cloud Act* ha peraltro contribuito ad acuire, è anche vero che quest'ultimo si proponeva, almeno nelle intenzioni, di facilitare la cooperazione internazionale attraverso lo strumento degli *executive agreement* e, al tempo stesso, offrire alle aziende destinatarie delle richieste di accesso un meccanismo giuridicamente azionabile per contestarne la legittimità. Alla base della soluzione prescelta dal legislatore USA vi erano infatti alcune condivisibili preoccupazioni. In primo luogo, l'aumento esponenziale delle richieste di accesso ai dati da parte di Paesi terzi, dovuto proprio all'esplosione dei servizi di *cloud computing* (i cui principali operatori sono, per l'appunto, domiciliati negli USA)[44].

L'aumentato carico di lavoro per l'ufficio dell'US Department of Justice (DOJ) ha comportato un repentino allungamento dei tempi necessari per completare i complessi adempimenti procedurali previsti dai vari trattati di mutua assistenza legale (MLAT), con il conseguente rischio di vanificare importanti indagini giudiziarie[45]: «The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world. While the MLAT process remains a critical evidence-gathering mechanism, the system has faced significant challenges keeping up with the increasing demands for electronic evidence in criminal investigations worldwide. Moreover, because many [Cloud Service Provider] move data among data storage centers in various countries, and split up data into different pieces stored in different locations, it can be difficult both for governments

and for the CSPs themselves to know where relevant data is located at any point in time for purposes of sending and fulfilling MLAT requests. The international community thus faces a critical question of how to provide governments efficient and effective access to evidence needed to protect public safety while preserving respect for sovereignty and privacy.»[46]

Due sono gli elementi essenziali del *Cloud Act*[47]. Il primo riguarda l'esplicito riconoscimento dell'applicabilità delle disposizioni dello SCA anche alle informazioni digitali conservate da fornitori di servizi *cloud* al di fuori del territorio USA. Ciò che conta è che il fornitore sia soggetto alla giurisdizione nazionale e abbia il possesso, la custodia o il controllo sui dati di cui si richiede la trasmissione: «A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.»

Per quanto, come si è accennato, tale previsione non abbia rappresentato di per sé una novità – in quanto il principio era già applicato da tempo dalla giurisprudenza prevalente, oltre che riconosciuto a livello internazionale dalla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[48] – la sua formalizzazione in un atto legislativo ha avuto se non altro il merito di aver reso esplicito l'atteggiamento del governo federale nei confronti degli operatori *cloud* domiciliati negli Stati Uniti, prevedendo al contempo alcune garanzie procedurali e sostanziali a tutela dei diritti dei cittadini e residenti USA, oltre che un meccanismo per contestare le richieste delle autorità federali (su cui subito *infra*).

Il secondo elemento è dato dalla previsione di un meccanismo basato su *executive agreement*, e dalla connessa definizione di *qualifying foreign government*. In particolare, il *Cloud Act* consente al governo USA di stipulare "accordi esecutivi" (*executive agreements*) bilaterali con Paesi terzi[49]. Questi accordi consentono ai Paesi firmatari di presentare, nell'ambito di indagini aventi ad oggetto *serious crimes*[50], richieste semplificate di accesso ai dati direttamente ai fornitori di servizi domiciliati negli Stati Uniti, secondo un meccanismo che andrebbe a completare, anziché a sostituire, le procedure attualmente previste dai trattati di assistenza giudiziaria esistenti.

Il *Cloud Act* introduce anche un meccanismo per consentire ai fornitori di servizi *cloud* di contestare (*quash*) le richieste delle autorità federali, qualora ricorrano due condizioni: il disvelamento delle informazioni può comportare per il fornitore il rischio concreto di violare un obbligo previsto dalla legislazione di un *qualifying foreign government*, e l'utilizzatore del servizio *cloud* non è un cittadino statunitense, né risiede negli Stati Uniti. Prima di accogliere la richiesta dell'operatore *cloud*, tuttavia, il giudice è chiamato a soppesare con attenzione tutti gli interessi in gioco nel caso specifico, alla luce di una serie di parametri indicati dallo stesso *Cloud Act* (la cosiddetta *comity analysis*)[51]. Nel prevedere una corsia preferenziale per i Paesi terzi che abbiano sottoscritto un *executive agreement* con gli Stati Uniti, il *Cloud Act* pone anche un importante limite a tutela dei cittadini e residenti USA. Per accedere ai dati di questi ultimi, infatti, il *Cloud Act* richiede il necessario ricorso ai tradizionali meccanismi previsti dagli accordi di mutua assistenza legale, ove esistenti.

Particolarmente interessante è la previsione del *Cloud Act* che esclude espressamente che gli *executive agreement* possano richiedere agli operatori *cloud* di decifrare i dati conservati sulla propria infrastruttura[52]. Questa previsione, che si pone in netta antitesi rispetto al timore del *going dark* che pure era alla base della stessa adozione del *Cloud Act*, è al tempo stesso un atto necessario per non danneggiare gli interessi economici degli operatori USA, e una vistosissima falla nell'intero meccanismo predisposto dal governo statunitense[53]. Non è un caso che, nelle pagine dedicate a illustrare l'impatto della nuova legislazione sulle loro politiche interne di protezione dei dati, i grandi operatori *cloud* d'oltreoceano – oltre a mettere ben in evidenza il loro costante impegno nell'opporsi alle richieste delle autorità ogni volta che ne ricorrano le condizioni – promuovano attivamente la cifratura quale strumento indispensabile per impedire l'accesso ai dati dei loro clienti da parte di "qualunque" soggetto terzo[54]. Del resto, la stessa elaborazione del modello di *Data Trust* illustrato nella prima parte di questo contributo è resa possibile, dal punto di vista tecnico, dall'applicazione generalizzata di algoritmi di cifratura sicuri.

Volendo tentare un primo bilancio degli effetti del *Cloud Act* sulla regolazione del fenomeno del *cloud computing*, gli aspetti negativi sembrano superiori ai benefici che il legislatore USA si proponeva di conseguire[55].

In primo luogo, nell'adottare un approccio unilaterale al fenomeno del *cloud computing* per garantire l'accesso alle informazioni da parte del governo USA, il *Cloud Act* ha finito per rafforzare le spinte verso la localizzazione dei dati da parte di molti Stati, proprio quando uno dei fini perseguiti era dichiara-

tamente quello di evitare l'esacerbarsi dei conflitti legali, e della conseguente proliferazione di obblighi di localizzazione negli altri Paesi[56]. Anche gli operatori, dal canto loro, hanno in più occasioni mostrato di preferire un approccio "pragmatico" quando tratta di opporsi alle richieste delle pubbliche autorità nei Paesi nei quali offrono i loro servizi: in alcuni casi, hanno fatto leva sul principio di localizzazione per limitare l'accesso da parte delle autorità ai soli dati conservati sui *data center* del Paese richiedente. In altri casi, hanno mostrato di preferire il ricorso al criterio del controllo sui dati per opporsi a richieste provenienti da Paesi diversi dagli USA, nel quale erano domiciliati.

Inoltre, se è certamente vero che le procedure previste dagli accordi di mutua assistenza legale si sono dimostrate – proprio a causa della crescente diffusione di Internet, in generale, e dei servizi *cloud* in particolare – sempre più onerose in termini di tempo e risorse, è altrettanto vero che queste procedure erano state progettate segnatamente per offrire adeguate garanzie a tutela dei diritti e delle libertà fondamentali degli individui contro indebite intromissioni da parte dei pubblici poteri: «The rigorous procedures in the MLAT system are important safeguards for privacy and due process. When providing an alternative way, one would expect that the new regime would provide at least equivalent safeguards to those provided by the MLAT system. The CLOUD Act, however, removes some of the layers of protections provided by the MLAT system such as the rigorous reviews by [Department Of Justice], Attorney General, and courts without providing equivalent safeguards. Hence, bypassing the MLAT system could be faster for law enforcement, but it diminishes privacy standards. This is especially true for individuals in countries where there is no adequate privacy protection»[57].

In terzo luogo, nella sua pretesa di disciplinare con un unico tratto di penna un fenomeno così complesso e articolato, il *Cloud Act* omette completamente di regolare i rapporti tra i vari fornitori che compongono la "filiera" *cloud*. Come abbiamo evidenziato nella prima parte, una larghissima parte dei servizi *cloud* offerti sul mercato sono resi possibili dalla combinazione, verticale e orizzontale, di numerosi elementi infrastrutturali e applicativi messi a disposizione da una pluralità di operatori, ciascuno dei quali può avere un grado variabile di "possesso, custodia o controllo" sui dati[58]. In uno scenario di questo tipo, come scegliere il soggetto a cui inoltrare la richiesta di fornire i dati richiesti? Occorre privilegiare il livello infrastrutturale (dove i dati sono "fisicamente" conservati) o quello applicativo (tramite il quale sono generalmente acceduti)? Come vedremo nelle prossime pagine, il problema della definizione dei ruoli dei vari soggetti coinvolti nella fornitura di un servizio *cloud* all'utente finale non sono esclusive del *Cloud Act*, ma affliggono in maniera simile anche la normativa comunitaria.

8. L'accesso ai dati conservati sul *cloud*: la proposta di Regolamento *e-Evidence*

Nonostante tutti i suoi limiti, il *Cloud Act* ha contribuito a sollevare il velo su una questione di centrale importanza, ovvero il superamento del criterio dell'ubicazione fisica dei dati nel determinare la giurisdizione applicabile, in favore di un diverso principio, quello cioè del controllo sui dati. Al tempo stesso, ha mostrato tutti i limiti di un approccio unilaterale al fenomeno, che ha consentito agli operatori di sfruttare la babele di legislazioni nazionali (oltre che elementi di natura tecnica) per vanificare la pretesa di mantenere una qualche forma di controllo per finalità di interesse pubblico. Il problema rimane di estrema attualità anche nell'ambito dell'Unione europea, ed è alla base della recente proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[59].

Rispetto al *Cloud Act*, la proposta di regolamento mostra grande attenzione al problema delle garanzie, procedurali e sostanziali, a tutela dei diritti e delle libertà degli interessati, ma – allo stesso tempo e in modo analogo al *Cloud Act* – prende atto della portata dirompente dei modelli di distribuzione e gestione dei servizi e delle infrastrutture di *cloud computing* per dedurne l'inapplicabilità del criterio dell'ubicazione dei dati come base per affermare (o negare) la giurisdizione di uno Stato: «In molti casi i dati non sono più conservati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura *cloud* che consente in linea di massima l'accesso da qualsiasi luogo. I prestatori di servizi non hanno bisogno di essere stabiliti o avere server in ogni giurisdizione ma ricorrono piuttosto a un'amministrazione centralizzata e a sistemi decentrati per conservare i dati e fornire i servizi. In tal modo ottimizzano il bilanciamento del carico e riducono i tempi di risposta alle richieste di dati degli utenti. (...). Le imprese possono così fornire i contenuti dal server più vicino all'utente o in grado di inoltrare la comunicazione attraverso una rete meno congestionata»[60].

Per questo motivo, il Regolamento abbandona esplicitamente «il criterio di collegamento rappresen-

tato dall'ubicazione dei dati, *poiché generalmente la conservazione dei dati non comporta alcun controllo da parte dello Stato nel cui territorio i dati sono conservati. Nella maggior parte dei casi il luogo di conservazione è determinato dal prestatore di servizi sulla base di considerazioni commerciali.*»[61].

Il Regolamento si applica ai servizi *cloud* e agli altri servizi di *hosting* che forniscono «una vasta gamma di risorse informatiche, quali reti, server o altre infrastrutture, mezzi di conservazione, app e servizi che permettono di conservare dati a diversi scopi»[62]. L'elemento decisivo per determinare se un servizio rientri o meno nell'ambito di applicazione del Regolamento è dato dalla conservazione dei dati, che deve rappresentare un momento essenziale del contratto di servizio: «I servizi per i quali la conservazione di dati *non è una componente propria* non sono contemplati dalla proposta. Sebbene la maggior parte dei servizi forniti dai prestatori comprenda qualche tipo di conservazione dei dati, specialmente quando sono forniti online a distanza, è possibile distinguere servizi per i quali la conservazione dei dati *non è una caratteristica principale bensì un elemento puramente accessorio*, quali servizi giuridici, architettonici, ingegneristici e contabili *forniti* online a distanza».

È facile immaginare come il criterio del carattere "non accessorio" della custodia dei dati sarà uno dei punti dolenti della normativa in sede di applicazione: oggigiorno, la conservazione dei dati per conto del titolare, anche nell'ambito dell'erogazione di servizi di natura professionale (si pensi ad esempio ai tantissimi servizi *cloud* utilizzati da aziende e privati per la contabilità, la gestione del personale, incluse le buste paga, la sicurezza sul lavoro, ecc.) rappresenta un elemento così comune dall'essere dato quasi per scontato. Al tempo stesso, si potrebbe anche obiettare che, nella fornitura di servizi IaaS e PaaS, la conservazione dei dati non rappresenta l'elemento principale, poiché lo scopo è quello di mettere a disposizione dell'utente una serie di risorse di natura logica, che questi è libero di utilizzare come meglio crede.

Ciò detto, la proposta di regolamento prevede due nuovi strumenti per la produzione e la conservazione dei dati che si rendono necessari nell'ambito di indagini o procedimenti penali: rispettivamente, gli ordini europei di produzione e gli ordini europei di conservazione. Entrambi gli ordini possono essere utilizzati per chiedere di produrre o conservare dati di cui il fornitore del servizio, situato in un'altra giurisdizione rispetto a quella dove gli ordini sono emessi, abbia la disponibilità. Tali ordini possono essere notificati direttamente al prestatore del servizio, e "sono eseguiti allo stesso modo degli ordini nazionali comparabili nella giurisdizione in cui il prestatore di servizi riceve l'ordine". Perché tali ordini siano validi, sono tuttavia necessarie alcune condizioni. In primo luogo, devono essere emessi o convalidati da un'autorità giudiziaria di uno Stato membro, previa valutazione della proporzionalità e necessità nel singolo caso, nell'ambito di un procedimento penale[63]. In secondo luogo, i dati di cui si richiede la conservazione o la produzione devono essere "necessari come prova in indagini o procedimenti penali". Devono cioè riferirsi a specifici autori, noti o sconosciuti, di un reato che è già stato commesso. In particolare, l'ordine europeo di conservazione consente di chiedere la conservazione solo di dati che sono già nella disponibilità del fornitore al momento della ricezione dell'ordine, e non di accedere a dati in una fase successiva alla ricezione dell'ordine stesso. In terzo luogo, gli ordini di produzione e conservazione possono essere emessi "solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione".

Il tema è, ancora una volta, troppo complesso e articolato per essere approfondito in questa sede nei suoi vari profili. Dalla particolare prospettiva di questo contributo, però, si deve segnalare come non sia sfuggita alla più attenta dottrina come, nella proposta di Regolamento, il tema della cifratura dei dati rappresenti (ancora una volta) il punto dolente in grado di vanificare l'intero edificio normativo messo in piedi dalla Commissione[64]. Nel Considerando n. 19 si legge infatti che i dati devono essere forniti dal prestatore di servizi "a prescindere dal fatto che siano criptati o meno". Mentre il *Cloud Act* esonera espressamente il fornitore del servizio dal comunicare alle autorità le chiavi di cifratura, nel caso del Regolamento la questione è assai più incerta, e dipende in ultima analisi da chi abbia il controllo sulle chiavi stesse. Se, come accade nella gran parte dei casi, le chiavi sono detenute dal fornitore del servizio, manca nel testo un'esplicita previsione che obblighi il rappresentante del *service provider* a produrre obbligatoriamente le chiavi di cifratura assieme ai dati cifrati, o quantomeno a produrre il testo decifrato mediante le chiavi in suo possesso. Si tratta di una lacuna tutt'altro che secondaria, anche considerato che molto spesso le chiavi sono detenute da soggetti stabiliti in Paesi terzi che, pur facendo capo al *service provider*, non coincidono con la società che rappresenta il *provider* nel territorio dell'Unione[65].

Nel caso in cui, invece, il fornitore utilizzi un sistema di cifratura c.d. *end-to-end*, la cifratura e la decifratura dei messaggi avviene interamente sui dispositivi degli utenti finali, con la conseguente impossibilità per i fornitori di accedere al contenuto dei messaggi perché, semplicemente, non dispongono

delle relative chiavi. In questa ipotesi, l'acquisizione dei dati attraverso l'ordine europeo di produzione si rivelerebbe del tutto inutile. È stato quindi osservato che, qualora l'Unione europea «non trovi il modo di obbligare tutti i prestatori di servizi a consegnare i dati in chiaro per finalità di giustizia, indipendentemente dal sistema di criptazione utilizzato, i progressi investigativi nell'acquisizione transnazionale della prova elettronica non potranno che essere esigui e la sensazione potrebbe essere alla fine che la montagna avrà partorito un topolino»[66]. Tuttavia, se si considerano le caratteristiche "intrinseche" del *cloud computing* che abbiamo sin qui sommariamente evidenziato, è lecito dubitare che esista realmente una strada praticabile per raggiungere il risultato voluto. Del resto, il silenzio del Regolamento sul punto, che dedica alla cifratura solo uno scarso passaggio nel Considerando n. 19, dovrebbe essere emblematico proprio di tale difficoltà.

9. Riflessioni conclusive

Alla fine di questa lunga carrellata, peraltro non esaustiva, dei problemi che la regolazione del fenomeno *cloud* ha incontrato e incontra tutt'ora a livello nazionale e internazionale, si possono tentare alcune riflessioni.

Come abbiamo evidenziato più volte nel corso di questo contributo, molte delle difficoltà che si incontrano quando ci si appresta a regolare il fenomeno del *cloud computing* discendono dall'estrema eterogeneità dei servizi genericamente ricondotti sotto l'ombrello del *cloud*. Se è vero che questi servizi presentano alcuni tratti comuni (il carattere logico delle risorse utilizzate, la loro assegnazione in base alla domanda, la possibilità per l'utente di gestire tali risorse in autonomia tramite piattaforme eterogenee, ecc.), questi elementi non sempre offrono un "appiglio" sufficiente dal punto di vista della regolazione. Anche dal punto di vista dei modelli di servizio (IaaS, PaaS e SaaS, per limitarci alla classificazione tradizionale) e dei modelli di distribuzione (*cloud* pubblico, privato, comunitario e ibrido), le differenze sono tante e tali da rendere estremamente difficile ricostruire un quadro unitario. Se a tutto ciò si aggiungono anche le variazioni nei modelli di gestione dell'infrastruttura, e dei dati che su tali infrastrutture transitano o sono conservati (cha abbiamo riassunto, senza peraltro alcuna pretesa di completezza, nella tripartizione *Data Shard*, *Data Localization*, *Data Trust*), il quadro che ne emerge assomiglia più a un complicato mosaico, in cui soluzioni tecniche, organizzative e, non ultime, legali, si combinano in modi sempre diversi a seconda del contesto e delle esigenze.

Proprio perché il contesto è così complesso e – per certi versi – confuso, è necessario trovare alcuni punti fermi da cui partire per regolare un fenomeno che non può e non deve essere lasciato interamente alle scelte degli operatori *cloud*, poiché riguarda aspetti fondamentali della nascente "società dei dati".

Innanzitutto, occorre partire da un rilievo di natura concettuale. Secondo una concezione più tradizionale, i dati non sarebbero poi così diversi dagli altri beni intangibili, come il denaro, e che il *cloud* in fondo sia poco più del metallo e dei bulloni che ne compongono l'hardware: «Despite the technological wizardry of modern life, the 'cloud' is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries.»[67]

Ovviamente, non c'è alcuna *wizardry* nelle modalità di funzionamento del *cloud* e, più in generale, di Internet. Tuttavia, se è vero che alla fine qualunque tecnologia può essere ridotta a una massa di server, dischi, cavi e altri apparecchi fisici, è anche vero che le "pratiche" che tali oggetti abilitano (si pensi, oggi, alle possibilità offerte dalle *blockchain*, dall'*Internet of Things* e agli sviluppi dell'intelligenza artificiale, solo per fare degli esempi) impongono di adottare un atteggiamento non riduzionista, e non unilaterale, in grado di guardare ai fenomeni nella loro complessità. Lo stesso vale, a maggior ragione, per i dati che su queste infrastrutture transitano. Discutere se, dal punto di vista dell'applicazione di istituti e norme giuridiche, questi presentino analogie con il denaro o con altri beni intangibili rischia di tradursi, almeno ad avviso di chi scrive, in un mero esercizio di stile. Se non altro, perché sono proprio i beni intangibili come la moneta o il debito ad andare incontro a vere e proprie "mutazioni genetiche" a seguito dell'erompere di nuove tecnologie "abilitanti" (si pensi al crescente peso acquisito dalle criptovalute come Bitcoin), e non viceversa.

Ciò è particolarmente vero quando si discute degli obblighi di localizzazione dei dati all'interno dei confini nazionali. Che la loro previsione possa essere sufficiente, "di per sé", a soddisfare le spesso contrastanti esigenze pubbliche legate alla disponibilità dei dati (inclusa la possibilità di sottoporre a sequestro i server su cui i dati sono conservati) non tiene in debito conto né la natura composita e al tempo stesso fluida di Internet, né delle possibilità tecnologiche che possono rendere vana qualsiasi pretesa di accesso

ai dati per l'esercizio di pubblici poteri, né – e questo è forse la lezione più importante impartita dal *Cloud Act* – delle possibili "reazioni" a catena che tali previsioni possono innescare da parte dei vari soggetti coinvolti, sia pubblici che privati (lo dimostra in modo esemplare il modello di *Data Trust* elaborato da Microsoft come risposta al *Cloud Act*).

Entrambi gli obiettivi perseguiti dal *Cloud Act*, ovvero ridurre il proliferare di obblighi di localizzazione a livello internazionale mediante la conclusione di accordi bilaterali, e assicurare alle autorità federali la possibilità di poter continuare ad accedere ai dati necessari all'esercizio delle funzioni pubbliche, possono dirsi falliti. Al tempo stesso, però, proprio il *Cloud Act* ha mostrato i limiti del criterio basato sul possesso, custodia o controllo dei dati, mediante il quale si cerca di agire sui fornitori di servizi *cloud* affinché siano questi ad attivarsi per rendere disponibili i dati dei propri utenti conservati – o, il più delle volte, sparsi – sulla loro infrastruttura globale, a prescindere dalla loro ubicazione geografica. A non funzionare, in questo caso, è stato soprattutto l'approccio unilaterale al fenomeno (oltre che una generale sottovalutazione della complessità della filiera *cloud*), che ha consentito ai grandi operatori di fare quello che di solito tendono a fare in casi simili: sfruttare la frammentazione delle legislazioni nazionali a loro vantaggio, in questo caso specifico per "spogliarsi", nella forma e nella sostanza, di qualunque controllo sui dati.

Molto meglio allora partire dalla particolare combinazione di elementi giuridici, organizzativi e tecnici alla base del modello di "Data Trust" per affrontare seriamente il problema della "sovranità dei dati". Indipendentemente dalle questioni circa la riproducibilità e la scalabilità dell'esperimento tedesco, l'introduzione del principio di separazione della "gestione dell'infrastruttura" rispetto alle questioni legate all'accesso ai dati potrebbe rivelarsi, con gli opportuni adattamenti, una delle chiavi di lettura di un futuro assetto europeo della regolamentazione sul *cloud*. Questa distinzione, del resto, la si ritrova anche all'interno del progetto di *cloud* franco-tedesco, oggetto di analisi all'interno di questo stesso volume. Come è stato osservato, infatti, nella documentazione di GAIA-X "vengono utilizzati sia il termine *data sovereignty* che *digital sovereignty*. Mentre la sovranità digitale viene definita come il potere di decidere «about how digital processes, infrastructures and the movement of data are structured, built and managed», la *data sovereignty* viene presentata come un particolare aspetto della sovranità digitale, consistente nel pieno controllo del *data owner* rispetto alla collocazione e all'uso dei dati. La sovranità sui dati sarebbe dunque il primo passo per assicurare una sovranità digitale piena"[68].

Note

[1]Nel 2020 il mercato mondiale dei servizi *cloud* ha raggiunto i 371.4 miliardi di dollari. Anche per effetto della recente pandemia di COVID-19, si stima che nel 2025 il mercato ammonterà a 832 miliardi di dollari, con un tasso di crescita annuo del 17.5% (fonte: *Research and Markets*).

[2]Per una sistematica revisione delle misure di localizzazione adottate a livello mondiale si vedano A. Chander, U.P. Le, *Data Nationalism*, in "Emory Law Journal", 2015, n. 3, p. 677-739; Organisation for Economic Cooperation and Development, *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL.

[3]Sulle vicende legate alla piattaforma "Immuni" si veda V. Pagnanelli, *Immuni: spunti per una riflessione privacy-oriented*, in "Questione Giustizia", maggio 2020.

[4]A. Chander, U.P. Le, *op. cit.*, p. 679.

[5]Per una disamina degli effetti negativi delle misure di localizzazione sulla sicurezza e la concorrenza si vedano, fra i tanti, J. Selby, *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?*, in "International Journal of Law and Information Technology", 2017, n. 3, p. 213-232; H. Brehmer, *Data Localization: the unintended consequences of privacy litigation*, in "American University Law Review", 2018, n. 3, p. 927-969; R. Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and other Online Activities*, National Telecommunications and Information Administration, 2016; J. Lenhart, *Security for the 21st Century Economy: Borders Hold Less Meaning – and That's a Good Thing*, Information Technology Industry Council, 2017.

[6]Fonte: *Statista*. Dati riferiti ad aprile 2020.

[7]Sulla storia e l'evoluzione del *cloud computing* si vedano, tra i tanti, M.S. Gendron, *Business Intelligence and the Cloud*, John Wiley & Sons, 2014; V.V. Arutyunov, *Cloud Computing: Its History of Development, Modern State, and Future Considerations*, in "Scientific and Technical Information Processing", 2012, n. 3, p. 173-178.

[8]A. Regalado, *Who coined "Cloud computing"?*, in "MIT Technology Review", 31 ottobre 2011.

[9]NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, 9 December 2011, Special publication n. 800-144, p. IV. Definire il fenomeno in modo univoco è difficile per almeno due ragioni: «First, as there is no clear difference between the cloud and the Internet itself, any attempt to create a legal distinction among various online services will invariably lead to legal "overreach" with unintended consequences. Second, forcing such a distinction is likely to mislead the very consumers that the legislation is intended to protect because they might wrongly think that a particular rule, regulation, or practice will protect them so long as the services they are using are labeled as cloud services» (Cfr. P.S. Ryan, S. Falvey, R. Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, in "Computer", 2013, n. 12, p. 55.

[10]I limiti propri di qualunque definizione sono del resto stati messi in evidenza dallo stesso NIST: «Much of what has been written about cloud computing is definitional, aimed at identifying important paradigms of deployment and use, and providing a general taxonomy for conceptualizing important facets of service». Cfr. NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, cit., p. 3).

[11]«Cloud computing can be considered a new computing paradigm insofar as it allows the utilization of a computing

infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. Because of the implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention», *ibidem*.

[12]NIST, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, September 2011, Special publication n. 800-145.

[13]Per "scalabilità" si intende la capacità di un sistema di aumentare o diminuire le proprie prestazioni (e dunque il carico di lavoro che è in grado di svolgere nella stessa unità di tempo) in funzione della necessità e della disponibilità. La scalabilità si distingue in "orizzontale" e "verticale". La prima è la capacità di aumentare la capacità di lavoro sfruttando più componenti hardware o software in modo che funzionino come una singola unità logica (in pratica, il lavoro viene suddiviso tra più sistemi, ciascuno dei quali in grado di operare autonomamente). La scalabilità verticale, invece, aumenta la capacità aggiungendo più risorse a una stessa unità (ad esempio, aggiungendo nuova memoria o dischi più capienti, aumentando il numero di processori, ecc.). Mentre prima della diffusione del *cloud* la scalabilità poteva essere ottenuta solo comprando o noleggiando ulteriori componenti hardware e software, e dunque solo a seguito di un'attenta pianificazione e a fronte di notevoli investimenti, i servizi *cloud* possono essere scalati "elasticamente", ossia in base all'andamento (in tempo reale) del carico di lavoro. Il che significa anche che, una volta che il carico diminuisce, è possibile ridurre l'erogazione delle risorse in eccesso e, cosa assai rilevante, smettere di pagare per ciò che non si usa.

[14]Per chiarire meglio l'impatto dei modelli di *cloud computing*, si può immaginare il caso di un'azienda che decida di vendere i propri prodotti sul web. Prima dell'avvento dei servizi *cloud*, per realizzare e ospitare sulla propria infrastruttura un sito di *e-commerce* avrebbe dovuto preoccuparsi di tutta la "filiera" tecnologica: l'acquisto, l'installazione e la configurazione di server, *firewall*, *load balancer* e apparati di rete, nonché della predisposizione di adeguate misure di sicurezza fisica (sale adeguate, impianti di condizionamento, sistemi antincendio, ecc.) e logica (DMZ, sistemi di autenticazione, monitoraggio del traffico di rete, ecc.), la configurazione degli ambienti di produzione e di test, l'acquisto delle licenze software necessarie, e tantissimi altri aspetti. Nel decidere il tipo di hardware da acquistare (numero di processori, memoria, spazio disco, ecc.), l'azienda avrebbe dovuto stimare accuratamente non il carico di lavoro "medio", ma quello massimo ipotizzabile. Il carico di lavoro di un servizio web, infatti, non è mai costante: periodi di bassa e moderata attività (ad esempio durante le ore notturne) si alternano a picchi di lavoro più o meno intensi che possono mettere a dura prova le risorse disponibili (si pensi, per esempio, al periodo natalizio o ai sempre più frequenti saldi promossi online). Se queste risorse non sono sufficienti per far fronte alle richieste in un certo momento, una parte di queste richieste non potrà essere servita, causando disservizi e malumori agli utenti, o addirittura malfunzionamenti del sistema. Al tempo stesso, durante i periodi di inattività o di "scarico", tutte le risorse in eccesso, acquistate solo per poter far fronte ai momenti di picco, sono destinate a rimanere inutilizzate, nonostante siano state investite somme ingenti per acquistarle. È vero che un'azienda avrebbe potuto noleggiare tutto il necessario, anziché acquistarlo in proprio, ma anche in questo caso la "rigidità" del sistema rimarrebbe sostanzialmente inalterata e i costi largamente fissi. Grazie al *cloud*, invece, l'azienda può concentrarsi su ciò che le interessa davvero, ossia vendere i propri prodotti sul web, senza doversi preoccupare di acquistare (o noleggiare) e configurare le risorse necessarie. Queste possono essere create, aggiunte o ridimensionate in tempo reale, per seguire l'andamento del carico di lavoro e, una volta che non sono più necessarie, possono essere dismesse in tutta facilità, smettendo così di pagare per ciò che non viene utilizzato.

[15]Il confine tra IaaS e PaaS, relativamente netto in teoria, nella pratica è andato sempre più sfumando, sia perché i primi offrono oggi funzionalità di alto livello, come ad esempio macchine virtuali già preconfigurate per poter svolgere un numero sempre crescente di compiti; sia perché i servizi PaaS tendono a permettere all'utente che lo desideri un controllo più granulare sulle caratteristiche della sottostante infrastruttura virtuale.

[16]Per una "carrellata" sui diversi modelli di servizio si rinvia a A. Biasiotti, *Il nuovo regolamento europeo sulla protezione dei dati*, EPC Editore, 2018, p. 723 ss.

[17]Questa affermazione deve essere presa con le dovute cautele, poiché sempre più spesso anche i servizi infrastrutturali e/o di piattaforma prevedono (si potrebbe dire "per impostazione predefinita") forme di cifratura dei dati, in transito o "a riposo", che permettono di assicurare già in partenza un livello di sicurezza piuttosto elevato, salva la possibilità per l'utente di applicare misure ulteriori per soddisfare requisiti di sicurezza più stringenti.

[18]In informatica, l'aggettivo "trasparente" ha un significato diverso dal linguaggio comune, indicando un processo che si svolge senza che l'utente ne sia consapevole e senza che a quest'ultimo sia richiesto alcun tipo di intervento. Ad esempio, una modifica che attiene al modo con cui un software salva e organizza i dati è "trasparente" rispetto all'utente finale se, dal punto di vista di quest'ultimo, il software continua a operare come prima, senza che vi siano cambiamenti nell'interfaccia utente o nei flussi di lavoro, che rimangono quelli soliti ai quali l'utente è abituato.

[19]Nel 2017 Dropbox ha avviato la migrazione di gran parte dei suoi sistemi dall'infrastruttura di AWS sui propri *data center*.

[20]Fonte: *Mordor Intelligence*.

[21]V.V. Arutyunov, *op. cit.*

[22]In merito alla strategia italiana per l'adozione dei servizi *cloud* nell'ambito delle Pubbliche Amministrazioni si veda V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in questo fascicolo.

[23]P.M. Schwartz, *Legal Access to the Global Cloud*, in "Columbia Law Review", 2018, n. 6, p. 1681-1762.

[24]Esistono almeno tre diverse strategie di partizionamento dei dati. Nel partizionamento "orizzontale" (quello chiamato propriamente *sharding*), ogni partizione ha lo stesso schema di tutte le altre, ossia contiene le stesse tipologie di dati (ad esempio, gli ordini dei clienti). Nel partizionamento "verticale", invece, ogni partizione contiene un particolare sottoinsieme dei dati archiviati, suddivisi in base al loro modello di utilizzo. In questo modo, i dati utilizzati più spesso possono essere collocati in una partizione verticale, mentre quelli usati raramente possono essere collocati in un'altra partizione. Infine, nel partizionamento "funzionale", dati sono aggregati in base alla loro modalità di utilizzo: in un sistema di *e-commerce*, ad esempio, i dati delle fatture potrebbero essere archiviati in una partizione dedicata all'area amministrativa, e quelli relativi all'inventario dei prodotti in magazzino in un'altra partizione, pronti per essere utilizzati dalla logistica e dalle vendite.

[25]In un server, la quantità di spazio di archiviazione su disco è in genere limitata, ma è possibile sostituire i dischi esistenti con versioni più capienti o aggiungere altri dischi man mano che i volumi di dati aumentano. Tuttavia, il sistema finirà prima o poi per raggiungere un limite oltre al quale non è più possibile aumentare la capacità di archiviazione, se non a costi proibitivi. Allo stesso modo, un singolo server che ospita

tutti i dati potrebbe non essere in grado di fornire la potenza di calcolo necessaria per servire le interrogazioni (*query*) degli utenti, con conseguente aumento dei tempi di risposta e frequenti errori dovuti all'indisponibilità delle risorse. Anche in questo caso potrebbe essere possibile aggiungere ulteriore capacità computazionale e/o memoria, ma il sistema raggiungerà comunque un limite quando non sarà possibile aumentare ulteriormente le risorse di calcolo. Infine, c'è da considerare la larghezza di banda della rete. Anche in questo caso, infatti, un elevato numero di richieste aventi ad oggetto grandi quantità di dati possono generare un traffico di rete superiore alla capacità della rete usata per la connessione al server, con conseguente aumento dei tempi di risposta ed errori.

[26] P.M. Schwartz, *op. cit.*, p. 1965.

[27] Per maggiori informazioni sulla complessiva infrastruttura di Amazon Web Services, si veda "Regioni e zone di disponibilità". Anche l'infrastruttura *cloud* di Microsoft Azure prevede un'articolazione simile; per maggiori informazioni si veda "Azure geographies".

[28] Timori peraltro non infondati, se solo si pensa al caso "Snowden" e all'acuirsi delle tensioni tra l'Unione europea e gli Stati Uniti. Per un approfondimento delle vicende si rinvia a E.J. Snowden, *Errore di sistema*, Longanesi, 2019.

[29] Riconosciuto nel nostro ordinamento grazie alla l. 16 ottobre 1989, n. 364, con cui è stata ratificata la Convenzione dell'Aja sulla legge applicabile ai *trusts* e sul loro riconoscimento, adottata da L'Aja il 1° luglio 1985.

[30] *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. 2016), 14 July 2016.

[31] Oltre al contenuto delle e-mail riconducibili a un determinato *account* di posta elettronica, l'ordine includeva anche la produzione di ulteriori informazioni collegate a detto *account*, conservate sui server della sede americana. Queste informazioni sono sostanzialmente di tre tipi: «First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database». *Ivi*, p. 9.

[32] Tale scelta dipendeva peraltro da esigenze di natura tecnica (*in primis* diminuire il tempo di latenza portando i dati più vicino al luogo di accesso), non quello di soddisfare particolari esigenze di localizzazione.

[33] *Microsoft Corp. v. United States*, cit., p. 20.

[34] *Ivi*, p. 7.

[35] D. Callaway, L. Determan, *The New US Cloud Act. History, Rules, and Effects*, in "The Computer & Internet Lawyer", 2018, n. 8.

[36] A riprova del carattere "eccezionale" del caso *Microsoft Ireland* si vedano anche i casi *Yahoo Winsconsin*, *Yahoo Florida* e *Google California*, tutti successivi al primo, nei quali viene riaffermato il principio per cui le disposizioni dello SCA trovano applicazione a prescindere dal luogo in cui sono ubicati i dati.

[37] P.M. Schwartz, *op. cit.*, p. 1685 ss.

[38] *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (2017).

[39] *Ivi*, p. 25-26.

[40] *Ibidem*.

[41] In argomento si vedano le considerazioni di D. Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE, May 22, 2017.

[42] *Ibidem*.

[43] P.M. Schwartz, *op. cit.*, p. 1681-1762.

[44] Oggi circa l'85% delle indagini di polizia si basa su elementi di prova digitali, e in due terzi di questi casi vi è la necessità di richiedere tali elementi a fornitori di servizi *cloud* localizzati in altre giurisdizioni. Il numero di richieste verso i principali operatori è cresciuto dell'84% in soli cinque anni (2013-2018). Dati della Commissione europea.

[45] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, April 2019.

[46] *Ibidem*.

[47] Per approfondimenti sul *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* si vedano, tra i tanti, J. Galbraith, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, in "American Journal of International Law", 2018, n. 3, p. 487-493; D. Callaway, L. Determan, *op. cit.*

[48] Si veda in particolare l'art. 18 della Convenzione, in base al quale «Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control (...)».

[49] Perché possa essere concluso un *executive agreement* con un Paese terzo, il *Cloud Act* prevede che l'*Attorney General*, assieme al Segretario di Stato, verifichino e certifichino in forma scritta al Congresso USA che la legislazione del Paese terzo offra «robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement».

[50] Sino ad oggi, l'unico accordo sottoscritto dal governo USA è quello con la Gran Bretagna. Nel testo viene chiarito che, per *serious crime* si intende, ai sensi dell'art. 1, n. 14, dell'accordo, qualunque reato che preveda come massimo edittale almeno tre anni di reclusione («Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years»). Cfr. l'*executive agreement*.

[51] Ai sensi dell'articolo 2713 dello SCA (come emendato dal *Cloud Act*) gli elementi che devono essere tenuti in considerazione dalla corte nel decidere sulla richiesta di *quash* sono i seguenti: «a) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure; b) the interests of the qualifying foreign government in preventing any prohibited disclosure; c) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; d) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; e) the nature and extent of the provider's ties to and presence in the United States; f) the importance to the investigation of the information required to be disclosed; g) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and h) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance».

[52] 18 U.S. Code § 2523 (b) (3): «the terms of the agreement shall not create any obligation that providers be capable of

decrypting data or limitation that prevents providers from decrypting data».

[53]Falla da cui, come si vedrà più avanti, non è esente neppure la proposta di Regolamento europeo relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*). Il tema della crittografia, in particolare quella c.d. *end-to-end* (nel quale solo gli utenti che stanno comunicando sono in grado di leggere i messaggi, ad esclusione di qualsiasi altro soggetto, incluso il fornitore del servizio) è tornata di recente sotto i riflettori a seguito della presentazione di due proposte di legge, al momento entrambe all'esame del Senato USA. La prima proposta, denominata *Lawful Access to Encrypted Data Act* (o *LEAD Act*), mira a obbligare i fornitori di dispositivi e di servizi internet a decifrare i dati e a metterli a disposizione delle autorità in forma intellegibile. In questo senso, la proposta «is an actual, overt, make-no-mistake, crystal-clear ban on providers from offering end-to-end encryption in online services, from offering encrypted devices that cannot be unlocked for law enforcement, and indeed from offering any encryption that does not build in a means of decrypting data for law enforcement» (R. Pfefferkorn, *There is now an even worse anti-encryption bill than EARN IT. That doesn't make the EARN IT bill ok*, in The Center for Internet and Society, Stanford Law School, 24 giugno 2020). La seconda proposta di legge, l'*Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (il c.d. *EARN IT Act*) pone una serie di ostacoli, per lo più indiretti, al ricorso alle tecniche di crittografia per proteggere i contenuti.

[54]Si consideri, a titolo di esempio, quanto riportato nella documentazione ufficiale di Amazon Web Services: «In the event we cannot resolve a dispute, we do not hesitate to go to court. Amazon has a history of formally challenging government requests for customer information that we believe are overbroad or otherwise inappropriate. We will continue to resist requests, including those that conflict with local law such as GDPR in the European Union, to do everything we can to protect customer data. We will also continue to notify customers before disclosing content, and we provide advanced encryption and key management services that customers can use to protect their content further. We have industry leading encryption services that give our customers a range of options to encrypt data in-transit and at rest, and to manage encryption/decryption keys – because encrypted content is rendered useless without the applicable decryption keys».

[55] Per una disamina approfondita del Cloud Act si vedano, tra i tanti, P.M. Schwartz, *op. cit.*, p. 1748 ss.; D. Callaway, L. Determan, *op. cit.*

[56]Si veda la lettera inviata da Peter J. Kadzik, *Assistant Attorney General* presso il Dipartimento di Giustizia USA, al presidente del Senato Joseph R. Biden (luglio 2016): «The current situation is unsustainable. Some countries have begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees. If foreign governments cannot access data, they need for legitimate law enforcement, including terrorism investigations, they may also enact laws requiring companies to store data in their territory. Such data localization requirements would only exacerbate conflicts of law, make Internet enabled communications services less efficient, threaten important commercial interests, undermine privacy protections by requiring data storage in jurisdictions with laws less protective than ours, and ultimately impede U.S.-government access to data for its investigations. And as the global market for Internet related services expands, the U.S. government will increasingly need effective and efficient access to electronic information stored or uniquely accessible abroad. Conflicts of law may increasingly pose an obstacle to such access».

[57]H.H. Abraha, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, in "International Data Privacy Law", 2019, n. 3, p. 213. Proprio per ovviare alle evidenti inefficienze dell'attuale sistema basato sull'accordo di mutua assistenza legale del 2001 tra Stati Uniti e Unione europea, rafforzando al contempo gli standard di protezione dei diritti degli interessati, il Comitato europeo per la protezione dei dati personali ha sottolineato l'urgenza di ridisegnare l'intero processo per dar vita a una "nuova generazione" di accordi: «The Mutual Legal Assistance Treaty already in force between the EU and the US, as a legal instrument mainly aimed at facilitating judicial cooperation, contains only very limited provisions relevant from a data protection point of view. The EDPB and EDPS therefore wish to emphasize the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation. In addition, the "dual criminality principle" providing safeguard against discrepancy between how a crime is defined under the foreign law and how the same crime is legally defined under EU law should be preserved» (EDPB, *LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, 10 luglio 2019).

[58]H.H. Abraha, *op. cit.*, p. 208: «In the cloud computing environment, 'the delivery of cloud services often depends on complex, multi-layered arrangements between various providers.' This means that different providers can be involved in a particular cloud service offering with different degrees of control over the underlying technologies and stored data. This complicates the task of law enforcement agencies in identifying who is in 'possession, custody, or control' of personal data in view of serving a subsequent order. The consequence is that the CLOUD Act may target service providers (such as Infrastructure Service providers) who do not have effective 'possession, custody, or control' over the sought-after data. In this regard, one would argue that the CLOUD Act is not compatible with some business and technological realities of cloud computing».

[59]Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, 2018/0108.

[60]*Ibidem*. Si osserva inoltre che «Dato che internet non conosce frontiere, tali servizi possono essere prestati da qualsiasi luogo del mondo e non richiedono necessariamente un'infrastruttura fisica né la presenza di un'azienda o di personale negli Stati membri in cui sono offerti o nel mercato interno nel suo insieme. Non richiedono nemmeno un luogo specifico in cui conservare i dati: spesso il prestatore di servizi sceglie tale luogo in base a considerazioni legittime quali la sicurezza dei dati, le economie di scala e la rapidità di accesso. Di conseguenza, in un numero crescente di procedimenti penali riguardanti qualsiasi tipo di reato, le autorità degli Stati membri richiedono l'accesso ai dati che potrebbero servire da prove e che sono conservati al di fuori del loro paese e/o da prestatori di servizi situati in altri Stati membri o in paesi terzi».

[61]*Ibidem*, nostro il corsivo.

[62]Il Regolamento si applica anche «ai mercati digitali che consentono ai consumatori e/o alle imprese di concludere operazioni tramite contratti di vendita o di servizi online. Tali operazioni sono effettuate o sul sito web del mercato online o sul sito web di un professionista che utilizza i servizi infor-

matici forniti dal mercato online. È pertanto questo mercato che generalmente detiene prove elettroniche che possono essere necessarie nel corso di procedimenti penali».

[63]Si intende dalla fase preprocessuale delle indagini preliminari fino alla chiusura del procedimento con sentenza o altra decisione. Il regolamento opera anche una distinzione tra (meta) dati relativi agli accessi e quelli relativi al contenuto dei dati stessi: «gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi per qualsiasi reato, mentre quelli per la produzione di dati relativi alle operazioni o al contenuto possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati precisati nella proposta e se vi è un collegamento specifico con gli strumenti elettronici e i reati rientranti nel campo di applicazione della direttiva (UE) 2017/541 sulla lotta contro il terrorismo».

[64]Sul punto si rinvia all'approfondita analisi e alle acute osservazioni di R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa della Commissione europea al vaglio del Consiglio dell'Unione*, in "Diritto Penale Contemporaneo", 2019, n. 1, p. 71 ss., da cui sono tratte le considerazioni che seguono.

[65]Sul punto cfr. R. Pezzuto, *op. cit.*, in part. pp. 73-74.

[66]*Ibidem*, p. 74.

[67]A.K. Woods, *Against Data Exceptionalism*, in "Stanford Law Review", 2016, n. 4, p. 729.

[68]V. Pagnanelli, *op. cit.*

* * *

Cloud computing: technical models and legal frameworks

Abstract: The cloud computing market has experienced an exponential growth rate in recent years, which the recent global pandemic emergency will eventually strengthen further. The success of this complex and varied "ecosystem" of technologies and services lies in a synergistic combination of factors, as well as the increasingly widespread diffusion of smartphones and tablets, which has led to new ways of using IT services. Cloud platforms today perform an enabling function with respect to a practically infinite variety of services, which could not exist without the resources made available by cloud computing providers. From a legal point of view, however, cloud computing leaves enormous questions still largely unresolved. How to protect the rights of data subjects when their data can be moved, unpacked, recomposed and replicated in any node of the global network with a simple click? How to regulate such kaleidoscope of different services and how to share obligations and responsibilities among the various subjects that make up the cloud supply chain? In many respects, the approach followed by the United States and the European Union could not be more different, but both pretend to unilaterally regulate a phenomenon - cloud computing and, more generally speaking, the Internet - in which "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Keywords: Cloud computing – Cloud Act – e-Evidence Regulation

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0021

La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa

Stefano Torregiani*

L'incremento esponenziale della circolazione dei dati dovuto all'avvento della digitalizzazione è stato accompagnato da un altrettanto rilevante aumento degli obblighi di localizzazione delle informazioni imposti dagli Stati membri dell'Unione europea. Il legislatore continentale, conscio dell'importanza che il libero flusso delle informazioni ricopre per la realizzazione del mercato unico digitale, ha reagito all'espansione dalla *data localization* attraverso una serie di interventi particolari e distinti, prevalentemente fondati sulla distinzione, non ancora del tutto pacifica, tra dati personali e dati non personali. Attraverso l'analisi delle similitudini e delle differenze che caratterizzano le principali fonti dell'ordinamento europeo in materia di dati, lo scopo del presente lavoro sarà quello di valutare se questo mosaico regolamentare, preferito ad un approccio onnicomprensivo, sia idoneo a disciplinare efficacemente lo spazio comune europeo dei dati.

Circolazione dei dati – Obblighi di localizzazione – Dato personale – Dato non personale

Sommario: *1. Introduzione – 2. La reazione europea alla* data localization *– 3. La circolazione dei dati personali – 3.1. All'interno dell'Unione europea – 3.2. Al di fuori dell'Unione europea – 4. La circolazione dei dati non personali – 4.1. Il divieto degli obblighi di localizzazione – 4.2. Una nuova portabilità autoregolamentata – 5. I punti deboli dell'impianto regolamentare europeo – 6. La necessità di una visione onnicomprensiva per la realtà digitale moderna*

1. Introduzione

Il fenomeno della data driven innovation è diventato l'indiscusso protagonista dell'attuale realtà economica e sociale nel giro di pochissimi anni, trasformandosi nel punto di riferimento per qualsiasi modello di sviluppo economico e tecnologico. Attualmente, il vero potere si trova nelle mani di chi, tramite la gestione di una vastissima mole di dati, riesce ad estrarre valore e, conseguentemente, prendere decisioni economicamente molto vantaggiose, a fronte di costi assai ridotti[1].

Questo è il principale motivo alla base della repentina acquisizione di rilevanza da parte del bene "dato", il quale oggi si presenta come una risorsa economico-finanziaria di cui nessuna attività, né pubblica, né privata, può più fare a meno[2].

Uno degli aspetti più importanti concernenti l'innovazione digitale è quello relativo alla circolazione di queste informazioni: l'addestramento degli algoritmi, le analisi di mercato, l'elaborazione di strategie pubbliche, l'adozione di piani aziendali sono tutte attività che hanno come denominatore comune la stretta correlazione con il trattamento di una serie di dati che provengono da fonti diverse e, nella maggior parte dei casi, da Paesi diversi. In tal senso, dunque, la tematica del flusso di dati gioca un ruolo chiave in una realtà economico-giuridica che si contraddistingue per la sua globalità e per la rilevante presenza di catene di valore transfrontaliere[3].

Tuttavia, parallelamente alla diffusione dei dati ed alla loro circolazione, l'ultima decade ha registrato la proliferazione del suo antagonista, gli obblighi di localizzazione (fenomeno internazionalmente co-

*S. Torregiani è dottorando di ricerca in Scienze giuridiche presso l'Università degli Studi di Macerata nel curriculum Istituzioni e territorio nella dimensione nazionale, europea e internazionale.

nosciuto con il nome di *data localization*)[4]. Il loro numero è cresciuto di pari passo all'aumento dell'importanza dei dati per la società, giacché anche il dato risponde all'antica logica secondo cui più un bene ha valore, più è incline al rischio di offesa e, di conseguenza, richiede una maggiore tutela. Difatti, le principali ragioni che sono alla base dell'introduzione di misure legislative o amministrative da parte degli Stati a difesa del proprio patrimonio informativo riguardano la sicurezza interna, la facilità di accesso delle autorità nazionali alle informazioni necessarie alla vigilanza e lo sviluppo industriale domestico[5].

L'obiettivo del presente contributo è quello di valutare come le due tematiche interconnesse, ma contrapposte, della libera circolazione e della *data localization* siano state affrontate dal legislatore europeo tramite gli ultimi interventi in materia di *data law*. Come si avrà modo di vedere nel prosieguo, anziché affrontare il problema proponendo una soluzione unica ed onnicomprensiva, l'Unione europea ha preferito prima effettuare una distinzione di fondo tra dato personale e dato non personale per poi procedere all'adozione di due normative distinte che, malgrado comunicanti, rischiano di scostarsi troppo da una realtà digitale in cui tale distinzione è molto meno chiara di quanto la normativa lasci presupporre[6].

2. La reazione europea alla *data localization*

Di regola, con il termine *data localization* non ci si riferisce solo ed esclusivamente a quelle misure che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento, poiché vengono ricomprese anche quelle disposizioni che fissano vincoli più o meno stringenti al trasferimento dei dati al di là dei confini nazionali[7]. Questa circostanza allarga enormemente il novero delle misure che possono rientrare nella definizione, coprendo sostanzialmente tutti gli ordinamenti che hanno una disciplina in materia di circolazione dei dati, in quanto, quando non impongono un divieto generale oppure permettono il trasferimento solo dopo un primo trattamento a livello locale[8], si premurano comunque di prescrivere una serie di condizioni affinché i dati possano abbandonare il territorio di provenienza.

Alla luce di queste considerazioni, le restrizioni alla libera circolazione possono distinguersi in "rigide" o "condizionali"[9]. Le prime, le quali obbligano il titolare ad eseguire una determinata fase del trattamento localmente, si suddividono a loro volta in sottocategorie, a seconda della rigidità della misura: partendo da una disposizione che richiede il solo storage a livello locale – ossia mantenere una copia interna – e passando per quelle che, oltre all'archiviazione, impongono il processing domestico, si arriva fino al divieto generale di trasferimento, con la conseguenza che, al di fuori dei propri confini, è vietato persino il semplice accesso alle informazioni[10]. Le restrizioni condizionali, invece, lasciano sempre uno spazio, più o meno angusto, al trasferimento, ma lo rendono più gravoso giacché alcuni requisiti devono essere soddisfatti dal soggetto trasferente o dal ricevente, oppure da entrambi[11]. Tale distinzione si riflette anche sul bersaglio delle restrizioni: mentre quelle condizionali sono concepite al fine di limitare i trasferimenti di un determinato tipo di dato – generalmente personale –, quelle rigide hanno una dimensione prettamente settoriale, con la conseguenza che la distinzione tra dato personale e non personale non acquisisce alcuna rilevanza[12].

A dispetto dell'incremento massivo, la dottrina è sostanzialmente concorde nel valutare come negativi gli effetti prodotti dalla *data localization* nei confronti delle economie statali, giacché gli obiettivi di sicurezza, controllo e privacy che sono alla base dell'introduzione di simili misure restrittive potrebbero essere raggiunti tramite strade alternative capaci di apportare incalcolabili benefici al settore produttivo domestico[13]. Lo stesso discorso vale per un'organizzazione internazionale quale l'Unione europea che, dal canto suo, non è stata risparmiata da questa ondata di protezionismo che ha reso la *data localization* il principale attore non protagonista delle normative concernenti la gestione dei dati. Invero, più di uno studio sulle legislazioni vigenti nei singoli Stati membri dell'Unione ha dimostrato che, anche nel nostro continente, l'aumento del valore dell'informazione è stato accompagnato da un clima di sfiducia nelle normative e, soprattutto, nei sistemi di sicurezza degli altri Paesi membri, sfociando in poco tempo nell'emanazione di una serie di obblighi giuridici atti ad internalizzare il trattamento nella misura più ampia possibile[14].

Resosi conto di questa preoccupante tendenza, con l'inizio della seconda decade di questo secolo, il legislatore europeo ha deciso di prendere una posizione netta al riguardo, invertendo la rotta nel tentativo di ristabilire un clima di fiducia reciproca in tutto il continente. Con queste premesse nasce la strategia per la creazione del "Mercato Unico Digitale", concepito nelle intenzioni delle istituzioni europee come un passo imprescindibile affinché il mercato interno possa continuare a funzionare nell'era della digitalizzazione[15]. Oggi è, difatti, impossibile condurre un'attività economica con caratteri transfrontalieri senza far fronte a tutte le questioni connesse al tema

del trasferimento delle informazioni: i dati devono necessariamente muoversi assieme al bene al quale ineriscono, pertanto, in un mercato in cui gli ostacoli allo spostamento di persone, merci, capitali e servizi sono stati abbattuti, è chiaro che l'incentivo alla libera circolazione delle informazioni si manifesta come un passaggio irrinunciabile[16].

Tra l'altro, riuscire nell'intento di trasformare simili iniziative in disposizioni normative efficaci ed innovative rappresenta uno dei pochi ambiti in cui il vecchio continente può ancora imporsi quale capofila: se l'arretratezza tecnologica nei confronti dei giganti del tech che hanno le loro sedi nel Nord America e nell'Asia orientale non sembra potersi recuperare nel breve termine[17], agire per rendere il mercato continentale più appetibile rimane un dovere dell'Unione europea[18]. Segnatamente, i primi passi mossi dagli organismi dell'Unione verso la soppressione delle barriere virtuali alla libera circolazione, in favore di un incremento nell'utilizzo transfrontaliero delle informazioni, risalgono al 2011, quando la Commissione europea riconosce che le precedenti normative in materia di armonizzazione e di incentivo all'apertura nell'utilizzo dei dati nel settore pubblico – in particolare la Direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico – non hanno sortito gli effetti sperati e che, di fatto, le barriere allo scambio di informazioni pubbliche costituiscono ancora un peso per l'economia continentale[19]. Tuttavia, dati i tempi non ancora maturi per una discussione profonda come quella odierna, soprattutto per quanto riguarda la distinzione tra dato personale e non personale[20], il documento circoscrive i suoi riferimenti ai dati pubblici, salvo qualche sporadico accenno alla tutela della vita privata ed alla protezione dei dati personali[21].

Dopo un'ulteriore comunicazione del luglio 2014 in cui viene evidenziato il problema degli ostacoli alla libera circolazione dei dati ed il loro effetto frenante nei confronti dello sviluppo del *cloud computing* e dello sfruttamento dei big data[22], i documenti istituzionali del biennio 2017-2018 si focalizzano quasi esclusivamente sugli sforzi necessari alla creazione del mercato unico digitale. Secondo la visione europea, lo sviluppo di tutte le tecnologie basate sullo scambio di informazioni – dal *cloud computing*, all'*Internet of Things*, dalla *data analysis*, all'intelligenza artificiale – sono in grado di crescere e prosperare all'interno dell'economia continentale grazie a due pilastri fondamentali. Da un lato, la protezione dei dati personali, la quale, una volta aggiornata e consolidatasi nell'ordinamento europeo a tutti i livelli[23], promette di mantenere l'essere umano come centro gravitazionale attorno al quale si sviluppa la tecnologia, e non viceversa. Dall'altro lato, invece, si trova la libera circolazione dei dati, sia personali che non, la quale, accompagnata da una (non ancora del tutto) aggiornata disciplina riguardante l'interoperabilità e l'accesso alle informazioni, costituirà un incentivo senza eguali al progresso dell'economia europea.

Tuttavia, ciò che distingue l'ordinamento europeo dai regimi giuridici dei Paesi tecnologicamente più avanzati, è proprio la preponderanza che il primo dei due pilastri, la protezione dei dati personali, assume nei confronti della libera circolazione delle informazioni. Prendendo come termine di paragone due fra i Paesi leader dell'attuale panorama mondiale, negli Stati Uniti la regolamentazione riguardante le informazioni relative alle persone fisiche viene ancora percepita in un'ottica perlopiù consumeristica, con la conseguenza che l'individuo riesce ad ottenere protezione proprio in quanto consumatore, ma non in quanto persona che gode di un diritto fondamentale alla protezione dei propri dati[24]. Una impostazione altrettanto differente è invece quella riguardante la Repubblica popolare cinese, dove, in un certo senso, traspare una duplice concezione: se, per un verso, l'ordinamento cinese sembra si stia avvicinando a quello europeo nell'ambito delle relazioni fra privati, per altro verso, il precedente approccio centralizzato continua a caratterizzare la disciplina nei rapporti verticali fra individuo e governo, secondo un sistema autoritario e gerarchico che pone al vertice la sicurezza dello Stato[25].

Nell'ordinamento europeo, invece, il ruolo cardine attribuito alla persona fisica ed ai suoi diritti fondamentali rappresenta il principale motivo per cui l'impianto normativo dedicato alle altre dimensioni del *data law*, soprattutto, quella economica, si sia sviluppato in un secondo momento o, quantomeno, sia stato ipotizzato come sussidiario. Infatti, è dopo l'approvazione del Regolamento generale sulla protezione dei dati personali (GDPR)[26], precisamente nella Comunicazione sulla costruzione di un'economia dei dati europea del 2017, che è stata concepita l'idea di un regolamento specificamente dedicato ai dati a carattere non personale[27]. Effettivamente, dal testo emerge la ormai raggiunta consapevolezza che per lo sviluppo di un'economia sana e stabile non è sufficiente la sola tutela dell'individuo, poiché si rivela fondamentale anche mettere le imprese e le pubbliche amministrazioni in una posizione che dia loro la possibilità di essere promotrici di un nuovo modello economico-sociale[28]. Pertanto, la Commissione sottolinea quanto sia importante un approccio organico alla materia e chiarisce espressamente che il principio della libera circolazione dei dati all'interno dell'Unione, inteso quale corollario imprescindibi-

le delle altre libertà riconosciute nel mercato unico europeo, non riguarda solo i dati personali – come avviene nel GDPR – ma interessa tutte le tipologie di informazioni[29]. Tuttavia, subito dopo questa statuizione che potremmo definire pionieristica, interviene una ulteriore precisazione volta a rimarcare la differenza insita in quei regimi giuridici dei dati che attuano il medesimo principio di libera circolazione: mentre le norme concernenti il flusso dei dati possono essere il risultato di trattative con Paesi terzi, quelle relative alla protezione dei dati personali hanno uno status diverso, in quanto, godendo del rango di diritti fondamentali, non possono essere oggetto di negoziazione[30].

Un ulteriore documento finalizzato alla costruzione delle fondamenta del mercato unico digitale, in cui l'eterogeneità del regime giuridico europeo in materia di circolazione dei dati si avverte con maggiore evidenza, è la Comunicazione "Verso uno spazio europeo comune dei dati". In tal caso, lo scopo principale della Commissione risiede nella proposizione del cosiddetto *data package*, ossia di un insieme di tre provvedimenti che, in aggiunta alla normativa sulla protezione dei dati personali appena entrata in vigore ed al regolamento sulla circolazione dei dati non personali – all'epoca non ancora definitivamente approvato –, mira a creare "uno spazio comune dei dati nell'UE, un'area digitale senza soluzione di continuità, la cui scala consenta lo sviluppo di nuovi prodotti e servizi basati sui dati"[31].

La proposta della Commissione sfocia nell'adozione di tre documenti diversi che, nonostante non si traducano tutti in strumenti di *hard law*, di fatto predispongono o incentivano la creazione di regole differenti per i dati a seconda del settore in cui essi vengono trattati[32]. Se il primo strumento, ossia la direttiva relativa al riutilizzo dell'informazione nel settore pubblico, fa riferimento ad un ampliamento della politica di messa a disposizione dei dati definiti come "pubblici"[33], il secondo consiste in una Raccomandazione volta ad incentivare il regime di *open access* per i dati raccolti e trattati nell'ambito della ricerca scientifica[34]. Il terzo provvedimento, infine, riguarda gli orientamenti sulla condivisione dei dati nel settore privato, tramite i quali la Commissione si offre quale promotrice di principi, accordi e regole a cui gli operatori privati dovrebbero fare ricorso al fine di trasformare il mercato europeo in un grande *hub* di informazioni, da cui tutti potrebbero trarre beneficio[35]. Ciò che accomuna i tre provvedimenti è l'idea di una politica, o meglio, di una cultura di condivisione dei dati che non si limiti semplicemente al settore pubblico – già in parte destinatario di un'apposita direttiva – ma che riguardi anche il settore privato nei rapporti tra imprese e nei rapporti tra imprese ed enti pubblici. Peraltro, nonostante l'intenzione fosse quella di incentivare lo spostamento delle informazioni all'interno del territorio continentale nella misura più ampia possibile, è evidente che la vasta gamma di strumenti regolatori messi in campo dalle istituzioni europee rischia di produrre una settorializzazione e stratificazione normativa in grado di compromettere la libera circolazione[36].

3. La circolazione dei dati personali

3.1. All'interno dell'Unione europea

Come detto, la disciplina riguardante il flusso dei dati personali in Europa è frutto dell'evoluzione normativa che negli anni recenti ha elevato la tutela dell'individuo con riferimento al trattamento delle sue informazioni al rango di diritto fondamentale. Conseguentemente, l'impianto normativo è concepito in maniera tale che la tutela giuridica continentale rimanga il più a lungo possibile ancorata all'informazione, continuando a seguirla in ogni suo spostamento, come una garanzia che non può essere scissa dal bene al quale si accompagna[37]. Questo principio pervade l'intera normativa e, infatti, ha rappresentato uno dei capisaldi attorno ai quali sono state plasmate le disposizioni in materia di circolazione dei dati personali, sia dal punto di vista interno, ossia limitato al flusso intra-europeo, sia dal punto di vista esterno, quando i dati lasciano l'Unione.

Per quanto riguarda la circolazione tra gli Stati membri, con l'impiego della fonte regolamentare in luogo della precedente direttiva, il legislatore europeo è riuscito ad uniformare le discipline nazionali, cosicché, almeno teoricamente, ogni regime giuridico conforme al GDPR deve assicurare lo stesso livello di tutela[38]. Pertanto, alla luce della forte spinta verso l'armonizzazione in materia di protezione dei dati, l'articolo 1, paragrafo 3 del GDPR stabilisce che i singoli Stati membri non possono più lamentare una lacuna nella protezione di tali dati come motivo alla base dell'imposizione di un divieto di trasferimento al di fuori dei propri confini[39]. Invero, nonostante anche la precedente direttiva esordisse con parole simili, la mancata armonizzazione dovuta all'impiego di una fonte normativa "più debole" non era di fatto riuscita a limitare la propagazione degli obblighi di localizzazione dettati da motivi attinenti alla tutela della privacy delle persone fisiche. Anzi, proprio gli ultimi anni di vigenza della precedente direttiva sono stati testimoni di una proliferazione di restrizioni senza precedenti, non solo a causa dell'avvento della digitalizzazione, ma anche perché la promessa di un

elevato livello di protezione dei dati veniva utilizzata come giustificazione di tali misure[40].

Ad ogni modo, nonostante la libera circolazione non venga espressamente annoverata tra i principi fondamentali del GDPR, una chiara affermazione in tal senso proviene direttamente dalla Commissione europea la quale, nell'intento di allargarne l'applicazione anche ai casi in cui agli Stati membri è consentito disciplinare materie specifiche, afferma che questi "dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati"[41].

Tuttavia, se il Regolamento generale sulla protezione dei dati personali rappresenta un apparato giuridico che, oltre che tutelare l'individuo, è funzionale al contrasto dell'insorgenza degli obblighi di *data localization*, è opportuno rammentare che i mezzi attraverso i quali gli Stati membri sono in grado di introdurre nuove restrizioni, o mantenere quelle già esistenti, non ricadono tutti nell'ambito di applicazione del GDPR[42]. Mentre la protezione della privacy degli individui non può più fungere da scudo della localizzazione, i singoli Paesi possono ancora fare affidamento sulle deroghe previste da altre fonti settoriali del diritto europeo riguardanti la gestione dei dati[43], le quali dovranno comunque superare il vaglio relativo alla loro compatibilità con quanto stabilito dal diritto dell'Unione in materia di libertà fondamentali[44].

A tal proposito, non ci si può esimere dal sottolineare ancora una volta come la moltitudine di fonti normative europee, nel tentativo di regolamentare dettagliatamente la gestione dei dati, non faccia altro che offrire ulteriori opportunità per l'introduzione di impedimenti al libero flusso delle informazioni.

3.2. Al di fuori dell'Unione europea

Un discorso diverso vale, invece, se si rivolge lo sguardo alle modalità con cui l'Unione europea disciplina la circolazione dei dati al di fuori dei propri confini, poiché è lo stesso ordinamento giuridico continentale a trasformarsi in un parziale obbligo di localizzazione dei dati personali.

Il meccanismo di trasferimento di informazioni personali verso Paesi terzi o organizzazioni internazionali muove dalla precedente impostazione sancita dalla Direttive 95/46/CE, riadattandola al nuovo contesto digitalizzato in cui si trova ad operare e, soprattutto, cristallizzando le regole di origine giurisprudenziale elaborate dalla Corte di giustizia dell'Unione nella vigenza della normativa ormai abrogata[45]. Pertanto, affinché i dati personali possano lasciare il territorio europeo, gli articoli 44 e seguenti del GDPR predispongono una serie di condizioni in assenza delle quali il trasferimento non può avere luogo. Dunque, nonostante il legislatore abbia predisposto un ampio ventaglio di possibilità di trasferimento capaci di adeguarsi al tipo di situazione in cui versa il titolare del trattamento, stando alla definizione generale di *data localization*, anche l'ordinamento giuridico europeo rientra a pieno titolo nel novero di quelle misure atte a limitare la libera circolazione[46].

Il ragionamento alla base del divieto di imporre obblighi di localizzazione all'interno dell'Unione, viene in questo caso impiegato *a contrario* proprio per condizionare il trasferimento verso l'esterno: dal momento in cui la tutela dei dati personali è ben lontana dal poter essere considerata omogenea a livello globale, l'Unione europea ha deciso di introdurre un meccanismo che sia in grado, quantomeno nelle intenzioni, di agganciare al dato la tutela europea, anche quando questo esce dall'ordinamento giuridico di origine[47]. Se da un lato, le norme europee appaiono come un garanzia imprescindibile nel panorama globale, dall'altro lato, non sono mancate insinuazioni volte a sollevare dubbi sul vero scopo dell'Unione nel predisporre un meccanismo di trasferimento così dettagliato. Non potendo essere alla pari di altre realtà dal punto di vista dello sviluppo tecnologico[48], sembra che l'Unione stia cercando di recuperare terreno sotto l'aspetto della disciplina giuridica, attraverso una applicazione extraterritoriale delle proprie regole[49], le quali, è bene ricordarlo, devono essere osservate, non solo la prima volta che i dati abbandonano l'Europa, ma anche per i trasferimenti successivi[50].

Entrando nel dettaglio, si nota sin da subito come il Regolamento generale racchiuda una serie di regole in cui il flusso internazionale dei dati è percepito come un "elemento strutturale"[51] della normativa e non più, come accadeva nella Direttiva – in vigore in un momento storico in cui lo spostamento delle informazioni tra Stati non aveva la rilevanza che ha oggi – come circostanza episodica annoverabile fra le ipotesi delle mere eccezioni. Dunque, la disciplina che governa il meccanismo di trasferimento esordisce con il principio in ragione del quale i dati possono lasciare il territorio europeo solamente se rispettano le condizioni del capo V. Lungi dal prescrivere un divieto generale come le misure restrittive più rigide, la consapevolezza raggiunta dal GDPR in merito alla essenzialità del flusso internazionale dei dati lo colloca nel complesso degli obblighi di localizzazione condizionali più tenui fra quelli attualmente in vigore[52].

A conferma di ciò, è possibile constatare che se la decisione di adeguatezza, di cui all'articolo 45[53], rimane il metodo principe per il trasferimento come avveniva in precedenza[54], ora questo stesso stru-

mento viene potenziato poiché tanto il diritto europeo quanto quello nazionale non possono fissare limiti al trasferimento extra-europeo nei confronti di quei Paesi o organizzazioni internazionali il cui ordinamento giuridico è stato riconosciuto come adeguato[55]. Tale previsione si inserisce nel disegno generale promosso dal legislatore europeo verso quella che sembra essere una maggiore apertura del continente, con lo scopo di rafforzare le relazioni con altri Paesi, senza però sacrificare la tutela dell'individuo[56].

Un ulteriore aggiornamento concerne la nuova impostazione assunta dal GDPR in materia di deroghe. Se prima tutto ciò che ricadeva fuori dalla decisione di adeguatezza era classificato come deroga, oggi questa qualifica spetta solamente alle ipotesi specifiche – e più numerose rispetto al passato –[57] elencate nell'articolo 49[58]. Ciononostante, la predisposizione di un sistema derogatorio apparentemente a maglie più larghe, non si traduce in un lasciapassare volto ad eludere le disposizioni in materia di protezione di dati: il Comitato europeo per la protezione dei dati è intervenuto sul punto con delle apposite linee guida, insistendo sul fatto che l'interpretazione delle disposizioni all'articolo 49 deve essere la più restrittiva possibile[59].

Infine, sulla base della stessa logica innovativa sono state aggiornate le garanzie adeguate, ossia quelle misure per mezzo delle quali è possibile trasferire i dati personali verso un Paese terzo il cui ordinamento giuridico non è stato valutato come adeguato da parte della Commissione europea. Il sistema in vigore, oltre a risultare più centralizzato rispetto al passato grazie ai maggiori poteri di controllo preventivo ed autorizzatorio concessi agli attori istituzionali, dimostra ancora una volta la presa di coscienza da parte del Regolamento del fatto che il movimento dei dati da un continente all'altro sia diventato un elemento essenziale dell'economia moderna. Il GDPR riesce a bilanciare la tutela dell'individuo con la circolazione dei dati personali tramite la responsabilizzazione dei soggetti coinvolti, ossia titolari e responsabili del trattamento, i quali, siano essi mittenti o riceventi, devono definire misure negoziali o paranegoziali al fine di sopperire alle lacune del sistema giuridico applicabile[60]. Oltre all'impiego di clausole contrattuali tipo, codici di condotta, meccanismi di certificazione o altri strumenti vincolanti, una delle principali novità risiede nell'introduzione delle "norme vincolanti d'impresa" (*Binding Corporate Rules*, o BCRs)[61]. Mentre nel testo della Direttiva non erano affatto prese in considerazione[62], queste disposizioni sono state concepite al preciso scopo di favorire lo scambio di informazioni sia nei gruppi imprenditoriali che nei "gruppi di imprese che svolgono un'attività comune"[63], di fatto prevenendo la formazione di barriere alla libera circolazione di informazioni che ostacolerebbero non poco l'attività commerciale del gruppo. L'inserimento delle BCRs e l'aggiunta di un articolo a sé stante nel regolamento segnano una presa di posizione forte da parte dell'Unione europea poiché, dalla totale assenza nella normativa precedente, sono ora divenute un *unicum* nel panorama del trasferimento extra-europeo dei dati personali, differente da tutte le altre garanzie[64].

Ad ogni modo, il fatto che l'ordinamento giuridico europeo risulti essere una normativa moderna, attenta alle esigenze delle imprese che conducono attività a carattere transfrontaliero e più permissivo rispetto ad altri sistemi giuridici, non è sufficiente a precluderne la qualificazione di regime giuridico di *data localization*[65]. Oltretutto, questa situazione sembra destinata a permanere ancora a lungo, giacché, se la motivazione alla base di questa restrizione risiede nella tutela della privacy degli individui che in altri ordinamenti potrebbe risultare non adeguatamente salvaguardata, l'eventuale soppressione delle condizioni restrittive presupporrebbe il raggiungimento di un livello di armonizzazione globale che, ad oggi, sembra lontano[66]. Invero, dal momento che numerosi Paesi stanno virando verso un'impostazione giuridica in materia di tutela di dati e di localizzazione degli stessi non necessariamente simile a quella del vecchio continente, si può presumere che negli anni avvenire, anziché ad una omogeneizzazione della normativa, assisteremo all'acuirsi dell'arroccamento all'interno delle proprie fortezze informatiche da parte di Stati gelosi del proprio patrimonio digitale.

4. La circolazione dei dati non personali

Nella mente del legislatore europeo, il Regolamento relativo ad un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (RDNP)[67] nasce come strumento diretto a colmare le lacune insorte in seguito all'approvazione del GDPR, il quale, circoscrivendo il suo ambito di applicazione alla categoria dei dati personali, aveva lasciato senza copertura altre tipologie di informazione e i relativi obblighi di localizzazione[68]. Così, al termine di un iter durato all'incirca un anno, precisamente nel 2018, il Regolamento sulla libera circolazione dei dati non personali è stato approvato e a partire dal 28 maggio 2019 trova applicazione nel territorio europeo.

Prima di procedere alla valutazione dell'impatto che la nuova disciplina ha avuto ed avrà con riguardo alla circolazione delle informazioni, è doveroso fare due osservazioni preliminari. La prima è volta a for-

nire una definizione della nuova categoria del dato non personale. A tal proposito, non sembra essere sufficientemente esaustiva la sola lettura dell'articolo 3 del RDNP che, nel primo punto, afferma che i dati non personali sono quelli "diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679"[69]. Pertanto, consapevole delle problematicità giuridiche che di regola si accompagnano alle definizioni di carattere negativo, l'articolo 8, paragrafo 3 del RDNP, ha attribuito alla Commissione europea il compito di formulare ulteriori "orientamenti informativi" atti a specificare il regolamento. Conseguentemente, le linee guida pubblicate a maggio dello scorso anno in ossequio a suddetta disposizione si sono rivelate estremamente opportune, in quanto contenenti una definizione più puntuale della nozione di dato non personale che, invece, non è presente nel testo del Regolamento. Pertanto, grazie al lavoro della Commissione, è ora possibile affermare che la categoria "dato non personale" è costituita sia dalle informazioni che sin dall'origine non si riferivano a una persona fisica identificata o identificabile[70], sia dalle informazioni che, pur inizialmente personali, sono state anonimizzate in un secondo momento.

Peraltro, è pur sempre doveroso osservare che la scelta di demandare (quantomeno in parte) la definizione di questa nuova fattispecie ad un atto il cui valore giuridico all'interno dell'ordinamento europeo non può di certo essere equiparato a quello delle fonti regolamentari, potrebbe comportare seri problemi di coordinamento con altre normative continentali e, soprattutto, potrebbe mettere a rischio la certezza e l'applicazione uniforme del diritto nell'Unione europea. Le linee guida della Commissione, difatti, nonostante offrano un punto di vista autorevole per l'interpretazione del diritto europeo e, in quanto tali, risultino funzionali a risolvere alcuni problemi in chiave applicativa del RDNP, rimangono pur sempre prive della forza di legge che contraddistingue le disposizioni contenute nel regolamento[71]. L'indeterminatezza riguardante la questione definitoria corre il rischio di minare la coerenza di qualificazione del dato fra gli ordinamenti giuridici degli Stati membri, specialmente in quegli ambiti in cui ciò è reso più difficoltoso sia dalle potenzialità di re-identificazione offerte dagli sviluppi tecnologici[72], sia dai margini di discrezionalità lasciati ai singoli ordinamenti nazionali, come avviene nel caso dei dati relativi alle persone fisiche decedute[73]. Naturalmente, la poca chiarezza che attiene alla disposizione cardine della nuova disciplina non potrà che avere ripercussioni negative sulla distinzione, ben lungi dall'essere pacifica[74], tra dato personale e non personale e sull'applicazione dei due regolamenti europei[75].

La seconda osservazione, invece, mira a sottolineare la profonda differenza che intercorre tra il Regolamento generale sui dati personali ed il RDNP per quanto concerne la disciplina della circolazione delle rispettive categorie di informazioni. Se, a differenza di quanto fatto dal GDPR nei confronti dei dati personali, il RDNP è principalmente focalizzato sul tema della circolazione e dell'accesso delle autorità amministrative in una dimensione prettamente interna, la sorte che spetta ai dati non personali – che sfuggono all'applicazione del meccanismo condizionale previsto dagli articoli 44 e seguenti del GDPR – nell'ipotesi in cui essi vengano destinati verso Paesi terzi non sembra essere stata presa in debita considerazione[76]. Pertanto, se da un lato, salvo l'unica eccezione relativa alla pubblica sicurezza che si vedrà in seguito, il regolamento non sembra contenere disposizioni di *data localization*, dall'altro, la mancanza di riferimenti alla dimensione extraeuropea potrebbe incoraggiare lo spostamento di informazioni di inestimabile valore per lo sviluppo delle nuove tecnologie in ordinamenti giuridici che rispondono a regole diverse, incentivando, pertanto, lo sfruttamento di questi dati solamente all'estero, dove l'Unione europea non potrebbe né controllarli né trarne alcun beneficio[77].

Rivolgendo ora l'attenzione a quanto avviene all'interno del territorio continentale, è possibile osservare che il legislatore europeo ha deciso di incentivare la libera circolazione concentrando i propri sforzi, sia verso il settore pubblico, con l'abbattimento degli obblighi di localizzazione derivanti da legislazioni o pratiche amministrative in vigore negli Stati membri[78], sia verso il settore privato, tramite l'incoraggiamento della portabilità delle medesime informazioni nell'ambito delle attività degli utenti professionali[79], in maniera tale da prevenire le pratiche di *vendor lock-in* nemiche del mercato unico[80].

4.1. Il divieto degli obblighi di localizzazione

Il primo scopo che il RDNP intende conseguire è quello di eliminare le restrizioni ingiustificate alla libera circolazione dei dati non personali, considerate dalla Commissione europea il più grande ostacolo allo sviluppo dell'economia dei dati nell'Unione[81]. In virtù di ciò, la norma centrale del regolamento è l'articolo 4, paragrafo 1, il quale vieta agli Stati membri l'introduzione e il mantenimento di obblighi di localizzazione dei dati quando non giustificati da motivi di pubblica sicurezza[82]. Ai fini del Regolamento, sono identificati quali obblighi di localizzazione le disposizioni di legge, gli orientamenti o le pratiche amministrative che, direttamente o indirettamente,

impongono l'elaborazione o la conservazione dei dati limitatamente ad una determinata area geografica[83]. In particolare, i documenti degli organi europei fanno spesso riferimento alle richieste delle autorità di controllo di archiviare localmente i propri dati, alle regole del segreto professionale che prediligono il trattamento a livello locale, alle linee guida amministrative che dispongono lo stesso principio relativamente ai dati gestiti da enti pubblici e, non da ultimo, alle norme di settore che impongono l'utilizzo di dispositivi omologati in un determinato Stato membro[84].

L'identificazione di simili restrizioni risulta molto più complessa di quanto possa apparire a prima vista. Uno studio di particolare interesse, eseguito anteriormente all'adozione definitiva del Regolamento, tende a distinguere tra due diverse categorie[85]. *In primis*, ci sono le cosiddette "barriere dirette", individuabili in maniera più agevole, le quali includono tutte le misure normative che stabiliscono espressamente dove conservare – o non conservare – i dati oppure che contengono obblighi tali per cui il loro rispetto può essere garantito solo tramite la conservazione in un determinato territorio[86]. Più ardue da riconoscere sono, invece, le "barriere indirette". Queste comprendono quelle norme la cui interpretazione può ragionevolmente limitare la scelta di chi gestisce i dati per quanto riguarda il luogo di archiviazione ed il libero flusso. La maggiore difficoltà deriva dal fatto che l'obbligatorietà della restrizione, essendo strettamente correlata all'interpretazione, potrebbe non essere uniformemente intesa[87].

La categoria delle barriere indirette, nonostante i suoi confini piuttosto sfumati, non può essere affatto sottovalutata, dal momento in cui al suo interno si cela la maggioranza degli ostacoli alla libera circolazione dei dati non personali: lo studio citato giunge alla conclusione che, delle quaranta barriere totali rinvenute al termine dell'analisi, trenta rientrano proprio in questa categoria più "sibillina"[88]. In realtà, alla luce delle ipotesi analizzate[89], questo squilibrio non desta troppo stupore: la circostanza che i dati debbano, da un lato, essere obbligatoriamente resi disponibili ai titolari del trattamento o alle autorità di vigilanza, mentre, dall'altro, non possano essere resi noti a terze parti, unita ai troppo spesso frequenti obblighi di autorizzazione prescritti per poter utilizzare una determinata struttura di archiviazione o un determinato responsabile del trattamento[90], possono verosimilmente spingere chi accumula queste informazioni a preferire una soluzione domestica – e magari più costosa in termini di conservazione – in luogo di una più funzionale alla propria impresa, ma che potrebbe attirare attenzioni indesiderate da parte delle autorità di controllo.

Peraltro, la questione degli obblighi di localizzazione permette di individuare una significativa differenza del Regolamento sui dati non personali rispetto al GDPR. Mentre il regolamento riguardante i dati personali concentra la sua attenzione, in primo luogo, sui soggetti che intervengono nella filiera del trattamento dei dati – il titolare ed il responsabile del trattamento – stabilendo gli obblighi da rispettare al fine di assicurare una tutela efficiente al *data subject*, il RDNP dedica la sua norma cardine agli Stati membri. D'altronde, non potrebbe essere diversamente giacché, se per il GDPR l'obiettivo (primario) è quello di tutelare un diritto fondamentale dell'individuo, il secondo regolamento si inserisce, invece, in quella serie di strumenti che, incentivando la circolazione, mirano a rafforzare il mercato unico[91]. Ad ulteriore conferma del ruolo di destinatari principali della disciplina ricoperto dai Paesi membri, il testo del Regolamento tiene a precisare che la normativa non è volta né a ridurre le facoltà di scelta delle imprese in relazione alla localizzazione dei dati, le quali rimangono comunque libere di optare per una soluzione domestica[92], né ad imporre l'esternalizzazione dei servizi da parte degli enti pubblici quando sussistono esigenze che li spingono a preferire l'autofornitura[93].

Come anticipato, la presa di posizione dell'Unione europea nei confronti della *data localization* nell'ambito della circolazione dei dati non personali scaturisce dal preoccupante aumento di misure restrittive verificatosi negli ultimi anni, spesso dettato dalla convinzione che la conservazione e l'analisi dei dati all'interno dei confini nazionali siano sinonimo di sicurezza oppure che facilitino l'accesso e la sorveglianza da parte delle autorità. In aggiunta, alcune limitazioni sono state imposte al preciso scopo di sfavorire i fornitori di servizi stranieri o multinazionali rispetto a quelli nazionali[94]. Stando alle stime prettamente economiche presentate dalla Commissione europea, la drastica diminuzione di queste restrizioni voluta dal nuovo regolamento permetterebbe all'economia dei dati di crescere fino a 739 miliardi di euro entro il 2020[95]. Oltretutto, secondo uno studio dello *European Centre for International Political Economy* (ECIPE), l'effetto sarà più che positivo per il mercato, poiché, beneficiando le industrie di costi minori legati alla maggiore flessibilità nella gestione dei propri dati, il PIL potrebbe crescere di circa 8 miliardi di euro l'anno[96]. Pertanto, la Commissione, al fine di cogliere le opportunità offerte dall'economia dei dati, ha ritenuto necessario garantire il libero flusso delle informazioni stabilendo il medesimo principio di libera circolazione, ma garantendolo tramite due fonti diverse, il GDPR, per il versante

dei dati personali ed il RDNP, per quello dei dati non personali[97]. Sebbene offrano un quadro all'apparenza nitido, le valutazioni della Commissione si focalizzano quasi esclusivamente sull'aspetto economico connesso all'aumento delle misure restrittive alla circolazione dei dati, senza tuttavia approfondire ulteriori profili che meritano di essere presi in considerazione. In tal senso, alcune delle ultime iniziative promosse tanto a livello europeo[98], quanto a livello nazionale[99], non sembrano avere come obiettivo una riappropriazione del bene "dato" in chiave monopolistica e con l'intento di escluderne gli altri dal *management* ma, al contrario, tentano con non poche difficoltà di riconquistare il terreno perduto dagli ordinamenti giuridici nazionali e sovranazionali in un ambito, quello della gestione dei dati a valenza strategica, in cui la posizione centrale un tempo ricoperta è stata fortemente ridimensionata dall'entrata in campo dei servizi offerti dagli OTT[100]. Pertanto, se per un verso, il gravame economico derivante da simili politiche è innegabile, per altro verso, la questione della *data localization* potrebbe essere riletta come un timido tentativo attuato dalle istituzioni del vecchio continente di stabilire un regime concorrenziale con riguardo al trattamento dei dati, attraverso la realizzazione di infrastrutture proprie che siano in grado di operare parallelamente a quelle ben più avanzate dei giganti del tech.

4.1.1. La sicurezza pubblica come unica eccezione

L'articolo 4 del Regolamento sulla libera circolazione dei dati non personali prevede come unica eccezione al divieto di imporre obblighi di localizzazione la sicurezza pubblica. Al fine di evitare l'insorgere o il permanere di discipline non fondate su tale base legittima, grava sugli Stati membri il dovere di procedere alla disamina di tutte le norme che impongono un obbligo di localizzazione per poi abrogare quelle non conformi al Regolamento. Tuttavia, nel caso in cui ritengano necessario il mantenimento di alcune misure restrittive, proprio perché fondate su motivi di pubblica sicurezza, devono darne comunicazione alla Commissione europea allegando la relativa giustificazione[101]. Per contro, alla Commissione è riconosciuta la facoltà di presentare osservazioni qualora ritenga opportuno che tali disposizioni debbano essere modificate o addirittura abrogate, in quanto non confacenti ai principi sanciti dal diritto comunitario[102] o dalla giurisprudenza della Corte di giustizia dell'Unione[103].

Il considerando n. 19 del RDNP agevola l'interpretazione del significato di sicurezza pubblica. Innanzitutto, il riferimento alla sicurezza sia interna che esterna permette di trattenere tutte le informazioni potenzialmente utili ai fini di prevenzione di attacchi provenienti da Paesi terzi, di fatto legittimando la conservazione di dati relativi a contesti non nazionali o non europei. Appare in tal caso evidente il legame con la speciale disciplina antiterrorismo diffusasi in tutto il continente a seguito degli attacchi terroristici degli anni recenti. Come evidenziato dalla dottrina, il timore di essere vittime di simili aggressioni ha scatenato la proliferazione di normative *ad hoc* che hanno eroso alcuni diritti fondamentali degli individui – soprattutto il diritto alla protezione dei dati personali – in nome della pubblica sicurezza[104]. *A fortiori*, un simile atteggiamento potrebbe contraddistinguere la regolamentazione dei dati non personali: scevro da rischi di lesione diretta ai diritti fondamentali della persona fisica, lo Stato tenterà di trattenere nelle proprie banche dati quante più informazioni possibili, legittimato dall'interesse alla difesa delle "questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati"[105].

Nel prosieguo, la normativa sembra ampliare di molto il novero di interessi legittimanti una deroga. Difatti, nell'esigere una minaccia "reale e sufficientemente grave ad uno degli interessi fondamentali della società", vengono espressamente riportati "il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari".

In questa definizione a prima vista dettagliata, potrebbero nascondersi non poche insidie interpretative: basti pensare al concetto di servizio pubblico essenziale, il quale, non godendo di una definizione uniforme a livello continentale[106], rischia di creare una disparità di trattamento tra i diversi Stati membri. Altrettante incertezze accompagnano le nozioni di incolumità pubblica e interessi militari. Se la prima può potenzialmente impedire la circolazione di numerose informazioni relative alla salute dei cittadini – già oggetto di significative barriere indirette secondo lo studio sopra citato –[107], gli interessi militari, a loro volta, tolgono dalla circolazione, non solo le informazioni *latu sensu* strategiche, ma anche la maggior parte dei dati relativi alla produzione di materiale utilizzato dalle forze armate, detenuti dalle industrie belliche.

Se questi sono i presupposti, è probabile che gli Stati membri, desiderosi di mantenere le informazioni più delicate nel territorio in cui possono esercitare un potere "diretto", daranno un'interpretazione

estensiva al concetto di sicurezza pubblica, al preciso scopo di limitare la fuoriuscita dei dati nella misura più ampia possibile. A tal riguardo, sono condivisibili le perplessità espresse dal Comitato economico e sociale europeo (CESE) con riferimento alla imprecisione con cui viene delineata questa nozione ed alla mancanza di un "riferimento alle controversie o alle modalità per verificare in che modo gli Stati membri rispetteranno i criteri della pubblica sicurezza, né ad eventuali sanzioni nei loro confronti, ove opportuno"[108].

Quanto detto assume particolare rilevanza a fronte del contesto in cui operano alcune agenzie governative, reso noto a seguito delle rivelazioni riguardanti la vicenda *Datagate*[109]. Questa esperienza ha dimostrato che ad essere interessati al possesso di dati non sono solamente le compagnie private, ma anche le agenzie di intelligence che, proprio al fine di garantire la sicurezza pubblica, si sono rese protagoniste di una raccolta massiva di informazioni mai vista nella storia[110]. È bene notare che, nonostante il dibattito manifestatosi in seno all'opinione pubblica a partire dal 2013 si sia concentrato sulla violazione della vita privata degli individui sottoposti a sorveglianza, le stesse osservazioni potrebbero essere svolte, *mutatis mutandis*, in relazione ai dati a carattere non personale. Ne è un esempio significativo il comprovato meccanismo in voga fra i funzionari degli organi inquirenti consistente nel chiedere accesso alle informazioni detenute da imprese private nel settore ICT. Richieste che nella maggior parte dei casi non trovano nessuna base giuridica riconosciuta dalla legge e che, solitamente, vengono assecondate per motivi di reverenza o per timore di ripercussioni negative[111].

In un certo senso, sussiste la possibilità che, grazie allo schermo della sicurezza pubblica, possa venire alla luce anche per i dati non personali una differenziazione già nota per quelli personali. Se il Regolamento generale assicura una disciplina giuridica parzialmente diversa – *rectius*, più stringente – per le cosiddette categorie particolari di dati[112], è plausibile che in futuro si andrà a delineare una distinzione simile anche per i dati non personali. Riprendendo la vecchia nomenclatura tanto cara al nostro legislatore[113], una sorta di dato non personale "sensibile", ossia un dato che per la sua connessione funzionale con l'interesse collettivo della sicurezza pubblica, giustifica un regime giuridico diverso, grazie al quale lo Stato può imporre all'ente che lo conserva, pubblico o privato che sia, un obbligo di localizzazione[114].

In ultima analisi, essendo ancora nella fase iniziale di vigenza del RDNP, l'ampiezza dell'area che il concetto di pubblica sicurezza andrà concretamente a ricoprire verrà definita dalla prassi degli Stati membri e, soprattutto, dall'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea, la quale, al fine di dare corpo alla nuova normativa, potrebbe ridurre la discrezionalità interpretativa riconosciuta dal regolamento.

4.2. Una nuova portabilità autoregolamentata

A seguito della risonanza che il diritto alla portabilità dei dati personali ha avuto con l'entrata in vigore del GDPR, anche per il Regolamento sui dati non personali viene sottolineato sin da subito l'impatto positivo che il libero trasferimento delle informazioni da un fornitore di servizi ad un altro, su richiesta dell'utilizzatore e senza costi eccessivi, potrebbe avere nei confronti della concorrenza nel mercato interno[115]. Inoltre, è lo stesso testo della nuova disciplina che effettua una comparazione fra il diritto già vigente nell'Unione – in particolare il GDPR – che garantisce una tutela solida al consumatore desideroso di cambiare il prestatore di servizi, e le lacune che, al contrario, riguardano la situazione in cui versano gli utenti professionali, i quali, sprovvisti di una simile protezione, spesso si trovano intrappolati a causa di pratiche di *vendor lock-in* che comportano oneri di mantenimento più alti ed, al contempo, danneggiano la competitività delle imprese[116].

Sfortunatamente, malgrado le premesse, per il particolare caso dei dati a carattere non personale il legislatore europeo ha deciso di intraprendere una strada diversa rispetto a quanto fatto nel 2016[117]: se alle persone fisiche è riconosciuto a livello normativo un vero e proprio diritto alla portabilità, gli utenti professionali possono solo fare affidamento sull'elaborazione di codici di condotta di autoregolamentazione che, benché supportata e controllata direttamente dalla Commissione, non riuscirà mai a garantire quella certezza del diritto e quella parità di condizioni che dovrebbero essere alla base dell'adozione di questo regolamento[118]. Oltretutto, è difficile comprendere perché ragioni quali la necessità di "mantenere il passo con la potenziale innovazione del mercato e tener conto dell'esperienza e delle competenze dei fornitori di servizi e degli utenti professionali di servizi di trattamento di dati"[119], possano giustificare una regolamentazione tramite codici di condotta in luogo di un vero e proprio diritto che sia in grado di bilanciare lo squilibrio di potere intercorrente tra tali utenti professionali, spesso piccole e medie imprese, e fornitori di servizi online, i quali con la digitalizzazione dei settori pubblico e privato, stanno velocemente trasformandosi negli attori più potenti del mercato[120].

La volontà del regolamento di distaccarsi in maniera netta dalla posizione adottata nel GDPR è di-

mostrata, prima che dalla predisposizione di una tutela giuridica più debole, anche dall'utilizzo di una terminologia differente: se l'individuo può fare affidamento sulla *portability* inglese o sulla *portabilité* francese, i codici di condotta devono essere orientati alla disciplina, rispettivamente, del *porting* o del *portage*[121]. Questa differenza terminologica deriva, probabilmente, dalla volontà di sottolineare in maniera chiara il tipo di relazione giuridica che viene presa in considerazione nei due testi. Il diritto alla portabilità di cui all'articolo 20 del GDPR fa riferimento ad una situazione giuridica in cui i due protagonisti sono, da un lato, l'interessato persona fisica e, dall'altro, colui che tratta le sue informazioni, il quale, di regola, incarna la figura del titolare del trattamento. Dunque, similmente a quanto si è visto nella tradizione statunitense[122], questo diritto si inserisce in un'ottica di tutela del consumatore nel rapporto con il fornitore del servizio[123]. Per i dati non personali, al contrario, l'articolo 6 circoscrive il suo riferimento non ad un utente generalmente inteso, bensì alla specifica categoria dell'utente professionale, il quale tratta i dati per fini connessi alla sua attività. Di conseguenza, il rapporto intercorrente tra l'utente professionale ed il fornitore di servizi di gestione di dati, più che in una dinamica B2C, può essere ricondotto nell'ambito business-to-business[124], similmente a quanto avviene nel caso di dati personali tra titolare del trattamento e responsabile del trattamento[125].

Ad avviso di chi scrive, la strategia che l'Unione europea ha deciso di perseguire appare discutibile. La necessità, più volte richiamata, del coinvolgimento delle PMI nel processo di elaborazione di questi codici di condotta non è uno strumento sufficientemente forte da dissuadere i dubbi che pervadono la preferenza per l'autoregolamentazione, soprattutto alla luce dell'attuale momento storico del mercato dei dati in cui poche grandi imprese stanno guadagnando capacità egemoniche. In questo frangente, l'Unione europea ha l'opportunità di distinguersi ancora una volta rispetto ad altre realtà giuridiche tramite una presa di posizione forte verso il riequilibrio di quella parità contrattuale che sembra essersi fortemente indebolita[126]. Proprio da tali esigenze sono di recente nate numerose istanze in ambito accademico volte a sollecitare un dibattito profondo sulla necessità di allargare la normativa a tutela del consumatore al fine di ricomprendere anche le piccole e medie imprese, così da scongiurare la formazione di posizioni dominanti che rischiano di alterare la libera concorrenza nel mercato europeo in modo irreversibile[127]. La prevenzione di pratiche simili potrebbe avvenire in maniera più efficace se solo il Regolamento fosse sceso più nel dettaglio, magari fissando a chiare lettere alcune delle norme inderogabili che i codici di condotta dovrebbero necessariamente includere oppure, come ha notato il CESE, definendo gli orientamenti da cui i meccanismi di autoregolamentazione dovrebbero muovere, non limitandosi al semplice richiamo alle migliori pratiche, agli obblighi informativi ed alle tabelle di marcia[128].

5. I punti deboli dell'impianto regolamentare europeo

Come si è avuto modo di vedere, l'ultimo decennio ha visto l'Unione europea assumere un ruolo centrale nel campo della regolamentazione del settore dei dati, attraverso una serie di iniziative che hanno gradualmente dato forma al mosaico del mercato europeo digitale. Tuttavia, le soluzioni di compromesso e le ampie lacune emerse al termine dell'iter legislativo che ha portato alla approvazione della disciplina del flusso dei dati non personali mostrano l'incompletezza di questo grande disegno[129].

In particolare, alcuni dei punti deboli della normativa in esame derivano da un contrasto che, benché preso in considerazione dal legislatore, non sembra essere stato risolto con una scelta adatta alle problematiche che titolari, responsabili del trattamento e gestori dei dati in genere si trovano ad affrontare quotidianamente. I regolamenti, le direttive e tutte le altre fonti, anche di *soft law*, adottate al fine di rendere l'economia dei dati alla portata di tutti sembrano essere lontane da una realtà dei fatti poliedrica ed interconnessa come quella odierna, con la conseguenza che quando differenti mondi entrano in contatto l'uno con l'altro tutto l'impianto normativo viene messo a dura prova.

Una chiara ipotesi in cui il Regolamento sui dati non personali sembra vacillare riguarda gli "insiemi di dati misti". Nonostante non vi sia una definizione esplicita nel Regolamento[130], sono considerati come tali quei dataset che sono composti sia da dati personali che da dati non personali. Il RDNP dedica a tale fattispecie il secondo paragrafo dell'articolo 2, il quale stabilisce che il Regolamento generale sulla protezione dei dati personali e quello sulla libera circolazione dei dati non personali si applicano alla rispettiva categoria di dati. Tuttavia – aggiunge la norma – quando tali insiemi sono "indissolubilmente legati"[131], il GDPR troverà applicazione nei confronti dell'intero dataset anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme[132], in ossequio alla costante logica della protezione prima della circolazione.

Il fenomeno in oggetto non sembra essere stato approfondito in maniera soddisfacente né dal Rego-

lamento, che, eccetto il riferimento alle valutazioni ed agli orientamenti della Commissione europea[133], gli dedica un solo paragrafo; né dalla Commissione stessa che nell'elaborazione di quelle linee guida che avrebbero dovuto semplificare il lavoro degli operatori del settore, si limita ad affermare che, in considerazione della diminuzione del valore derivante dalla eventuale separazione dell'insieme in dati personali e non personali, dell'assenza di una obbligo che imponga tale separazione e, soprattutto, del fatto che tali insiemi rappresentano la maggioranza dei dataset esistenti, il GDPR si applicherà, di regola, a tutti gli insiemi di dati misti[134].

In realtà, la vera falla del sistema da cui sembra provenire l'approccio, in un certo senso "sbrigativo", che traspare tanto dal testo del Regolamento quanto dalla guida della Commissione, può essere rinvenuta nel differente peso attribuito al concetto di rischio nei due regolamenti, il quale, creando un dislivello alla base delle normativa europea in materia di dati, contribuisce a rendere fragile l'intera struttura. Se il *risk-based approach* costituisce uno degli elementi qualificanti il Regolamento generale sui dati personali[135], la stessa cosa non può dirsi con riferimento alla disciplina dei dati non personali, dove la valutazione del rischio, che si rivelerebbe uno strumento assai utile per comprendere la natura del dato e per individuare le implicazioni che i dati non personali possono avere sull'insieme di dati misti, non viene presa in dovuta considerazione[136]. Difatti, la decisa accelerazione della digitalizzazione della società moderna ha messo in crisi la definizione stessa di dato personale, portando con sé innumerevoli difficoltà nell'individuazione della linea di confine tra carattere personale e non personale e causando non pochi disagi tanto ai titolari del trattamento quanto alle autorità di controllo che devono monitorarli. Pertanto, in un mondo dove la natura delle informazioni cambia frequentemente, non è più possibile limitare la valutazione del rischio – generalmente inteso e non limitato esclusivamente alla c.d. "valutazione d'impatto sulla protezione dei dati" prevista dall'art. 35 del GDPR – alle sole ipotesi di dati personali, ma appare opportuno, se non necessario, estenderla a tutti i dati che il medesimo soggetto ha a disposizione, includendo anche quelli non personali[137]. Purtroppo, è proprio l'assenza di una visione onnicomprensiva capace di tenere conto della mutevolezza della realtà digitale a minare l'efficacia delle disposizioni del RDNP, le quali non riescono a soddisfare l'esigenza di coordinamento con il Regolamento generale sui dati personali.

Questo particolare deficit potrebbe ripercuotersi negativamente sulla effettività della libera circolazione di tutti i tipi di informazione sia all'interno che all'esterno dell'Unione. In primo luogo, risultano evidenti le problematicità che dovrebbe affrontare il titolare del trattamento desideroso di usufruire delle possibilità offerte dal RDNP giacché, malgrado l'assenza di un obbligo diretto di separazione del dataset, si vedrebbe costretto a scindere il suo insieme in due parti: una costituita da dati personali che, ipoteticamente, potrebbe essere sottoposta ad una misura restrittiva della circolazione – motivata da ragioni diverse dalla protezione dei dati – mentre l'altra parte, contenente dati non personali, potrebbe essere trasferita liberamente[138]. Di conseguenza, graverebbe sul titolare del trattamento un onere aggiuntivo ed implicito che, prescrivendo di fatto un'operazione costosa e di difficile riuscita[139], rischia di incentivare quell'atteggiamento di chiusura che il Regolamento mira ad eliminare[140].

In secondo luogo, l'interpretazione fornita dalla Commissione che, nel tentativo di dare precedenza alla tutela dei dati personali, propende per un'applicazione aprioristica del regime più restrittivo previsto dal GDPR nei confronti degli insiemi dei dati misti, potrebbe condurre ad un'ulteriore barriera indiretta alla libera circolazione dei dati non personali, trasformandosi in buona sostanza proprio in una misura di *data localization*[141].

In ultima analisi, la delicatezza del problema degli insiemi di dati misti e le difficoltà nel gestire le conseguenze di una regolamentazione così scarna si possono osservare anche con riferimento alla questione della portabilità, dove la predisposizione di una tutela a due livelli suscita alcune perplessità. Innanzitutto, se i codici di condotta non riconosceranno un vero e proprio diritto di portabilità, l'utente professionale intenzionato a spostare presso un nuovo *provider* l'intero insieme, senza procedere ad una complicata separazione, rischierebbe di dover affrontare un lungo contenzioso con il precedente fornitore del servizio i cui tempi di risoluzione sono del tutto inconciliabili con la velocità a cui procede la società digitale[142]. Oltretutto, anche nell'ipotesi in cui venisse riconosciuto dai codici di condotta e da clausole contrattuali, la prevalenza di una prerogativa di questo genere non può essere data per certa nell'eventualità in cui dovesse entrare in conflitto con altri diritti espressamente stabiliti dalla lettera della legge[143], in particolare con quelli più maturi e radicati nel mondo digitale – ad esempio, la proprietà intellettuale, i segreti commerciali o i diritti connessi alla tutela giuridica delle banche dati[144].

6. La necessità di una visione onnicomprensiva per la realtà digitale moderna

L'economia globale ed interconnessa che caratterizza la nostra epoca si basa su un incessante scambio di informazioni che partono ed arrivano in tutte le parti del mondo in tempi praticamente nulli. In risposta al rapido aumento del valore economico e dell'importanza strategica dei dati, sia personali che non, si è assistito ad una crescita del sentimento di sfiducia fra gli Stati, sfociato poi nell'adozione di normative aventi ad oggetto obblighi di localizzazione. Di fronte ad un cambiamento di simile portata, l'ordinamento giuridico europeo ha deciso fronteggiare la sfida posta dal fenomeno della *data localization* non attraverso un'iniziativa singolare ed unica, ma seguendo un percorso a tappe, in linea con la gerarchia di valori della tradizione giuridica continentale. In prima battuta, il legislatore ha deciso di predisporre una tutela elevata all'interno dell'Unione europea per quanto riguarda il trattamento dei dati personali. Partendo da tale presupposto, ha poi elaborato un insieme di regole che, per un verso, incentivasse la circolazione di tali dati sul suolo continentale e, per l'altro, permettesse alla tutela di viaggiare con il dato personale anche quando questo viene trasferito verso Paesi terzi.

La disciplina riguardante l'altro versante del *data law*, quello del dato non personale, ha visto la luce in un secondo momento, quando il peso della mancanza di una normativa completa a sostegno dell'economia europea dei dati non era di fatto più sostenibile. Sfortunatamente, il Regolamento sulla libera circolazione dei dati non personali non sembra avere soddisfatto le aspettative, in quanto non riesce a fornire un quadro normativo sufficientemente aderente alle dinamiche della realtà digitale.

Allargando lo sguardo all'impianto generale in materia di dati, la critica principale che può muoversi nei confronti del legislatore europeo concerne la carenza di una risistemazione in chiave organica di tutta la disciplina. Attualmente, l'ordinamento continentale consta di una vasta gamma di normative settoriali e, in alcuni casi, non coordinate, la cui stratificazione nel corso dell'ultimo decennio rischia di confondere l'interprete e di tradursi in uno strumento non adatto a servire lo sviluppo della società digitale[145]. Le lacune patite dal Regolamento sui dati non personali non rappresentano altro che il precipitato ultimo di questa disordinata ipertrofia normativa: nonostante l'apparente complementarietà, le sue disposizioni sono state concepite come facenti parte di un *corpus* separato rispetto al Regolamento generale sulla protezione dei dati personali, in evidente contrasto con quella visione di insieme che è ormai imprescindibile se si vuole regolamentare il mondo virtuale con la speranza di ottenere risultati concreti. Viceversa, il RDNP rischia di diventare un regolamento senza oggetto in quanto l'assenza di una impostazione sistemica che tenga conto della preponderanza degli insiemi di dati misti e, soprattutto, delle caratteristiche dei soggetti che trattano questi insiemi, non permette di inquadrare il problema nella prospettiva idonea ad attribuire al dato non personale l'importanza che merita. In aggiunta, oltre alla prevalenza schiacciante del GDPR patita dal Regolamento sui dati non personali, non sono da sottovalutare le ulteriori problematiche di coordinamento di questi due regolamenti con le altre discipline settoriali che, spesso, prescindono dalla distinzione personale-non personale[146].

La risoluzione degli interrogativi che inevitabilmente emergono da questa confusione normativa è posta totalmente a carico del soggetto che gestisce i dati, il quale, disorientato in un labirinto di regole, si rifugerà nei lidi più sicuri, ma anche più costosi, dell'internalizzazione del trattamento dei dati. Tuttavia, è bene ricordare, simili pratiche non sono economicamente sostenibili da parte delle piccole e medie imprese che, ancora una volta, saranno costrette a pagare le conseguenze di disposizioni normative non coordinate adeguatamente fra loro.

Note

[1] OCSE, *Data-driven innovation. Big data for growth and well-being*, OCSE Publishing, Parigi, 2015.

[2] A. McAfee, E. Brynjolfsson, *Big data: the management revolution*, in "Harvard Business Review", 2012, n. 10.

[3] H.A. Ünver, G. Kim, *Cross-border data transfers and data localization*, EDAM Cyber Policy Paper Series, 2016, n. 3, p. 2-6.

[4] M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, ECIPE occasional paper, 2014, n. 3, p. 3-10.

[5] M.F. Ferracane, *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper, 2017, n. 1, p. 6.

[6] M.L. Montagnani, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in "Mercato concorrenza regole", 2019, n. 2, pp. 311-313.

[7] M.F. Ferracane, *op. cit.*, p. 2-3.

[8] Come, ad esempio, accade in Russia. Per un approfondimento, si veda A. Savelyev, *Russia's new personal data localization regulations: a step forward or a self-imposed sanction?*, in "Computer Law & Security Review", 2016.

[9] M.F. Ferracane, *op. cit.*, p. 2-3.

[10] *Ibidem.*

[11] *Ibidem.* Naturalmente, la realtà dei fatti non rispecchia così nettamente la classificazione appena svolta, giacché le differenze possono essere molto più labili di quanto si pensi, ed

anche una misura condizionale può facilmente tramutarsi in rigida se l'iter necessario ad addivenire al trasferimento è troppo oneroso per la dimensione in cui opera il trasferente.

[12] *Ivi*, p. 8-9.

[13] M. Bauer, H. Lee-Makiyama, E. van der Marel, B. Verschelde, *The cost of data localisation: friendly fire on economic recovery*, cit., p. 5-10.

[14] P.S. Ryan, R. Falvey, S. Merchant, *When the cloud goes local: the global problem with data localization*, in "Computer", Vol. 46, 2013, n. 12, p. 54-59; A. Chander, U.P. Le, *Breaking the web: data localization vs. the global internet*, Working Paper, 2014, n. 1, p. 10-16; European Commission, *Cross-border data flow in the digital single market: study on data location restrictions* (SMART n. 2015/0054), Publication Office of the EU, 2017.

[15] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa* - COM(2015) 192 final, pp. 15-21.

[16] La relatrice del Parlamento europeo Anna Maria Corazza Bildt, a seguito dell'approvazione del Regolamento (UE) 2018/1807, ha affermato che è stata introdotta una "quinta libertà di circolazione" che riguarda tutti i dati.

[17] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti* - COM(2017) 228 final, 2017, pp. 23-26.

[18] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, ECIPE policy brief, 2016, n. 3, pp. 12-13. In particolare: «A ban on data localisation is a powerful political message that the Single Market is open for business. This argument is particularly pertinent as the EU seeks to convince the market and turn the tide on the digital investments, and both inward and domestic investments into Europe's digital economy are withheld or diverted to other regions».

[19] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente* - COM(2011) 882 final, pp. 7-8. In particolare: «Nonostante l'armonizzazione minima introdotta dalla direttiva del 2003 sul riutilizzo delle informazioni del settore pubblico, permangono differenze significative nelle norme e pratiche nazionali, con conseguente frammentazione del mercato interno dell'informazione e presenza di ostacoli alla creazione di servizi di informazione transfrontalieri».

[20] A tal proposito, è opportuno ricordare che, nonostante la tematica dei dati personali stesse prendendo piede, la prima proposta ufficiale emanata dalla Commissione con riguardo alla riforma della disciplina della protezione dei dati personali è datata gennaio 2012.

[21] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Dati aperti, un motore per l'innovazione, la crescita e una governance trasparente*, cit., pp. 5-6.

[22] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Verso una florida economia basata sui dati* - COM(2014) 442 final, pp. 12-13.

[23] Per un'analisi dettagliata del percorso che ha condotto all'istituzionalizzazione del diritto alla protezione dei dati personali, si vedano: G. Gonzalez Fuster, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014; G.F. Aiello, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale «disomogeneo» alla luce della nuova proposta di General Data Protection Regulation*, in "Osservatorio del diritto civile e commerciale", 2015, n. 2.

[24] L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in "diritticomparati.it", 2014, pp. 8-13.

[25] Per un approfondimento, si vedano: H. De Hert, V. Papakonstantinou, *The data protection regime in China. In-depth analysis for the LIBE Committee*, Publication Office of the EU, 2015, p. 13-27; Z. Yuexin, *Cyber protection of personal information in a multi-layered system*, in "Tsinghua China Law Review", 2019, n. 1.

[26] 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.

[27] C. Colpaert, M.-C. Janssens, *Work in progress: the proposal of the free flow of non-personal data regulation*, KU Leuven - CITIP Blog, 2018.

[28] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea* - COM(2017) 9 final, pp. 9-14.

[29] *Ivi*, pp. 2-5.

[30] *Ibidem*.

[31] Id., *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Comunicazione "Verso uno spazio comune europeo dei dati"* - COM(2018) 232 final, p. 1.

[32] M.L. Montagnani, *op. cit.*, pp. 298-302.

[33] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[34] Raccomandazione (UE) 2018/790 della Commissione del 25 aprile 2018 sull'accesso all'informazione scientifica e sulla sua conservazione.

[35] Commissione europea, *Documento di lavoro dei servizi della Commissione. Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso uno spazio comune europeo dei dati"* - SWD(2018) 125 final.

[36] M.L. Montagnani, *op. cit.*, pp. 298-302.

[37] S. Kirschen, *Il trasferimento all'estero dei dati*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018", Giuffrè, 2019, pp. 265-268.

[38] Regolamento (UE) 2016/679, considerando n. 13. In particolare: «Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione

non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[39]Regolamento (UE) 2016/679, art. 1, par. 3: «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».

[40]M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit., p. 3-8.

[41]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[42]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union* - COM (2019) 250 final, p. 15, dove è riportato un esempio eloquente al riguardo: «Una normativa nazionale prevede che la contabilità del personale sia situata in uno specifico Stato membro per ragioni riguardanti il controllo regolamentare, ad es. da parte dell'amministrazione fiscale nazionale. Tale normativa nazionale non rientrerebbe nell'ambito di applicazione dell'articolo 1, paragrafo 3, del regolamento generale sulla protezione dei dati, in quanto i motivi non riguardano la protezione dei dati personali. Questo obbligo dovrebbe invece essere valutato sulla base delle disposizioni relative alle libertà fondamentali e delle deroghe consentite a tali libertà previste nel trattato sul funzionamento dell'Unione europea».

[43]Gli esempi generalmente riportati fanno riferimento, ma non sono limitati, a: Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno; Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno; Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

[44]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 14-15.

[45]Tra le sentenze più significative, si ricordano: Corte di Giustizia UE, 13 maggio 2014, causa C-131/12; Corte di Giustizia UE, 6 ottobre 2015, causa C-362/14; Corte di Giustizia UE, 28 luglio 2016, causa C-191/15. Per una panoramica generale sull'evoluzione della giurisprudenza della Corte di giustizia, si veda: S. Calzolaio, voce *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017, pp. 620-624.

[46]Institute of International Finance, *Data flows across borders. Overcoming data localization restrictions*, 2019.

[47]Commissione europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato* – COM(2017) 7 final, pp. 4-6. In particolare: «L'obiettivo principale di tali norme è garantire che, quando i dati personali dei cittadini europei vengono trasferiti all'estero, la tutela viaggi con loro».

[48]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*, cit., pp. 23-26.

[49]V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in "Il diritto dell'informazione e dell'informatica", 2015, n. 4-5, pp. 683-695; L. Valle, L. Greco, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in "Il diritto dell'informazione e dell'informatica", 2017, n. 2, pp. 198-201; S. Kirschen, *op. cit.*, pp. 265-268.

[50]Regolamento (UE) 2016/679, art. 44.

[51]S. Kirschen, *op. cit.*, pp. 261-265.

[52]M.F. Ferracane, *op. cit.*, p. 5.

[53]Regolamento (UE) 2016/679, art. 45, par. 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».

[54]S. Kirschen, *op. cit.*, pp. 261-272; L. Valle, L. Greco, *op. cit.*, pp. 188-191.

[55]Infatti, l'articolo 49, paragrafo 5 del GDPR recita: «In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione». S. Kirschen, *op. cit.*, pp. 283-291.

[56]*Contra*, L. Valle, L. Greco, *op. cit.*, pp. 218-219. In particolare: «[...] per quanto concerne l'altro profilo della regolazione transfrontaliera dei dati personali relativo al trasferimento verso Paesi terzi esso è legato a dei canoni, come quello del controllo dell'adeguatezza della disciplina del Paese terzo e della decisione sull'adeguatezza di clausole standard da parte della Commissione europea, che poco si adattano ad un flusso di dati quale quello che si reputa conveniente allo sviluppo delle attività economiche nel mondo contemporaneo».

[57] S. Kirschen, *op. cit.*, pp. 283-291.

[58]L'elenco delle deroghe di cui all'articolo 49 del GDPR ricomprende: il consenso esplicito dell'interessato, l'esecuzione o la conclusione di un contratto in cui l'interessato è parte o beneficiario, importanti motivi di interesse pubblico, difesa o esercizio di un diritto in sede giudiziale, interessi vitali, quando le informazioni sono contenute in un registro aperto alla consultazione pubblica e, infine, interessi legittimi cogenti del titolare del trattamento.

[59]European Data Protection Board (EDPB), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 2018. Invero, il Comitato, forzando il significato letterale del testo, afferma che i concetti di "occasionalità" e "non ripetitività" indicati con riferimento alla sola eccezione relativa agli interessi legittimi cogenti del titolare del trattamento, devono essere applicati a tutte le ipotesi previste nell'articolo, anche se non indicato esplicitamente.

[60]S. Kirschen, *op. cit.*, pp. 274-283.

[61]L'articolo 4, punto 20, del GDPR definisce le norme vincolanti d'impresa come «le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune». Pertanto, tali norme sono

costituite da quell'insieme di regole, politiche e strumenti applicabili (solamente) all'interno delle società del gruppo al fine di assicurare il rispetto dei principi, dei diritti e degli obblighi riguardanti la protezione dei dati personali nell'Unione europea. Per un approfondimento si veda, G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al safe harbor agreement?*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai «Safe Harbour Principles» al «Privacy Shield»", Tre Press, 2016.

[62]Tuttavia, il loro impiego non era sconosciuto prima dell'avvento del GDPR, tanto che il Gruppo di lavoro Articolo 29 si era già espresso a tale riguardo nel 2003: Article 29 Data Protection Working Party (WP29), *Working document: transfers of personal data to third countries: applying article 26 (2) of the EU data protection directive to binding corporate rules for international data transfers* (WP74).

[63]S. Kirschen, *op. cit.*, pp. 274-283.

[64]*Ibidem.*

[65]Per una visione critica (e metaforica) del meccanismo europeo, si veda: A. Mantelero, *From "safe harbour" to "privacy shield". The "medieval" sovereignty on personal data*, in "Contratto e Impresa/Europa", 2016, n. 1.

[66]C. Focarelli, *Privacy. Proteggere i dati personali oggi*, Il Mulino, 2015, pp. 123-175.

[67]Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[68]Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Costruire un'economia dei dati europea*, cit., pp. 5-8.

[69]A tal proposito, è doveroso osservare che, nonostante il considerando 9 del Regolamento sembri accennare ad una definizione concreta della nozione di dato non personale, il suo carattere meramente esemplificativo non permette di trarre conclusioni inequivocabili al riguardo.

[70]Gli esempi riportati dalla Commissione sono quelli dei dati sulle condizioni meteorologiche prodotti da sensori o i dati sulle esigenze di manutenzione delle macchine industriali.

[71]Lo stesso documento sottolinea sin da subito il carattere puramente informativo della guida della Commissione: «Il presente documento è fornito dalla Commissione europea esclusivamente a titolo informativo. Esso non contiene alcuna interpretazione autorevole del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, né costituisce una decisione o un'opinione della Commissione europea. Tale documento non pregiudica eventuali decisioni o opinioni della Commissione europea, né le competenze della Corte di giustizia dell'Unione europea per l'interpretazione del regolamento conformemente ai trattati dell'UE».

[72]S. Stalla-Bourdillon, *A. Knight, Anonymous data v. personal data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in "Wisconsin International Law Journal", 2017, n. 2; G. D'Acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, 2017.

[73]Il GDPR, come indicato al considerando 27, esclude i dati dei deceduti dal suo ambito di applicazione ma, al contempo, permette ai singoli Stati membri di adottare una scelta differente, disciplinando questo tipo di informazioni alla stregua di quelle a carattere personale (come avviene in Italia, ex art. 2-terdecies, d.lgs. 30 giugno 2003, n. 196). Di fatto, la discrezionalità riconosciuta ai singoli legislatori nazionali, legittimando una classificazione normativa differente dello stesso tipo di informazione, potrebbe portare alla creazione di ambiti normativi non totalmente coincidenti all'interno dell'unico ordinamento giuridico europeo.

[74]S. Calzolaio, voce *Protezione dei dati personali*, cit., pp. 605-608; S. Forge, *Optimal scope for free-flow of non-personal data in Europe*, IPOL, 2016, p. 1-6; I. Grae, R. Gellert, M. Husovec, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation*, in "European Law Review", 2019, n. 5, p. 605-621.

[75]M.L. Montagnani, *op. cit.*, pp. 304-310.

[76]European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 15-16. In particolare: «Il regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea non riguarda gli obblighi di localizzazione di dati imposti dagli Stati membri sull'archiviazione dei dati non personali in un paese terzo, che possono essere presenti negli ordinamenti giuridici nazionali».

[77]*Parere del Comitato economico e sociale europeo (CESE) sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, p. 6. In particolare: «Inoltre, la proposta della Commissione non tiene debito conto della natura globale e transeuropea dell'economia digitale e si preoccupa solo di regolamentare il mercato interno, dimenticando che quest'ultimo si sviluppa in un mercato globale, senza alcuna garanzia che gli altri paesi e continenti seguano le stesse regole che essa stessa intende attualmente applicare e senza il potere di imporle nei negoziati internazionali».

[78]Regolamento (UE) 2018/1807, considerando n. 4.

[79]La figura dell'"utente professionale" è definita dal punto 8, dell'articolo 3 del Regolamento come: «una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati per fini connessi alla sua attività commerciale, industriale, artigianale, professionale o a una sua funzione».

[80]Regolamento (UE) 2018/1807, considerando n. 6.

[81]European Commission, *Staff working document impact assessment, Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"* - SWD (2017) 304 final, part 1/2.

[82]L'articolo 4, rubricato *Libera circolazione dei dati all'interno dell'Unione*, al paragrafo 1 stabilisce: «Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Il primo comma del presente paragrafo fa salvo il paragrafo 3 e gli obblighi di localizzazione dei dati stabiliti sulla base del diritto vigente dell'Unione».

[83]Regolamento (UE) 2018/1807, art. 3, punto 5.

[84]European Commission, *Commission staff working document impact assessment. Accompanying the document "Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union"*, cit.

[85]European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Questo studio molto approfondito identifica gli obblighi di localizzazione che si possono trovare in alcuni Stati membri dell'Unione europea, p. 18.

[86]A titolo esemplificativo, possono essere citate due fra le più recenti barriere dirette introdotte dal legislatore italiano. La prima è contenuta nel d.l. 21 settembre 2019, n. 105,

recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica» convertito in l. 18 novembre 2019, n. 133, il quale, tramite la creazione di un perimetro di sicurezza nazionale cibernetica, potrebbe limitare la circolazione di informazioni inerenti all'esercizio di "una funzione essenziale dello Stato" oppure alla "prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale». La seconda barriera, invece, può rinvenirsi nell'art. 6 del d.l. 30 aprile 2020, n. 28 convertito in l. 25 giugno 2020, n. 70, recante «Misure urgenti per l'introduzione del sistema di allerta Covid-19», che istituisce una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti che usufruiscono della app "Immuni". Per un approfondimento, si rinvia a S. Calzolaio, *Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020*, in E. Calzolaio, M. Meccarelli, S. Pollastrelli (a cura di), "Il diritto nella pandemia. Temi, problemi, domande", Macerata EUM, 2020.

[87] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. Lo studio tiene comunque a precisare che le barriere indirette sono state considerate tali alla luce delle valutazioni fatte da esperti del settore.

[88] *Ivi*, p. 6.

[89] *Ibidem*.

[90] *Ivi*, p. 103. Nello specifico, lo studio recita: «More numerous were the indirect data location requirements, which included the accessibility of data to specific supervisors or regulators, the definition of generic technical requirements, prior authorisation schemes for infrastructure or service providers, the mandatory use of a specific infrastructure, data segregation requirements, subcontracting restrictions, and data destruction requirements».

[91] Merita evidenziare che, mentre il Regolamento generale sulla protezione dei dati personali ha come base giuridica l'articolo 16 TFUE, il Regolamento relativo alla libera circolazione dei dati non personali è stato adottato sulla base dell'articolo 114 TFUE, il quale attribuisce al Parlamento ed al Consiglio la competenza ad adottare «le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno».

[92] Regolamento (UE) 2018/1807, considerando n. 4. In particolare: «Il presente regolamento non limita in alcun modo la libertà delle imprese di stipulare contratti che stabiliscano dove devono essere localizzati i dati. Il presente regolamento è inteso unicamente a salvaguardare tale libertà garantendo che il luogo stabilito possa trovarsi ovunque nell'Unione».

[93] Regolamento (UE) 2018/1807, considerando n. 14. In particolare: «Mentre le autorità pubbliche e gli organismi di diritto pubblico sono incoraggiate a considerare i vantaggi economici e di altro tipo dell'esternalizzazione a fornitori esterni di servizi, essi potrebbero avere ragioni legittime per scegliere l'autofornitura di servizi o l'internalizzazione. Di conseguenza, il presente regolamento non obbliga in alcun modo gli Stati membri a subappaltare o esternalizzare la fornitura di servizi che essi intendono fornire direttamente o organizzare con mezzi diversi dagli appalti pubblici».

[94] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit. p. 17. In particolare: «These barriers can of course take many forms. In some cases, there is a clear and objective compliance requirement behind them, such as a legal obligation to store data locally in order to maintain national control over essential systems and services. In other cases, a barrier can result from business requirements (e.g. customer demand to store data locally), policy preferences (e.g. a desire to keep data within one's own jurisdiction), operational needs (e.g. a requirement to be able to destroy data), or even personal preferences (e.g. favouring local companies) and personal concerns (e.g. concern that foreign entities may seize data stored abroad)».

[95] IDC, Open Evidence, *European data market study*, Final Report (SMART 2013/0063), 2017.

[96] M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel, *Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states*, cit.

[97] Regolamento (UE) 2018/1807, considerando n. 10. In particolare: «Il regolamento (UE) 2016/679 e il presente regolamento forniscono un insieme coerente di norme che disciplinano la libera circolazione di diversi tipi di dati».

[98] La proposta congiunta lanciata dai Ministeri dell'economia tedesco e francese di creare una infrastruttura digitale di matrice europea, denominata GAIA-X, rispondente ai valori continentali di sicurezza e tutela dei dati è evidentemente diretta a ridurre la dipendenza nei confronti dei fornitori di servizi non europei e ad incentivare la concorrenza. In tal senso, *GAIA-X: A pitch towards Europe. Status report on user ecosystems and requirements*, Federal Ministry for Economic Affairs and Energy (BMWi), 2020.

[99] La predisposizione di una piattaforma unica nazionale per la gestione del sistema di allerta degli utenti della app "Immuni" nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19 rappresenta una chiara presa di posizione da parte del legislatore italiano, il quale ha preferito una soluzione con titolarità pubblica e con infrastrutture localizzate sul territorio nazionale. Per un approfondimento, si rinvia a: C. Colapietro, A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in "Dirittifondamentali.it", 2020, n. 2.

[100] A tal proposito, eloquente è il caso dei *Community Mobility Reports* messi a disposizione da Google per fornire una panoramica della variazione degli spostamenti della popolazione durante la pandemia causata dal Covid-19, i quali dimostrano quanto sia pervasiva e vasta la raccolta e l'analisi dei dati realizzata dai servizi OTT.

[101] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21. La medesima procedura è prevista al paragrafo 2 nell'eventualità in cui gli Stati intendano introdurre un nuovo obbligo dello stesso tenore.

[102] Regolamento (UE) 2018/1807, art. 4, par. 3 e cons. 21.

[103] Per le sentenze della Corte di giustizia dell'Unione europea più rilevanti a tale riguardo, si rinvia alla European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 13.

[104] M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in "federalismi.it", 2016, n. 23.

[105] Regolamento (UE) 2018/1807, considerando n. 19. A tale riguardo, il rischio di difformità nelle normative degli Stati membri che potrebbe derivare da questa facoltà di deroga si aggiunge a quello dovuto alla scelta, da parte del legislatore, di ricorrere allo strumento della direttiva per disciplinare il trattamento dei dati personali effettuato da autorità pubbliche in ambito penale. In particolare, ci si riferisce alla Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali

ed alla Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[106] L. Tarantino, *Promozione della concorrenza e disciplina dei servizi pubblici*, 2016, pp. 8-11; A. Di Giovanni, *I servizi di interesse generale tra poteri di autorganizzazione e concessione di servizi*, Giappichelli, 2018, pp. 1-17.

[107] European Commission, *Cross-border data flow in the digital single market: study on data location restrictions*, cit.

[108] *Parere del CESE sulla "Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"*, adottato il 25 settembre 2019.

[109] M. Nino, *Il caso "Datagate". I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in "Diritti umani e diritto internazionale", 2013, n. 3, pp. 735-737.

[110] C. Focarelli, *op. cit.*, pp. 10-16.

[111] C. Kuner, F.H. Cate, C. Millard, D.J.B. Svantesson, *Systematic government access to private-sector data redux*, in "Articles by Maurer Faculty, Indiana University", 2014, n. 4. Due eccezioni degne di nota sono quelle di Microsoft ed Apple che si sono opposte alle richieste di accesso da parte delle autorità statunitensi, si veda M. Rubechi, *op. cit.*, p. 23.

[112] Ci si riferisce all'articolo 9 del Regolamento (UE) 2016/679, rubricato *Trattamento di categorie particolari di dati personali*.

[113] Prima dell'abrogazione, la Legge n. 675 del 31 dicembre 1996 relativa alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, all'articolo 22, riportava la rubrica "Dati sensibili". Anche il Decreto legislativo 30 giugno 2003, n. 196, riportava la medesima dicitura prima della modifica ad opera del decreto legislativo 101 del 2018 relativo alle disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

[114] Un concetto simile è presente nell'ordinamento giuridico della Repubblica popolare cinese dove viene in rilievo la nozione di *important data*, la quale, benché possa comprendere sia dati personali che non, appronta una disciplina più rigida proprio in virtù della particolare importanza di queste informazioni in riferimento alla sicurezza, all'economia o alla stabilità sociale del Paese. A questo proposito, si veda Z. Yuexin, *op. cit.*, p. 159-169.

[115] Regolamento (UE) 2018/1807, considerando n. 29.

[116] European Commission, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy. Accompanying the document Communication Building a European data economy* - SWD(2017) 2 final, p. 46-49.

[117] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[118] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[119] Regolamento (UE) 2018/1807, considerando n. 30.

[120] *Parere del CESE sulla "Comunicazione della Commissione*, cit. Per un'analisi dettagliata del diritto alla portabilità che ne include gli eventuali effetti negativi, anche se con riferimento ai dati personali, si veda: P. Swire, Y. Lagos, *Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique*, in "Maryland Law Review", 2013, n. 2, p. 335-380.

[121] Nelle versioni italiane viene impiegato il medesimo termine, "portabilità", in entrambi i regolamenti.

[122] L. Miglietti, *op. cit.*, pp. 8-13.

[123] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 18-21.

[124] *Ibidem*.

[125] Il rapporto giuridico sussistente tra utente professionale e fornitore del servizio non sempre può essere declinato all'interno della dinamica titolare-responsabile del trattamento come delineata dal GDPR, poiché l'assunzione di tali ruoli ha luogo solamente se sono coinvolti (anche) dati a carattere personale.

[126] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[127] J. Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, Max Planck Institute for Innovation & Competition Research Paper No. 16-13, 2016, p. 55-66; T. Fia, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in "Nuovo Notiziario Giuridico", 2019, n. 1, pp. 125-126; *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[128] M.L. Montagnani, *op. cit.*, pp. 304-310; *Parere del CESE sulla "Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea"* - 2018/C 227/12, cit., pp. 5-6. In particolare: «In questo senso, il CESE ritiene che il regolamento all'esame dovrebbe almeno fornire un insieme di norme di base relative ai rapporti contrattuali tra i fornitori di servizi e gli utenti e prevedere una lista nera di clausole vietate a causa della limitazione del diritto di portabilità, secondo i parametri indicati in particolare nel suo parere sull'autoregolamentazione e sulla co-regolamentazione. Tuttavia, è inconcepibile che la Commissione non abbia neppure proposto di definire «orientamenti» per l'elaborazione dei codici di condotta precedentemente citati, come ha già fatto in altri settori, sostenuta in questo approccio dal CESE».

[129] Particolarmente azzeccata è l'osservazione secondo la quale è «anche dall'efficacia del Regolamento [sulla libera circolazione dei dati non personali] che si misura quella dell'intero quadro regolatorio sulla libera circolazione dei dati», in M.L. Montagnani, *op. cit.*, p. 304.

[130] Il termine "insiemi di dati misti", che compare in diversi documenti antecedenti all'approvazione del Regolamento, è stato poi ripreso dalla Commissione europea nelle Linee guida di maggio 2019.

[131] Riprendendo le parole della commissione, l'ipotesi dell'insieme indissolubilmente legato ricorre quando questo «contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile», European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 10. Regolamento (UE) 2018/1807, art. 8.

[132] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[133] Regolamento (UE) 2018/1807, art. 8.

[134] European Commission, *Communication from the Commission to the European Parliament and the Council. Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit., p. 8-11.

[135] G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in S. Sica, V. D'antonio, G.M.

Riccio, "La Nuova Disciplina Europea Sulla Privacy", Wolters Kluwer, 2016, pp. 55-78; A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in "Le Nuove Leggi Civili Commentate", 2017, 1, pp. 144-164.

[136] M. Finck, F. Pallas, *They who must not be identied – distinguishing personal from non-personal data under the GDPR*, in "International Data Privacy Law", 2020, n. 1, p. 11-36.

[137] A tal proposito, sia consentito rinviare a S. Torregiani, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18, pp. 317-341.

[138] C. Flynn, *Shortcomings of the EU proposal for free flow of data*, in "InterMEDIA", 2018, n. 4, p. 30-35.

[139] Le difficoltà insite nell'identificazione del tipo di dato che si sta trattando non permettono sempre di raggiungere un risultato esatto in senso assoluto. In proposito, S. Forge, *op. cit.*, p. 1-6.

[140] M.L. Montagnani, *op. cit.*, pp. 304-310.

[141] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

[142] *Ibidem.*

[143] Nonostante durante l'ultimo decennio si siano ritagliati uno spazio importante nell'ordinamento europeo, non è ancora chiaro quale natura giuridica debba essere riconosciuta ai codici di condotta. Le linee guida fornite dal Comitato europeo per la protezione dei dati definiscono i codici di condotta previsti dal GDPR, nello specifico all'articolo 40, come "strumenti di responsabilizzazione volontari" che possono rivelarsi utili "in quanto forniscono una descrizione dettagliata dei comportamenti più appropriati, in termini giuridici ed etici, con riguardo a un determinato settore" (così European Data Protection Board, Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679, 2019).

[144] J. Drexl, *op. cit.*

[145] M.L. Montagnani, *op. cit.*, pp. 311-313.

[146] *Parere del CESE sulla "Comunicazione della Commissione*, cit.

* * *

The European legal framework for the free flow of data. The peril of a regulatory burden

Abstract: The increase in the free flow of data due to the digitalization has been followed by an even relevant growth of data localization restrictions required by EU member States legislative or administrative measures. The European legislator, willing to build a digital single market where all data can flow freely across EU, decided to face the data localization phenomenon through many different and sector-specific interventions, mainly based on the – still blurred – distinction between personal and non-personal data. Thanks to the analysis of the main sources of the European legal framework, this paper will assess if this patchwork, chosen over an overarching approach, is the most adequate for the common European data space.

Keywords: Free flow of data – Data localization – Personal data – Non-Personal Data

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

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0028

Cross-border Data Transfer Regulation in China

Yuan Li

With the growing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being disintegrated and reshaped. It is of particular importance for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules. China keeps leveraging the data sovereignty to fasten the law-makings to support the development of critical technology in digital domains and infrastructure construction. This paper aims to systematise Chinese regulations for cross-border data exchange following the chronological order. The enacted and draft provisions as well as binding and non-binding regulatory rules are studied, and various positive dynamic developments in the framing of China's cross-border data regulation are shown. Despite certain limitations, the Cybersecurity Law, together with Civil Code and Personal Information Protection Law, demonstrates great willingness towards a stronger data protection regime and more flexible regulatory mechanism.

China – Cross-border data flow – Cybersecurity

Sommario: *1. Introduction – 1.1. Global Data Transfer – 1.2. Problem Statement – 2. The Evolution of China's Personal Data Protection Laws – 2.1. Cybersecurity Law – 2.2. Enforcement and Authorities – 3. Data Export Regulations – 3.1. Critical Information Infrastructure Data Export – 3.2. Personal Information Export – 4. Conclusion*

1. Introduction

The regulation of cross-border data transfers represents one of the greatest challenges that data protection experts and legislators are facing around the world[1]. The global data protection law regime is fragmented by the divergence among various data protection standards. The potential negative effects shall not be undermined. From the perspective of countries, the adoption of the "adequate level of protection" approach *de facto* restricts the less developed regions, especially those that have not enacted data protection laws, from entering the global data flows. It further leads to the elimination of such countries from participating in global digital trade and exacerbates the polarization of the world economy. From the perspectives of entities, particularly those in the Information Communication Technology (ICT) sector, the legal requirements set out in different jurisdictions are likely to impose additional administrative and technical burdens when conducting business internationally. The overlapping jurisdictions over various countries, cumbersome transfer assessment rules, and excessive discretionary powers of supervisory authorities have led to increased compliance costs while reducing the transaction efficiency of multinational businesses. From the perspective of data subjects, individuals' rights and

Y. Li is Early Stage Researcher in the framework of the HEART project (*HEalth related Activity Recognition system based on IoT – an interdisciplinary training program for young researchers*), at the University of Macerata (Italy). The HEART project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 766139. This article reflects only the author's view and the REA – Research Executive Agency is not responsible for any use that may be made of the information it contains.

responsibilities vary from nationality, residence, or information collection region. It is, however, contrary to the original purpose of protecting personal data while promoting data sharing.

1.1. Global Data Transfer

The benefits that can be derived from cross-border data flows are growing, while the ability of countries to reap such benefits may vary[2]. Although it is widely recognized that countries should have a common interest in facilitating cross-border data flows and reconciling different policy objectives in this field, the implementation of the free flow of cross-border data remains vague. Due to the differences lay in digital economic development, legal systems, and data sovereignty objectives, it is difficult for countries to impose effective regulations on cross-border data transfer through one's own. In contemporary legislations, a trend of preference for establishing one data flow model inside a region within a given group of countries is emerging.

Multilateral international agreement

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted by the Council of Europe in 1981 is the first and up-to-date only binding multilateral international agreement to set standards for the transborder data flows. The early version of Convention 108 provides general principles that require signatory countries not to restrict or impose any special authorisations to prevent the flow of personal data among the member states and aims to achieve greater unity between its members[3]. The Convention 108 was further developed in the Additional Protocol in 2001 to introduce the concept of an "adequate level of protection" for the intended data recipient countries that are not the signatories to Convention 108[4]. Such exporting party is also subject to exceptions where the transfer is in the need of individual's legitimate interests and public interest, or is based on authority-approved contractual clauses.

The Convention 108 is the result of the implementation of the European Convention on Human Rights with regard to privacy protection. It attempts to build consistent data protection principles to safeguard individual's rights while keeping active exchanges of such personal information across the borders. Be great as it may, the significance of Convention 108 is limited[5]. Although international agreement as an instrument for dealing with modern societal and legal topics is advantageous in terms applicable scope of the rules, enforcement and guidance, its complex and lengthy establishment procedures have slowed down the reaction time to the emerging issues in international community, especially in areas where international consensus has not yet been reached.

Bilateral international agreement

In view of the latency of the international community's cooperation in the field of cross-border personal data transfer, multiple emerging countries in digital economy have actively launched bilateral negotiations based on their own development needs. By reaching the bilateral agreement, it is provided with a legal basis for the personal data exchanges between the signatory countries. The EU-U.S. Privacy Shield Framework is an example. In 2014, being the direct response to the Snowden revelations, *Schrems I* case led to the revocation of the Safe Harbor as a valid mechanism for transfers between the EU and the U.S. by the Court of Justice of European Union (CJEU)[6]. The EU and the U.S. successfully reached the Privacy Shield Framework as the alternative, putting forward more stringent and descriptive data transfer requirements for data controllers[7]. After receiving wide critics, the EU Commission's adequacy determination for the Privacy Shield was rendered[8]. American companies may be permitted to acquire personal data from a total of 28 European countries after being registered under the Privacy Shield program and demonstrated that they fulfil the "adequacy protection" requirement by self-certify procedures. Privacy Shield Framework additionally includes verification, assessment and supervision mechanisms, as well as special rules related to arbitration procedures[9]. The bilateral agreement allows two countries to make more detailed arrangements for cross-border data transfer issues. It is advantageous in terms of negotiation efficiency and enforcement, as well as the flexibility of contents. Yet, its scope of application is limited to the jurisdictions of the two countries. For the establishment of a regional framework of personal data cross-border transfer, bilateral agreement has very limited effect on bridging different legal standards.

Soft laws

Soft laws often play important roles in encouraging reluctant states to consider and eventually agree upon policies and strategies in areas where serious differences exist. Many international organisations have issued soft laws to regulate cross-border transfer of personal data, which has given certain guidance to the national legislation and implementation. The OECD Privacy Guidelines released in 1980 serve as the first internationally agreed upon set of personal

information protection principles and focus on balancing between the needs for digital economy and the protection of individual's rights. It addressed the needs for greater efforts to tackle the global dimension of privacy through improved interoperability and provided the member states a basic framework of free flow of personal data for further negotiations. The APEC framework, published by the Asia-Pacific Economic Cooperation in 2004, is a framework to protect privacy while enable regional personal information transfers to promote consumer trust and business confidence, to lighten compliance burdens and booster digital economy. The data controllers' obligations are particularly emphasised as data subject's consent is mandatory prior to the transfer of the personal information, and the adequate level of data protection shall be guaranteed. This framework is used as a basis for the APEC Cross-Border Privacy Rules ("CBPR"). The U.S.-led CBPR system comprises Privacy Enforcement Authority, privacy certification institutions and recognized entities operating upon nine general privacy principles and a bundle of practical requirements. A joint APEC-EU working team attempts to discover more opportunities for "double compliance" via EU BCR and APEC CBPR referential[10]. Additionally, the Southern African Development Community (SADC) developed the Model Law on Data Protection in 2010 containing general data protection principles for cross-border data transfer. Notwithstanding the efforts, many African countries are still struggling with enacting laws to regulate the collecting and processing of personal information. The organisations' practices stopped at proposing a broad framework of guidance. Further discussions over effective solutions to the conflicts of applicable laws of personal data transborder regulation are needed. However, the international negotiations and corporations are worthy of recognition.

1.2. Problem Statement

China is imminently in need for a strong and more coherent data transborder flow regulatory framework, backed by transparent enforcement and legal certainty. As the world's second largest economy, China's demand for data exchange across borders has grown significantly. On one hand, cross-border e-commerce transactions reached 134.7 billion RMB (approximately 17.7 billion Euro) and is expected to reach one trillion Euro by the year 2020, accounting for 37.6% of China's total imports and exports[11]. On the other hand, technical innovations have brought unprecedented threats to privacy and data security. Furthermore, global trade and political tensions are rising. Against this background, China needs to carefully assess domestic and international economic and legal situations to create a quality strategy for cross-border data flow regulation.

China's cross-border data transfer regulation is an evolving project that still under development, with various administrative regulations and department rules mushrooming. The Personal Information Protection Law has been incorporated into the law-making plan of the 13th Standing Committee of National People's Congress, and was released with the draft for public comment on October 21, 2020. The legislators especially emphasised the protection of public interest and state security, taking into account the needs of the protection of data subject's rights, and took a reluctant position on the regulation of cross-border data transfer. *The Cybersecurity Law* (enacted in 2017) for the first time addressed data localisation and security assessment of data export requirement for Critical Information Infrastructure providers[12]. *The Civil Code of China* (adopted May 28, 2020) newly introduced greater protection of privacy rights and personal information[13]. It clarified that (i) the rights and interests of natural persons over their personal information are civil rights and private rights; (ii) the natural persons' rights to their personal information belong to personality rights; and (iii) the distinction is made between privacy and personal information. These three pieces of legislations constitute the foundation of China's personal information protection laws.

The Measures on Personal Information and Important Data Export Security Assessment (draft for comments) was released on 2017 by the Cyberspace Administration of China (CAC). It was planned to contain elements in the scope of the security assessment, such as the consent of data subject, the security protection status of data recipient, and risk of data leaving China. Upon receiving constructive criticism, the CAC updated its second version of *The Measures on Personal Information Export Security Export* (draft for comments) in 2019. One essential element – the important data – was removed while one important element – the standard contractual clauses – was introduced.

This paper aims to provide a comprehensive analysis of China's cross-border data transfer regulation. The rest of the paper is organised as follows. Section 2 demonstrates how the personal data protections laws have evolved owing to transitions in the Chinese economy with a focus on the objectives and characteristics of cybersecurity law followed by how the Cybersecurity Law (CSL) is enforced and authorities responsible for the same. Section 3 highlights

the Data Export Regulations in China, broadly classified into Critical Information Infrastructure Data Export and Personal Data Export and how the approaches vary in terms of the measures and assessments. This section is followed by the conclusion derived from this study. Notably, this paper includes important drafts of laws and regulations to demonstrate the possible future developments in China.

2. The Evolution of China's Personal Data Protection Laws

Chinese concepts of privacy and personal data protection vary through different historical periods. Most of them are rooted from Chinese traditional ethics or moral standards, and partially integrated with socialism ideology[14]. Since the economic transmission from central planned market to free market in the 1990s, Chinese communities began to experience greater variety of roles in participating economic, societal and political activities. Although traditional predominant values still hold a deep influence on people's behaviours, individualism and subjectivity have dramatically been promoted in their social life. Scrutiny and concerns over the importance of individual's privacy and protection of emerging personal data processing are ever growing. Baidu, the largest Chinese search engine provider, was sued by a consumer rights protection association for illegally collecting user data without consent[15]. Alibaba, another internet giant, was challenged by Chinese users for the misuse of their digital transaction records and social media presence on Zhima Credit (an online credit service that offers loans based on users' digital activities)[16]. The consciousness of privacy in contemporary China has been gradually expanded and individuals have raised their expectations for the right to be let alone.

Prior to the CSL, China's personal data protection policy was integrated in a number of laws and administrative rules through the protection of personal dignity and reputation. Article 28 of the Chinese Constitution provides citizens an inviolable personal dignity from "insult, defamation or false charge." Article 252 of Criminal Law (1997) prohibits any violation to the freedom of citizen's communication rights by hiding, destructing or illegally opening other's letters. Article 101 of General Principles of Civil Law (1986) confers natural person and legal person the right of reputation. The Supreme People's Court in 2001 for the first time confirmed the legal ground for claiming remedies for the damages caused by the violation of one's privacy or other personal rights.

Personal Information was firstly defined in the Notice concerning Punishing Criminal Activities of Infringement of Citizen's Personal Information in 2013, stating that "personal information includes any information that can identify the citizen's personal identity or information and data involving the citizen's personal privacy, such as name, age, ID number, and so on." In response to the rapid development of technology, Chinese authorities released over 200 pieces of laws, administrative regulations and sector-specific rules regulating the collecting and processing of personal information across domains like banking, healthcare, medical record or disease control[17]. A comprehensive framework for personal data protection laws is urgently in need.

2.1. Cybersecurity Law

In November 2016, the final legislation of Cybersecurity Law was passed by the Standing Committee of National People's Congress imposing new cybersecurity requirements on *network operators* that "own or manage networks, or provide network services." It applies to any activities related to the "construction, administration, maintenance and use of networks."[18] The CSL is up to date the highest-level legal instrument concerning personal information protection in China. Be broad as it is, three pillars constitute the substantive provisions of the Law: multi-level protection scheme, critical information infrastructure protection, and personal information protection.

2.1.1. Objectives

Article 1 of the CSL sets multiple objectives aiming to "safeguard cyberspace security, to guarantee cyberspace sovereignty, state security and social public interests, to protect legitimate interests of citizens, legal persons and other organisations, to promote the health development of informationalisation of economic society"[19]. This is aligned with the special aspect in terms of multiple objectives in Chinese law makings, particularly those areas where face most of the challenges brought by emerging issues. As this provision suggests, the objectives are to govern everything within the country's cyberspace infrastructure, ranging from internet activities to data export.

The downside is, however, observable. It is not unusual that such generality and flexibility, sometimes excessive omissions, can be found in Chinese law drafting. Coupled with a wide discretionary power conferred on lower-level competent authorities in order to implement the law, predictability and certainty of law often are compromised. Furthermore, in order to identify a complete set of independent objectives and to prioritize them, the law makers are re-

quired to hold clear concepts, logical foundations and thought-provoking procedures[20]. In China, most of the data protection rules were made in the response to an existing problem. Despite insufficient experiences in data protection law makings and "rent-seeking" among various authorities, one essential aspect is the missing of a unified value for the protection of personal information. It is yet not crystal clear in other jurisdictions as technology and law in this regime are significantly inter-dependent. Without the clear value set ahead, multiple objectives would affect the fundamental principles as well as the conceptual framework of data protection. The immediate consequence is the vague defining of rights and obligations for stakeholders involved. This echoes the lack of legal predictability and certainty.

2.1.2. Multi-level Protection Scheme

Article 21 of the CSL requires all network operators to be obliged with different security measures according to the *cyberspace Multi-level Protection Scheme* (MLPS). Under the MLPS, network operators shall safeguard the cyberspace from interference, destruction or unauthorised access, and to protect the internet data from leak or fraud. Security obligations include but not limited to (i) the establishment of the internal security management protocol; (ii) the appointment of a person in charge of security affairs; (iii) the deployment of technical measures for cyber attacks; (iv) the record of internet operation activities no shorter than six months and the response plan for security incidence; and (v) the classification of data and the backup and encryption of the important data.

The MLPS was born from the demands of the national computer system security in 1994 and thus falls under the competence scope of the Ministry of Public Security (MPS). After a series development of administrative regulations, the updated draft of *Regulation on Cybersecurity Multi-level Protection Scheme* as a milestone was released in 2018. Together with a bundle of supplementary national technical standards, the so-called MLPS 2.0 framework of cybersecurity in China is finalised[21]. The MLPS Regulation as a supporting document of Article 21 CSL defines descriptive obligations and requirements for the network operators fell under different levels of MLPS. Eleven general obligations are listed to clearly allocate the liability and to set technical and organizational security measures. Specific obligations need to be met according to the level of the network operator's activities that would affect the state and public security, scaled from 1 the least risky to 5 the most risky[22]. After being classified, which is based upon a self-assessment, the network operators are required to deploy special security measures such as personnel management, datasets backup and encryption to protect important data.

The compliance with the MLPS 2.0 will be essential for understanding the personal data export regulation in China. Not only because such compliance is mandatory, but also the second pillar of the CSL, critical information infrastructure protection, is based on the classification within MLPS.

2.1.3. Critical Information Infrastructure

Critical Information Infrastructure (CII) is a major challenge in implementing China's cybersecurity strategy and had been recurred at top-level national cybersecurity meetings. On the basis of the cybersecurity MLPS, the state implements key protections to CII which, «if destroyed, suffering a loss of function, or experiencing leakage of data, might seriously damage national security, social welfare, and public interests.» A non-exhaustive example list (including public telecommunication and information service, energy, transportation, water resources, finance, public service and e-governmental information) is given in Article 31 CSL showing the broad scope of the application of CII requirement. In principle, any network operators that being graded above level III (including level III) under the MLPS shall be regarded as CII operators.

CII operators are imposed stricter security requirements due to the nature of the data being processed. More importantly, Article 37 CSL rules that:

> «Personal information or important data that CII operator collected or generated during its operations within the territory of the People's Republic of China shall be stored within the territory of China.»

Transferring CII information outside of China is only allowed under exceptional circumstances where actual needs for business are in place and a security assessment is approved by competent authorities. Under the CSL, CII operator is the only subject-matter that is required to comply with the data localisation policy and security assessment for cross-border data transfer. However, the definitions of CII and other key concepts such as important data remain unclear.

CII is in essence a network facility, information system, digital asset, or a collection of such elements[23]. In the early stages of informationalisation, CII was considered to be part of Critical Information (CI) that was scoped clearly. With the changing of the technical landscape, sources of risks are far beyond the scope of CI, such as the attacks coming from

virtual entities, i.e. ICT or Operation Technology domain[24]. At present, large-scale network destruction of CII is a high-risk yet low-probability incident that very limited examples of CII being damaged from cyber-attacks or data leakage can be provided. Therefore, the assessment of security and risks of CII mainly reply on the experts in the domain, instead of evidences or case studies. This brought inconsistency in determining the scope of CII and eventually made it difficult to implement relevant policies. Generally, all ICT service providers fall within the scope of CII operators according to the laws, which is not efficient in the digital economic community.

2.1.4. Personal Information Protection

There is no chapter entitled "personal information protection" in the CSL, yet provisions related to the protection of personal information are scattered through this law. Chapter 4 Network Information Security covered most of the personal information protection provisions. Network operator is the core subject-matter that most of the obligations imposed upon. Data subject's rights have been conferred passively through the legal obligations for network operators, i.e. network operator shall correct or delete on the request of the data subject when the personal information are incorrect or wrongly processed.

The structure comprises basic principles for processing, legal grounds for processing and a non-exhaustive example list of prohibited conduct. Personal information can only be collected when data subject is informed and agree to the purpose and scope of the collection. The processing of personal information must follow basic principles listed in Articles 40-42, 47, 49 which share substantive similarities with the APEC privacy framework. Consent is the ONLY legal ground for processing of the personal information[25]. This is to ensure that data subject has sufficient autonomy to decide the way his or her personal data will be collected, processed and distributed. Such autonomy is endorsed by the sufficient informing requirement, meaning that only after data subject is informed of the purpose, scope and means of processing of the personal data can he or she be capable of giving the genuine consent. The network operator has to perform the information obligation before collecting the individual's personal data.

2.2. Enforcement and Authorities

The CSL's provisions relating to data privacy formed the most comprehensive and broadly applicable set of privacy rules. It acts as an umbrella that covers a bundle of administrative regulations and numerous normative texts scattered across most of the industries. To date there is no independent authority for data protection. Multiple competent authorities or supervisory authorities are in charge of the implementation and enforcement of the rules.

2.2.1. Regulatory Framework

Various types of documents have the force of law in China. Among all the legal instruments, the Constitution Law enjoys the highest primacy yet is rarely applied directly. The law made by the National People's Congress or the Standing Committee of NPC has the highest legal effect in the respective regime, such as the Cybersecurity Law.

Administrative regulations are rules promulgated by the State Council. Its legal effect is lower than the Law but higher than the Department rules. To date, two administrative regulations were issued: the *Regulation on Critical Information Infrastructure Security Protection and the Regulation on Cybersecurity Multi-level Protection Scheme*. Additionally, sector-specific administrative regulations also affect China's personal data export study, such as the *Regulation on Computer Information Security Protection and the Regulation on Human Genetic Resources Information Management*.

Department Rules are legal documents issued by the ministries and commissions under the State Council, along with other agencies with administrative functions directly under the State Council. The applicable scope is determined by the competence of the issuing government department. For example, the aforementioned *Measures on Personal Information Export Security Assessment* is a department rule issued by the CAC. To date, around 30 department rules were issued by various authorities in the field of security, data protection and export.

Judicial interpretations are the explanations to specific legal questions made by the State Supreme judicial institutions during the application of the laws. Both the Supreme People's Court and the Supreme People's Procuratorate had released interpretations relating to cases that infringe personal information.

Standards (no legal effect) are mandatory or voluntary technical standards published by the Standardisation Association of China (SAC). In Cybersecurity and Data protection fields, TC260 group under the SAC is responsible for a series of standards titled Information Security Technology that covers methodologies, definitions or scopes of the norms. Within China, national standards play an important role in implementing laws and regulations. Despite the non-compulsory nature, they are better understood as a quasi-regulation rather than a technical specification typically presented in Western context.

Since 2010, over 240 national standards in this field have been published. It is remained debatable with the necessity of such a big amount of technical standards in force.

Additionally, local regulations are directly applied within the scope of the provinces, autonomous regions and municipalities directly under the Central Government.

2.2.2. Competent Authorities

Under the CSL, different parties are in charge of specific area of works. The *State* is to (i) make cybersecurity strategies; (ii) clarify fundamental requirements and objectives of cybersecurity; (iii) guide key area cybersecurity policies and measures. Additionally, the State shall adopt measures to guarantee the cyberspace free from attacks, interferences and crimes. The *network-related industrial associations* shall provide guidance for entities' self-regulation and promote the healthy development of the industries. The *network operators* are required to fulfil obligations addressed in the CSL and to uphold societal responsibilities.

Respectively, the *Congress* is responsible for determining the scope of CII and key areas. The *Cyberspace Administration of China*, an administrative agency directly under the State Council, is in charge of the coordination and management of all cybersecurity related issues. The MIIT and MPS are responsible for supervising and managing affairs within the scope of their competence[26]. The SAC publishes national and sectoral technical standards.

The CAC, also framed as an agency directly under the Chinese Communist Party, inherently carries a heavy stroke of political colour. It is the most important supervisory authority of cybersecurity and directly reports to the State Council for managing Internet information and contents. It works independently from the Ministries of information, public security or commerce. The CAC also leads the drafting of department rules implementing the CSL. Its branches at the province level are the main enforcement institutions that supervise, investigate, and impose administrative fines.

2.2.3. Enforcement

Enforcement of the CSL and related rules in China follows a typical bottom-top approach. Supervisory authorities have broad discretionary powers as well as the competence to impose administrative fines upon entities. Overlapping areas of jurisdictions often pop up among different authorities. The CAC is responsible to coordinate all issues arise through the enforcement. Although not legally binding, the competent authorities often refer to the Information Security Technology standards when performing assessments or issuing certifications.

The supervisory authorities are actively performing their duties since the year 2015. Means of enforcement include communication with the operator, supervising the modification of business, or administrative fines and termination of the operation. A special operation targeting at illegally collecting and processing personal information through mobile applications is jointly conducted by the CAC, MIIT (Ministry of Industry and Information Technology of the People's Republic of China) and SPS.

It is rebuttable that the CAC has the competence in imposing administrative fines. According to the Organic Law of the State Council, the CAC is not one of the departments under the State Council. The legal ground for the CAC should be Article 11 of the Organic Law of the State Council ruling that "the State Council can establish agencies directly under the Council for managing specific affairs or assisting the Primer to handle specific affairs". However, it is not explicitly informed that which agency the CAC is established for. The official documents issued by the later agencies are categorised as "other kind of administrative documents" which cannot be enforced as the basis for administrative fines[27].

According to the CSL, it is clear that the responsibilities of the CAC is coordination and supervision. Therefore, the rules and measures issued for imposing fines might not be legitimate, even their legal effect could be challenged (emphasis mine). Such gap originated from the boost of cybersecurity legislations, and shall be bridged in the future law makings. With the working-in-progress Personal Information Protection Law, the CAC is expected to (i) remain as an agency under the CCP for supervising the Internet affairs, and the national independent Data Protection Authority is formed for data protection regulation; or (ii) be conferred the legitimacy under the new law.

3. Data Export Regulations

3.1. Critical Information Infrastructure Data Export

The starting point for the study of personal data export is to define the CII operator. Quoting the data localisation requirement discussed in 2.2.3, any personal information or important data that are involved in CII shall not be transferred abroad unless a security assessment is conducted with the supervisory authorities' approval.

Defining CII

On 11 July 2017, the CAC released the draft for comments *Regulation on Critical Information Infrastructure Security Protection* (CII Regulation). Aligned with the CSL, the scope of the CII shall be determined by a two-step test: (i) if business falls within the industry or sector listed in the Regulation; and (ii) if the business is graded security level 3 or above as demonstrated in Table 1.

Table 1: Security levels under the Regulation on Cybersecurity Multi-level Protection Scheme

Subject-matter of the infringement	Severity of damage		
	Harm	Serious Harm	Particularly serious harm
Legitimate interests of citizens, legal persons or other organisations	I	II	III
Social order and/or public interest	II	III	IV
State security	III	IV	V

Additionally, the CAC's Guidelines on State Cybersecurity Inspection (no legal effect) proposed three aspects to help self-evaluating the CII:

1. key business domain, e.g., data centre cloud service, domain name resolution service, or voice data internet basic network and hub in Telecommunication sector;
2. information system or industrial control system that supports the key business, e.g., generator set control system or information management system;
3. quantity of CII device, e.g., registered users above 10 million, or active users above 1 million, or daily transaction exceeds 10 million RMB for a platform service.

Defining CII operator

The rules apply to registered entities operating inside the territory of the PRC, as well as those which do not register inside China but offer business and services to Chinese customers. The criteria to determine whether the entity provides business or service in China include: (i) using RMB as currency; (ii) using Chinese as the language; and (iii) delivering goods to China. Any of the abovementioned criteria is sufficient to lead multinational companies to store the collected personal information and important data inside China.

3.2. Personal Information Export

3.2.1. Personal Information

Personal Information is defined as "any information that is recorded, electronically or by other means, can be used or in combination with other information to identify the identity of a natural person" (Art. 76(5) CSL; Art. 4 Personal Information Protection Law (draft)). It is a commonly adopted "capacity to identity" methodology.

In the Information Security Technology – Personal Information Security Specification 2017, based on the definition given in the CSL, this standard enlarged the scope by using a very expansive wording: "any information recorded electronically or by other means". This targets all operators from both public and private sector, as well as all collecting and processing activities of personal data they conduct. Furthermore, the standard added that "personal information is ... or any information that can reflect a specific natural person's activities". This may be consistent with the broad interpretation of personal data held by the CJEU.

Important Data has been repeatedly addressed in the CSL. It is of crucial importance for assessing CII and CII data export requirement, yet surprisingly not defined in the law. The draft of Information Security Technology – Data Export Security Assessment Guidelines (the Guidelines) defines important data as "raw data and inferred data collected or generated by entities, organisations and individuals inside of China, that do not involve national secrecy, but are closely related to state security, economic development or public interests". Publicly accessible government information is excluded from the scope of important data. An index for determining important data is attached with this standard, comprising of 27 main categories and 223 sub-categories. The categorisation is similar to the U.S. Controlled Unclassified Information (CUI) system.

3.2.2. Measures on Personal Information and Important Data Export Security Assessment 2017

On 11 April 2017, the CAC circulated the draft for public comments entitled "Measures on Personal Information and Important Data Export Security Assessment" (the 2017 Measures). Unlike the CSL, the 2017 Measures expand the subject-matter of Article 37 CSL from "CII providers" to "network operators". Under the CSL, any owners or managers of networks and network service providers are defined as network operators. It is disappointing since the main issue

that practitioners were expecting from the 2017 Measures is to distinguish between the CII operator and the ordinary network operators. A clear definition of important data is also missing, only stated that "data closely related to state security, economic development and societal public interests." It further cited the Guidelines as the reference.

Being the first legislation concerning data export regulation of China, the 2017 Measures provided guidance to assess the necessity of the export and data that are prohibited from exporting. Security assessment is classified into self-conducted and authority conducted. Data that do not exceed the benchmark (500,000 pieces of personal information/1,000 GB data/important domains) can be exempted from administrative procedures of approval. Unfortunately, all essential issues were kept untouched, or otherwise worded vaguely, making it very difficult to comment.

3.2.3. Measures on Personal Information Export Security Assessment 2019

After receiving a large number of public comments, the CAC published the second draft titled "Measures on Personal Information Export Security Assessment" (the 2019 Measures). As its name suggests, the 2019 Measures only apply to personal information. The legal requirements set out in the 2019 Measures are significantly more onerous than the 2017 Measures. Within two-year considerations, the legislators demonstrated observable preference in data export regulation approach.

Data localisation

The 2019 Measures require all personal information to be stored domestically for security assessment before being provided to recipients outside of China[28]. Two aspects are implied: all personal information need to be locally stored; and all personal information exports need to go through security assessment.

While data localisation is gradually adopted in international data regulation standards, one shall notice that data localisation does not necessarily mean the restrictions over cross-border data flows. Either the EU GDPR or the U.S. CUI system both emphasise that data localisation, backed with transparent regulatory rules, can reconcile the objectives of safeguard state security and personal rights and free flow of data across borders, which are of equal importance. The 2019 Measures itself aims to functioning as a precise and predictable mechanism for cross-border personal data transfer.

Security assessment

Network operators shall submit the applications for a clearance for the personal information export to the province-level Cyberspace Administrations after a transfer contract is signed with the recipient. The supervisory authority after received the application shall conduct security assessment based on the submitted documents, and to complete it within 15 working days, with the possibility of extensions depending on the complexity of the export.

The security assessment focuses on (i) legal compliance; (ii) protection of data subject's rights; (iii) enforceability of the transfer contract; and (iv) the recipient's record on whether it had infringed data subject's rights or had security incidence. When serious data leakage or data misuses occur, the data subjects are unable to protect their legitimate interests, or the parties are unable to provide protection of the personal information, the authority can request the network operator to pause or terminate the transfer. The security assessment shall be performed at least once per two years. When the substantive factors, such as the purpose of transfer or the retention period, have changed, a new application of assessment shall be submitted.

Standard contractual clauses

The requirement of the legally-binding contractual agreement between the network operator and the recipient is probably the biggest surprise in the 2019 Measures. This so-called transfer contract is the EU Standard Contractual Clauses alike, taking into consideration the limitation of territorial jurisdiction, recognises *inter partes* autonomy.

The contractual clauses are required to include: (i) the purpose, type and retention period of the personal information export; (ii) the data subject is the beneficiary of the clauses involving data subject's interests; (iii) the legal ground for the data subject to claim for remedies when infringement occurs; (iv) when the recipient is unable to perform the contract due to its state's legal environment changed, the contract shall be terminated or re-assessed; and (v) the termination of the contract shall not exempt the obligations involving the legislative interests of the data subject, unless the personal information is destroyed or anonymised. The 2019 Measures further clarifies the contractual obligations of network operator and recipient, respectively.

The adoption of standard contractual clauses integrates the regulatory requirements into contract autonomy. It is expected to indirectly abide offshore entities by the China's standard. This approach largely depends on the supervision of the

post-transfer performance of the parties. Considering that China is still waiting for her own Personal Information Protection Law, it is more likely that China's personal data protection and cross-border transfer regulation will be tilted towards the European standard. On the other hand, there is no clear line between personal information and important data. Important data naturally could contain a large amount of personal information. The regulation on important data and important data export is waiting for the other boot to drop.

3.2.4. Personal Information Protection Law (draft)

On 21 October 2020 the Legislative Affairs Commission of the Standing Committee of the National People's Congress released the draft of Personal Information Protection Law (the PIPL) and invited for public comments. Different from the 2019 Measures, the PIPL draft does not require all kinds of personal information transborder activities to be examined through the security assessment.

Derogations

Cross-border transfer of personal information is by default not allowed, unless at least one of the derogations is granted:

1. Where the amount of personal information being processed reaches the threshold for CAC security assessment, the personal information processor shall firstly store the personal information inside China. Such personal information can only be transferred outside of China after the security assessment being conducted and approved by the CAC[29].
2. Prior to the cross-border transfer, the processor shall provide the data subject with information including the identify and contact of the recipient, purpose and means of processing, types of personal information, and means for data subject to implement the rights. The transfer is allowed when the individual's consent is obtained[30].
3. A personal information protection certificate issued by a CAC-recognised organisation[31].
4. Contractual obligations over the recipient with regard to the personal information protection[32] (similar to the contractual clauses described in Sec. 3.2.2).

Restrictions

For the concerns of the protection of China's data subjects and data sovereignty in the global data governance, as well as to achieve a delicate balance in international relations, the PIPL draft for the first time introduced restrictions and countermeasure clauses over personal data. The measures embodied a "black list", on which the subjects to the restrictions or countermeasures will be included in the list that personal information transfer is restricted or prohibited. The applicable conditions of restrictions and countermeasures have also been strictly limited. The subjects to the restrictions include foreign institutions or individuals engaged in personal information processing activities that (i) damage the rights of Chinese data subjects; and (ii) endanger China's national security and public interests[33]. The subjects to the countermeasures are countries or regions that impose discriminatory restrictions, prohibitions or similar measures on China[34].

DPIA requirement

Data protection impact assessment (DPIA) is one of the most important means for the continuous and autonomous operation of the compliance operations that personal information processors shall demonstrate and/or self-certify. Prior to the Personal Information Protection Law, DPIA is recommended via non-mandatory technic standards. For the first time DPIA is ruled as a legal compliance that more stringent requirements have been put forward for the establishment of an organisation's internal compliance system. Specifically, the DPIA is required when personal information are transferred to a recipient that is located outside of China. A period of minimum three years has been proposed as the retention time for keeping the result of the DPIA and the record of the processing[35].

Transfer by national agencies

The access and transfer of personal information are possible based on the request for international judicial assistance. Where national agencies need to transfer personal information abroad, special laws and regulations shall be complied with[36].

4. Conclusion

With the increasing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being broken and reshaped. It is particularly important for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules.

China keeps leveraging the data sovereignty to fasten the law makings to support the develop-

ment of critical technology in digital domains and the infrastructure construction. The cross-border data transfer regulation prefers a strict unidirectional data flow administration that focuses on controlling the flow of the data being transferred outside of China. The regulation is largely orientated by the CAC agencies, which weakens the autonomy for individuals and entities in terms of self-governance and enforcement. It is better to objectively value the importance of efficiency in digital economy and to avoid the excessive rigid adherence to traditional sovereignty, of which, the data localisation requirement as the strongest manifestation of data sovereignty is imposed.

In practice, either the "common European data space" proposed by the European Data Strategy, or the "certified governments" recognized by APEC CBPR system are both an attempt to establish cross-border judicial corporation frameworks among trusted entities for the application of rules and efficient enforcement. However, China has not established a mutual trusted mechanism for transborder data flow with other countries. The proposed initiatives largely remain at the conceptual level without practical operability.

Despite the limitations, there are various positive dynamic developments in the framing of China's cross-border data regulation. The CSL, together with Civil Code and Personal Information Protection Law demonstrate great willingness towards a stronger data protection regime and more flexible regulatory mechanism. By introducing contractual obligations and statutory derogations while strengthening domestic personal data protection standard, it is observable that China's legislation is continually moving towards the European approach. Given the fact that countries are unlikely to form a corporation framework in a short period, cross-border data transfer between China and the EU would be profoundly rooted in bilateral and multilateral trade and investment negotiations.

Notes

[1]There is a lack of clarity as to the meaning of the term "cross-border data transfer" even inside one jurisdiction, and often regulatory instruments use different definitions to apply the measures. The EU General Data Protection Regulation (GDPR) refers to "transfer to a third country of personal data" (recital 153) without defining "data transfer"; the APEC Privacy Framework variously uses the terms "international transfer", "information flows across borders", cross-border information flow" and "cross-border data transfer" interchangeably to refer to the movement of personal data across national borders. The OECD Privacy Guidelines refer to "transborder data flows", defining the term as "movements of personal data across national borders" (Section 1(c)), while the Convention 108 refers to "transborder flows of personal data", defined as "the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed" (Article 12(1)). It is also unclear whether merely making personal data accessible should be considered to result in such a transfer, or whether this requires some active or automatic transmission of the data (see Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971). In this article, cross-border data flow and transborder data flow are interchangeable, based on the context as well as the specific document it is referred to.

[2]See OECD, *Declaration on Transborder Data Flows*, 1985.

[3]See Council of Europe, *Details of Treaty No.108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1985.

[4]See Council of Europe, *Details of Treaty No.181. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, 2004.

[5]Limited signatory countries, overbroad content and free applicable scope eliminate the practical performance of the Convention 108. Additionally, International Law Commission listed "protection of personal data in the transborder flow of information" in its long-term working programs as early as 2006, yet fruitless so far. See *Report of the International Law Commission Fifty-eighth session (1 May-9 June and 3 July-11August 2006)*, p. 489.

[6]The CJEU found that the U.S. government permitted generalized access to electronic information and failed to provide redress mechanisms. Therefore, the CJEU determined that the U.S. law did not provide an adequate level of protection essentially equivalent to EU laws. See *Schrems v. Data Protection Commissioner*.

[7] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM/2015/0566 final.

[8]Digital Rights Ireland brought the first challenge on 2016, seeking the annulment of the determination on the basis that the Shield failed to provide sufficient substantive changes from the Safe Harbor Framework. This challenge was dismissed for lack of admissibility. French advocacy group La Quadrature du Net also challenged the Commission's decision arguing that the Shield not only continues to violate the Charter, but also fails to provide effective redress mechanisms. This case remains pending.

[9]Similarly, the U.S. also reached Swiss-U.S. Privacy Shield Framework with Switzerland.

[10] The Referential for Requirements for Binding Corporate Rules (BCR) and APEC Cross Border Privacy Rules system serves as an informal checklist for companies to apply certifications under the BCR and CBPR system. The referential outlines common compliance requirements and ad hoc requirements for each of the systems. Although the referential was superseded after the enactment of the GDPR in 2018, EU representatives have continued to express a strong interest in developing a work plan for future efforts. See Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents.

[11]See Ministry of Commerce of PRC, *Report on E-Commerce in China*, 2018.

[12]The *Cybersecurity Law*, 2017.

[13]«The personal information of a natural person shall be protected by law. Any organization or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. Any illegal collection, usage, processing, and transfer of the individual's personal information, or illegal trade, making available or disclosure of other's personal information is the violation of law.» Article 111 Civil Code of the People's Republic of China.

[14]See B.S. McDougall, A. Hanson (eds.), *Chinese Concepts of Privacy*, Brill, 2002, p. 8.

[15]See M. Jing, *China consumer group accuses Baidu of snooping on users of its smartphone apps*, 2018.

[16]See X. Wang, *Zhima Credit apologizes for its annual report's "mistake"*, 2018.

[17]China provides direct protection of personal information through The Seventh Amendment of Criminal Law, Tort Law, Telecommunication Law, Junior Protection Law, Consumer Protection Law, etc. Indirect protection of personal information is provided though Constitution Law and Civil Law. For example, the Ministry of Industry and Information Technology is in charge of regulating the ISPs via *Measures on Protecting Personal Information of Telecommunication and Internet Users, Measures on SMS service management*, etc.

[18]*Cybersecurity Law* (n12), Article 2.

[19]*Ivi*, Article 1.

[20]See R.L. Keeney, *Identifying, prioritizing, and using multiple objectives*, in "EURO J Decis Process", 2013, n. 1, p. 45-67.

[21]The three newly released national standards are: (1) GB/T 22239-2019 *Information Security Technology-Basic Requirements for the Multi-level Protection*, (2) GB/T 25070-2019 *Information Security Technology- Cybersecurity Multi-level Protection Security Design Technical Requirements*, and (3) GB/T 28448-2019 *Information Security Technology-Cybersecurity Multi-level Protection Assessment Requirements*, which was into force on 1 December 2019. Another national standard titled GB/T 25058-2019 *Information Security Technology-Implementation Guide for Cybersecurity Classified Protection* comes into effect on 1 March 2020.

[22]For the description of the security levels, see Table 1.

[23]CAC, *National Cyberspace Security Strategy*, 2016 (unofficial English translation). See also, Title VII, the USA PATRIOT Act, 2001; M.P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, National Institute of Standards and Technology of the U.S., 2018.

[24]For example, some malware target industrial operation system in electricity, gas, or chemical plants, while some cyber attacks target the control or tampering of information and data.

[25]*Cybersecurity Law* (n12), Article 41.

[26]*Ivi*, Article 8.

[27]*Law of the People's Republic of China on Administrative Penalty*, 2018, Article 14.

[28]*2019 Measures*, Article 2.

[29]*Personal Information Protection Law* (draft), Article 38(1) and Article 40.

[30]*Ivi*, Article 39.

[31]*Ivi*, Article 38(2).

[32]*Ivi*, Article 38(3).

[33]*Ivi*, Article 42.

[34]*Ivi*, Article 43.

[35]*Ivi*, Article 54.

[36]*Ivi*, Article 41.

* * *

La disciplina cinese del trasferimento transfrontaliero dei dati

Riassunto: In virtù della crescente partecipazione dei paesi emergenti alla governance globale dei dati, il paradigma normativo tradizionale dominato dall'Unione Europea e dagli Stati Uniti viene costantemente disintegrato e rimodellato. È di particolare importanza per la Cina stabilire il quadro normativo del trasferimento transfrontaliero dei dati, poiché non solo coinvolge i diritti dei cittadini e delle istituzioni cinesi, ma anche la sovranità digitale e la sicurezza nazionale, nonché la definizione delle regole globali del cyberspazio. La Cina continua a far leva sulla sovranità dei dati per consolidare i processi di produzione di norme a sostegno dello sviluppo di tecnologie critiche in domini digitali e della costruzione di infrastrutture. Questo articolo mira a fornire una analisi sistematica delle normative cinesi relative allo scambio transfrontaliero dei dati. Vengono analizzate sia le disposizioni già adottate sia quelle in corso di adozione, come anche le norme vincolanti e quelle non vincolanti; vengono inoltre evidenziati gli sviluppi positivi verso la definizione in Cina di un quadro regolatorio del flusso transfrontaliero dei dati. Nonostante alcune limitazioni, la legge sulla sicurezza informatica, insieme al codice civile e alla legge sulla protezione dei dati personali, dimostra un forte orientamento verso un regime di protezione dei dati più forte e un meccanismo di regolamentazione più flessibile.

Parole chiave: Cina – Circolazione transfrontaliera dei dati – Sicurezza informatica