UNIVERSITÀ
DI TRENTO
Facoltà di
Giurisprudenza

NUMÉRIQUE & ENVIRONNEMENT

Université d'été franco-italienne
Actes du colloque
6-8 Juillet 2022
Université de Limoges

a cura di
LUISA ANTONIOLLI
MONICA CARDILLO
FULVIO CORTESE
LOUIS DE CARBONNIÈRES
FRANTZ MYNARD
CINZIA PICIOCCHI

2024

UNIVERSITÀ
DI TRENTO
Facoltà di
Giurisprudenza

QUADERNI DELLA FACOLTÀ DI GIURISPRUDENZA

79

2024

Al fine di garantire la qualità scientifica della Collana di cui fa parte, il presente volume è stato valutato e approvato da un *Referee* interno alla Facoltà a seguito di una procedura che ha garantito trasparenza di criteri valutativi, autonomia dei giudizi, anonimato reciproco del *Referee* nei confronti di Autori e Curatori.

ISBN 978-88-5541-065-6
ISSN 2284-2810

Maggio 2024

NUMÉRIQUE & ENVIRONNEMENT

Université d'été franco-italienne
Actes du colloque
6-8 Juillet 2022
Université de Limoges

a cura di
LUISA ANTONIOLLI
MONICA CARDILLO
FULVIO CORTESE
LOUIS DE CARBONNIÈRES
FRANTZ MYNARD
CINZIA PICIOCCHI

Università degli Studi di Trento 2024

INDICE

Pag.

Pag.

Pag.

PARTE I

L'ÉTAT FACE AU NUMÉRIQUE: LES DÉFIS DU XXIE SIÈCLE

OSSERVAZIONI SUL CLOUD COMPUTING E SULLA "SOVRANITÀ DIGITALE" NELLA PROSPETTIVA DEL DIRITTO INTERNAZIONALE

Antonino Alì[*]

SOMMARIO: *1. Gestione dei dati e sovranità nazionale in un mondo interconnesso. 2. L'accesso transfrontaliero ai dati: una sfida per il diritto internazionale. 3. Microsoft Corp. v. United States of America. 4. Il Cloud Act. 5. La localizzazione forzata dei dati nel territorio dello Stato. 6. La narrativa della protezione della privacy quale driver della localizzazione forzata dei dati nel territorio dello Stato.*

Riassunto

Nonostante l'avvento del cloud computing, la sovranità nazionale rimane cruciale per la gestione dei dati. Molti stati hanno introdotto normative al fine di controllare i dati all'interno dei propri confini, mettendo in discussione la libera circolazione dei dati su Internet. Ciò solleva delle questioni relative all'equilibrio fra sovranità nazionale, privacy e sicurezza. La collocazione dei data center è influenzata da una serie di fattori, incluse la legislazione e la stabilità politica. Gli stati devono bilanciare la protezione nazionale dei dati con la necessità di innovazione e di cooperazione internazionale.

Abstract

Despite the advent of cloud computing, national sovereignty remains central to data management. Many states have introduced laws to control data within their borders, challenging the free movement of data on the Internet. This raises questions about the balance between national sovereignty, privacy and security. The location of data centers is influenced by a number of factors, including legislation and political stability. States must balance national data protection with the need for innovation and international cooperation.

Résumé

Malgré l'avènement de l'informatique en nuage, la souveraineté nationale reste au cœur de la gestion des données. De nombreux États ont adopté des

[*] Professore associato di Diritto internazionale, Facoltà di Giurisprudenza, Università di Trento.

lois visant à contrôler les données à l'intérieur de leurs frontières, remettant en cause la libre circulation des données sur l'internet. Cela soulève des questions sur l'équilibre entre la souveraineté nationale, la protection de la vie privée et la sécurité. La localisation des centres de données est influencée par un certain nombre de facteurs, notamment la législation et la stabilité politique. Les États doivent trouver un équilibre entre la protection des données nationales et le besoin d'innovation et de coopération internationale.

1. Gestione dei dati e sovranità nazionale in un mondo interconnesso

Il *cloud computing* ha rivoluzionato il modo in cui le attività informatiche vengono svolte, offrendo agli utenti un facile accesso a risorse di calcolo, archiviazione e applicazioni attraverso internet. Inoltre, l'aumento della domanda di potenza di calcolo e i limiti delle tecniche di calcolo tradizionali hanno reso il *cloud* un elemento indispensabile. La proliferazione dei *data center* e delle *web farm* interconnesse alla rete ha favorito lo sviluppo del *cloud computing* e ha portato a un aumento significativo dei dati conservati a distanza. Tuttavia, questa modalità presenta delle sfide per gli Stati nel mantenere il controllo esclusivo all'interno dei propri confini, dal momento che i dati possono essere accessibili, processati e conservati al di là delle frontiere nazionali.

È quindi cruciale stabilire un equilibrio tra la protezione della sovranità statale e l'incoraggiamento di un flusso libero e sicuro dei dati, nonché la condivisione trasparente di informazioni a livello globale. La necessità di servizi di *cloud computing* efficienti e affidabili solleva anche preoccupazioni sulla protezione dei dati[1] e, più in generale, sull'esercizio del potere da parte degli Stati[2]. Questo fenomeno ha progressivamente indebolito l'esercizio del potere da parte degli Stati, poi-

[1] Così, V. NARAYANAN, *Harnessing the Cloud: International Law Implications of Cloud-Computing*, in *Chicago Journal of International Law* 12(2), Article 11, 2012, p. 783 ss.

[2] Per un'analisi complessiva vedi G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, pp. 87-119; ID., *Il ruolo del consenso del sovrano territoriale nel transborder data access tra obblighi internazionali e norme interne di adattamento*, in *La Comunità internazionale*, 2016, p. 183 ss.

ché i dati e i centri di controllo della rete sono dispersi in tutto il mondo, oltre i confini nazionali.

In un mondo sempre più globalizzato e interconnesso, la maggior parte degli Stati cerca di esercitare uno stretto controllo sulle informazioni relative a individui e aziende che ricadono nel proprio territorio. La crescente circolazione di dati attraverso Internet e la loro distribuzione su territori appartenenti a più Stati rappresenta una sfida all'*imperium* statale, di conseguenza, a uno dei pilastri fondamentali del diritto internazionale: la sovranità[3].

Nonostante l'apparente natura senza confini della "nuvola"[4], il territorio statale gioca ancora un ruolo significativo. Negli ultimi anni, sono numerosi gli Stati che hanno introdotto normative volte ad assicurare che la gestione dei dati avvenga entro i loro confini. Questi atti sono generalmente motivati dalla volontà di mantenere un controllo sulle attività esercitate sul proprio territorio.

La posizione geografica sulla rete, l'interconnessione con le principali dorsali di traffico, il costo dell'energia, le norme regolamentari, la stabilità politica e le politiche economiche e fiscali degli Stati influenzano le decisioni su dove stabilire i *data center* e le *web farm*. La scelta della collocazione geografica diventa un fattore cruciale, poiché determina l'accessibilità, l'affidabilità e la sicurezza dei dati. La legislazione e le regolamentazioni riguardanti la localizzazione dei dati e il controllo delle informazioni diventano strumenti importanti per cercare di bilanciare questi interessi e tutelare gli interessi nazionali senza ostacolare l'innovazione e la cooperazione internazionale.

Da tempo, si è consapevoli del problema dell'accesso transfrontaliero ai dati, un'attività che coinvolge l'accesso ai dati conservati all'inter-

[3] Sul *cloud computing* e le implicazioni per il diritto internazionale v. B.J. KOOPS, M. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, Tilburg University, TILT – Tilburg Institute for Law, Technology, and Society, CTLD – Center for Transboundary Legal Development, 2014.

[4] A. REGALADO, *Who coined "Cloud computing"?*, in *MIT Technology Review*, October 31, 2011, *https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/*.

no dei confini di altri Stati[5]. La questione della localizzazione dei dati e l'evoluzione della tecnologia del *cloud computing* danno luogo a problematiche delicate[6] che mettono in discussione l'autorità e il potere degli Stati, minacciando la loro capacità di mantenere il controllo sui dati che coinvolgono i propri cittadini e le attività svolte entro i loro confini.

In generale, gli Stati manifestano una decisa avversione alle intrusioni non autorizzate nei propri sistemi informatici, interpretando tali azioni come violazioni della propria sovranità e dell'ordine giuridico interno. Questo disappunto non è meramente espresso in termini astratti, ma è enfatizzato ancor più quando le operazioni in questione sono eseguite sul territorio nazionale da altri Stati. Si tratta di fenomeni che generano questioni rilevanti per il diritto internazionale e che possono portare a tensioni diplomatiche e, in casi estremi, possono aprire la strada a controversie internazionali.

Il diritto internazionale e il diritto europeo offrono un quadro normativo complesso e non sempre chiaro. La complessità della questione è accresciuta dalla sovrapposizione di normative, principi e interpretazioni giuridiche, richiedendo un'analisi accurata che consideri non solo il diritto positivo, ma anche le dinamiche geopolitiche in gioco[7].

---

[5] V. A.M. Osula, *Accessing Extraterritorially Located Data: Options for States*, NATO Cooperative Cyber Defence Centre of Excellence, Tallin, Estonia, 2015; Id., *Transborder access and territorial sovereignty*, in *Computer Law & Security Review* 31(6), 2015, p. 719 ss.; W. Maxwell, C. Wolf, *A Global Reality: Governmental Access to Data in the Cloud. A comparative analysis of ten international jurisdictions*, Hogan Lovells White Paper, 2012.

[6] V. le osservazioni di I. Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, Queen Mary University of London, School of Law, Legal Studies Research Paper N. 74/2011; M. Zoetekouw, *Ignorantia Terrae Non Excusat*, Crossing Borders: Jurisdiction in Cyberspace conference, 2016.

[7] V. N. Seitz, *Transborder Search: A New Perspective in Law Enforcement?*, in *Yale Journal of Law and Technology* 7(1), Article 2, 2005, p. 23 ss.

2. L'accesso transfrontaliero ai dati: una sfida per il diritto internazionale

Sono diversi gli ordinamenti giuridici che utilizzano il cosiddetto "criterio degli effetti" per influenzare le attività che si verificano al di fuori dei loro confini territoriali. Questa tecnica permette loro di applicare le leggi nazionali o trattati internazionali a circostanze che si verificano in territorio straniero, ma che hanno ripercussioni all'interno del loro territorio. Come è stato osservato[8], regolare efficacemente le attività internazionali si è rivelato difficile, soprattutto quando non ci sono persone od oggetti fisici associati a queste attività dentro i confini del paese che cerca di applicare tali regole. In sostanza, per potenziare l'efficacia delle legislazioni statali, è cruciale che le entità o i beni materiali implicati in specifiche attività siano sottoposti alla giurisdizione dello Stato. Questo principio risulta di estrema importanza in settori come quello della concorrenza, del settore bancario/finanziario e ambientale, non ultimo il settore delle sanzioni economiche internazionali.

Pur essendo importante, la giurisdizione di uno Stato non garantisce di per sé l'attuazione efficace delle sue leggi, specialmente per attività che si svolgono oltre i suoi confini nazionali[9]. Il diritto internazionale si trova di fronte a una sfida critica: definire la sovranità e la giurisdizione degli Stati in relazione ad attività che superano i confini territoriali e, più subdolamente, quelle che avvengono all'interno di questi confini. Per garantire una regolamentazione efficace, è essenziale trovare un equilibrio che armonizzi la protezione della sovranità statale con la necessità di un'applicazione trasparente delle leggi nazionali a livello internazionale.

Per gestire le sfide legate all'accesso ai dati oltre i confini nazionali, molti Stati hanno instaurato relazioni sia formali che informali, incluse alleanze bilaterali o multilaterali di mutua assistenza legale (MLA). Ta-

[8] Così, J.L. GOLDSMITH, *The Internet and the Abiding Significance of Territorial Sovereignty*, in *Indiana Journal of Global Legal Studies*, 1998, p. 475 ss.; v. anche W.H. VON HEINEGG, *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict, 2012, p. 7 ss.

[9] C. VELASCO, *Cybercrime jurisdiction: Past, Present and Future*, in *ERA Forum Journal of the Academy of European Law* 16(3), 2015, p. 331 ss.

li accordi stabiliscono una base giuridica per lo scambio di assistenza in indagini e procedimenti penali. Al di là degli MLA, esistono altre forme di cooperazione internazionale, come la Convenzione sulla cybercriminalità del Consiglio d'Europa, la Convenzione europea di assistenza giudiziaria in materia penale e, nell'ambito dell'UE, la Direttiva 2016/680 sulla protezione dei dati personali per fini giudiziari[10]. A livello europeo, meccanismi come il sistema d'informazione Schengen, Europol, Eurojust e Interpol facilitano ulteriormente lo scambio di dati e la collaborazione tra autorità di polizia e giudiziarie degli Stati membri.

Va osservato che, a complemento dei metodi formali, si sono resi necessari strumenti alternativi. Questi includono la collaborazione con i *service provider*, i quali hanno stabilito uffici specifici per gestire le richieste di accesso ai dati da parte delle autorità statali. Nonostante gli sforzi mirati a un coordinamento, i rapporti tra le autorità governative e i *service provider* sono tutt'altro che fluidi e possono determinare frizioni non indifferenti. Queste sfide possono essere attribuite in parte alla diversità dei sistemi giuridici e alla mancanza di allineamento tra le normative nazionali e internazionali sulla protezione dei dati personali. Inoltre, le limitazioni imposte dalla legislazione e le politiche interne delle società tecnologiche, che solitamente ruotano attorno al principio di non discriminazione tra utenti e alla difesa della loro privacy, possono costituire un freno alla collaborazione con le autorità governative.

L'accesso ai dati attraverso i confini nazionali è, ovviamente, una delle principali difficoltà della cooperazione giuridica internazionale. Il coordinamento tra le autorità governative e i *service provider* emerge come un tassello fondamentale per affrontare tale problema. Ciò richiede, però, un impegno per promuovere una più ampia armonizzazione tra le norme nazionali e internazionali relative alla protezione dei dati personali alla ricerca di un equilibrio tra la necessità di proteggere la privacy degli utenti e l'esigenza di assicurare l'efficienza delle indagini penali.

[10] Vedi P. VOGIATZOGLOU, T. MARQUENIE, *Assessment of the implementation of the Law Enforcement Directive*, Study requested by the LIBE Committee, European Parliament, 2022, in *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf*.

3. Microsoft Corp. v. United States of America

Per illustrare le complessità menzionate, possiamo considerare il caso di un contenzioso diventato emblematico per le sue implicazioni nel *cloud computing* e nella gestione transnazionale dei dati. Si tratta di un caso che ha coinvolto il Governo USA e la società Microsoft (*Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, United States v. Microsoft*, No. 14-2985-CV) e che rappresenta un esempio lampante delle difficoltà e delle sfide legate alla localizzazione dei dati nel contesto della rete[11].

Nel dicembre del 2013, un giudice del *Southern District* di New York emise un mandato di perquisizione nei confronti di Microsoft, richiedendo la divulgazione dei contenuti di un account di posta elettronica e autorizzando il governo a esaminare i dati al fine di dimostrare un presunto traffico internazionale di droga. Tuttavia, la società sollevò il problema che gran parte dei dati richiesti era collocata nel *data center* di Dublino, in Irlanda. La Microsoft acconsentì a fornire i dati memorizzati nei *data center* degli Stati Uniti, ma rifiutò la richiesta per quelli situati in Irlanda. Microsoft sostenne che per ottenere i dati conservati nei *data center* irlandesi non si dovesse applicare la normativa interna statunitense, bensì il Trattato di Mutua Assistenza Legale (MLAT) sottoscritto tra gli Stati Uniti e l'Irlanda. Tuttavia, il giudice americano obiettò che la legge interna (*Section* 2703) consentiva l'accesso ai dati indipendentemente dalla loro ubicazione. Microsoft impugnò la richiesta, ma il *Chief District Judge* la respinse, affermando che in caso di mancata esecuzione del mandato del giudice, si sarebbe dovuto ricorrere allo strumento di cooperazione dell'MLAT. Inoltre, poiché gli Stati Uniti avevano concluso accordi soltanto con circa sessanta Paesi, in assenza di un accordo specifico, certe informazioni non sarebbero state accessibili, poiché al di fuori del campo di applicazione della legge. Di conseguenza, Microsoft impugnò nuovamente la richiesta davanti alla *District Court*, la quale tuttavia la confermò.

[11] V. per tutti D. SVANTESSON, F. GERRY, *Access to extraterritorial evidence: The Microsoft cloud case and beyond*, in *Computer Law & Security Review* 31(4), 2015, p. 478 ss.

Successivamente, Microsoft presentò un'ulteriore impugnazione presso il *Second Circuit*. In questa fase, sia il governo irlandese che numerose società, tra cui Apple, Amazon, CNN, Fox News, Verizon, The Washington Post e diverse altre aziende del settore delle tecnologie dell'informazione e dei media, intervennero nel processo. Numerosi studi legali ed esperti del campo della *computer science* e della gestione dei dati delle principali università e centri di ricerca degli Stati Uniti.

Nel documento presentato nel processo il 15 dicembre 2014, un gruppo di trentacinque esperti, in qualità di *amici curiae*, hanno sottolineato alcuni punti rilevanti per la soluzione del caso[12]. Nel loro intervento, gli studiosi hanno evidenziato l'importanza del *cloud computing* nella gestione dei dati, poiché offre significativi vantaggi in termini di efficienza ed economicità rispetto alla conservazione locale dei dati. Il gruppo ha poi esaminato il concetto di *cloud computing* in sé. Secondo gli esperti l'immagine della "nuvola" rappresenta un'astrazione attraente, ma non tiene conto della complessa realtà tecnologica necessaria per gestire l'accesso remoto ai *data server*. Nonostante sembri che i dati siano immateriali, in realtà sono conservati in modo tradizionale tramite sistemi di storage nei *data center* sparsi in tutto il mondo. Per concludere gli *amici curiae* sostennero che la risoluzione del caso avrebbe dovuto prendere in considerazione il fatto che

> la posta elettronica basata sul web e gli altri dati archiviati nel *cloud* hanno almeno una sede fisica identificabile e che il contenuto delle *e-mail* dei clienti è almeno un luogo fisico identificabile, e che il contenuto delle *e-mail* dei clienti viene memorizzato in modo sicuro come proprietà riservata del titolare dell'*account*[13].

Questa posizione sinteticamente evidenzia il conflitto tra chi sostiene una posizione tradizionale che richiede l'autorizzazione dello Stato dove sono localizzati i server per l'accesso ai dati contenuti in essi e che fa perno sulla "fisicità" dei dati e quella che fa leva su una presunta efficacia extraterritoriale di alcune leggi. Per inciso, è interessante os-

[12] V. *Brief for amici curiae computer and data science experts in support of appellant Microsoft corporation*, in *https://blogs.microsoft.com/wp-content/uploads/sites/149/2014/09/Computer-Science-Academics-AmicusBrief.pdf*.

[13] V. n. precedente.

servare a quest'ultimo riguardo che per superare il problema relativo alla dislocazione dei dati su più territori, non è mancato chi, nel contesto degli studi organizzati a livello di Consiglio d'Europa, ha fatto leva sul potere di accedere, di modificare i dati (ovunque siano "dispersi" sulla rete)[14].

Il 14 luglio 2016, la *District Court* riconobbe a Microsoft il diritto di rifiutare la richiesta governativa di accesso ai dati conservati nel *data center* irlandese, sostenendo che l'acquisizione delle *email* richiedesse l'attivazione del Trattato di mutua assistenza legale concluso tra gli Stati Uniti e l'Irlanda. La sentenza ha suscitato un ampio dibattito riguardante la localizzazione dei dati e ha sollevato interrogativi riguardanti la sovranità dei dati, la tutela della *privacy* e l'urgente necessità di un quadro normativo internazionale per affrontare le complesse sfide transfrontaliere legate all'accesso e alla conservazione dei dati[15].

4. Il Cloud Act

L'importanza delle questioni sollevate durante il processo, e altrettanto importante, la ferma posizione dell'esecutivo degli Stati Uniti in merito alla questione, hanno determinato il deferimento del caso alla Corte Suprema degli Stati Uniti[16].

Tuttavia, prima che la Corte si pronunciasse sul caso, il Congresso degli Stati Uniti ha introdotto il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* per risolvere il problema dell'accesso ai dati elettronici transfrontalieri per motivi legati all'applicazione della legge. Questa modifica legislativa ha imposto ai fornitori di servizi di posta elettroni-

[14] Come osservato da G.M. RUOTOLO, *Hey! You! Get Off My Cloud! Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Archivio penale*, 2013, p. 794, in relazione al *Discussion paper* della Divisione su crimine economico della Direzione generale del Consiglio d'Europa, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, in *https://rm.coe.int/16802fa3df*.

[15] V. *Microsoft v. United States*, No. 14-2985 (2d Cir. 2016), *https://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html*.

[16] V. *United States v. Microsoft Corp.*, 584 U.S. (2018), *https://supreme.justia.com/cases/federal/us/584/17-2/*.

ca l'obbligo di rivelare le comunicazioni elettroniche di loro custodia (anche all'estero). Il governo ha emesso e notificato un nuovo mandato a Microsoft in conformità con questo emendamento normativo in sostituzione dell'originale che era al centro del caso iniziale. La Corte suprema ha pertanto ritenuto cessata la materia del contendere e ha ordinato alla Corte distrettuale di archiviare il caso, considerandolo ormai irrilevante.

IL *CLOUD Act* introduce due modifiche distinte alla legislazione esistente sull'accesso transfrontaliero ai dati in ambito penale. In primo luogo, essa chiarisce alcuni punti oscuri dello *Stored Communications Act* (SCA) del 1986. Viene imposto ai fornitori di servizi internet, che ricadono sotto la giurisdizione degli Stati Uniti, di produrre i dati memorizzati anche al di fuori del paese, in conformità con l'SCA. In secondo luogo, il *CLOUD Act* modifica alcune disposizioni dell'*Electronic Communications Privacy Act* (ECPA). La nuova disciplina consente inoltre il trasferimento di dati archiviati negli Stati Uniti a determinati Stati stranieri che lo richiedano legittimamente. Un pilastro del *CLOUD Act* è, dunque, la possibilità per il governo statunitense di richiedere alle società stabilite nel suo territorio di richiedere i dati anche se archiviati in altri Paesi. La legge prevede che gli Stati Uniti possano stipulare accordi internazionali con altri Stati per consentire ai propri organi competenti di richiedere dati a società statunitensi per indagini che hanno luogo al di fuori degli Stati Uniti. Il CLOUD contiene disposizioni che cercano di bilanciare gli interessi della privacy con la sicurezza nazionale. L'approvazione del *CLOUD Act* ha anche aperto la strada alla conclusione di un accordo bilaterale di condivisione dei dati tra Stati Uniti e Regno Unito, considerato un modello per futuri accordi con altri Paesi.

La nuova legislazione presenta indiscutibilmente spunti interessanti adottando un approccio che non è distante da quello presente nelle discussioni, già precedentemente illustrate all'interno del Consiglio d'Europa, e basato sul concetto di "potere di disposizione". Come osservato nel rapporto:

> [q]uesto potere formale di disposizione collega qualsiasi dato a individui o entità che detengono l'accesso esclusivo o congiunto a tali dati e

> che hanno il diritto legale di apportare modifiche, cancellare, sopprimere o disabilitare tali dati. Inoltre, essi hanno il diritto di escludere altri soggetti dall'accesso e dall'utilizzo dei dati in questione[17].

Un potere di disposizione completamente indipendente da parametri di localizzazione geografica di qualsiasi tipo.

5. La localizzazione forzata dei dati nel territorio dello Stato

A livello globale, gli Stati stanno cercando di superare le difficoltà legate all'accesso ai dati personali attraverso la modifica dei loro ordinamenti giuridici. In molti casi, gli Stati stanno favorendo o addirittura obbligando i *service providers* a conservare i dati personali dei loro cittadini all'interno del territorio nazionale. Questo spostamento verso la localizzazione "forzata" dei dati personali nei confini nazionali implica che i *service providers* devono costruire data center all'interno dei paesi interessati dalle normative. Tuttavia, queste normative hanno creato problemi logistici non trascurabili per le aziende private del settore, tra cui la necessità di acquisire spazi adeguati per i *data center*, la duplicazione degli archivi, la formazione di partnership con società straniere indicate dai governi e così via.

La tendenza a imporre la localizzazione dei dati all'interno del territorio dello Stato è un fenomeno che si sta diffondendo in molti paesi del mondo, come dimostra il caso della Russia. Nel 2015, la legislazione russa ha stabilito che le società che operano nel campo dei dati informatici devono conservare i dati personali dei cittadini russi all'interno del territorio dello Stato. Questa disposizione è stata applicata con rigore e ha portato a provvedimenti drastici nei confronti di coloro che non si sono conformi alla legge. Per esempio, nel 2016, l'autorità di controllo nel settore delle comunicazioni elettroniche russa, *Roskomnadzor*, ha sanzionato il *social network* LinkedIn per non aver rispettato gli obblighi di conservazione dei dati personali dei cittadini russi all'interno del territorio dello Stato.

[17] V. il *discussion paper supra* n. 13, pp. 10-11.

È interessante notare come molte delle recenti modifiche della legislazione russa nel campo dei dati personali siano state giustificate dal bisogno di adeguarsi agli standard europei di protezione dei dati. Questo è stato evidenziato dalla riforma della normativa UE sui dati personali (GDPR) e dalle sentenze della Corte di giustizia dell'Unione europea, che hanno dichiarato invalida la direttiva 2006/24/CE sulla *data retention* e hanno annullato la decisione che consentiva il trasferimento dei dati dall'UE verso gli USA basata sui *Safe Harbour Principles*. Questo fenomeno ha spinto la Commissione UE a raccomandare agli Stati di intervenire sui sistemi normativi per ridurre la tendenza alla localizzazione forzata dei dati. Con il Regolamento (UE) 2018/1807, per esempio, si propone di eliminare le barriere che attualmente impediscono la libera circolazione transfrontaliera all'interno della UE dei dati non personali (i dati che non riguardano persone fisiche identificate o identificabili). Le disposizioni di quest'ultimo si integrano con quelle contenute nel Regolamento (UE) 2016/679 (GDPR) che prevedono la libera circolazione e la portabilità dei dati personali all'interno dell'UE[18]. Gli sforzi della Commissione sono stati poi sinteticamente raccolti nella Comunicazione intitolata "Una strategia europea per i dati"[19] con l'obiettivo creare un mercato unico dei dati che garantisca la competitività globale dell'Europa e la sovranità dei dati. L'assetto normativo è stato completato negli ultimi anni grazie al regolamento sulla governance europea dei dati (Regolamento 2022/868)[20] e al recentissimo regolamento riguardante norme armonizzate sull'accesso equo ai dati e

[18] V. anche la Comunicazione della Commissione europea del 2 luglio 2014 "Verso una florida economia basata sui dati", in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52014DC0442&from=EN*, e le Comunicazioni del 25 aprile 2018 (in *https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)232&lang=it*) e del 15 maggio 2018 (*https://eur-lex.europa.eu/resource.html?uri=cellar:ef4c7837-583f-11e8-ab41-01aa75ed71a1.0022.02/DOC_1&format=PDF*), essenziale per lo sviluppo del mercato unico digitale e dell'economia dei dati all'interno dell'Unione.

[19] V. *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066*.

[20] V. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati) *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R0868*.

sul loro utilizzo (c.d. Data Act, Regolamento 2023/2854 del 13 dicembre 2023)[21]. In particolare in quest'ultimo atto vengono adottate precauzioni per prevenire lo spostamento non autorizzato di informazioni attraverso confini internazionali, mirando a creare un ambiente di fiducia e sicurezza, con un incremento nella tutela delle informazioni personali e anche di quelle non personali ma di natura sensibile, quali i segreti commerciali.

6. La narrativa della protezione della privacy quale driver della localizzazione forzata dei dati nel territorio dello Stato

Un dato è sicuramente interessante, sebbene la narrativa ufficiale relativa agli obblighi di localizzazione dei dati sia ancorata all'esigenza di proteggere la riservatezza dei dati personali, altre ragioni sembrano sottostare a questa pratica[22]. Gli Stati cercano di affermare la propria sovranità sul traffico di dati e di promuovere allo stesso tempo la propria politica commerciale e lo sviluppo economico/tecnologico in questo settore. Non ultima, la localizzazione forzata può anche essere utile per far rispettare le regole dell'ordinamento giuridico ai fornitori di servizi e per facilitare la raccolta informativa da parte delle agenzie di *intelligence*.

Questa tendenza è spesso associata al tentativo degli Stati di mantenere il transito dei dati (c.d. *routing*) interamente all'interno del proprio territorio, senza deviazioni verso territori stranieri, quando il traffico avviene tra entità che operano all'interno dello stesso ordinamento giuridico. In questo modo, gli Stati cercano di garantire che gli snodi principali dell'autostrada digitale passino attraverso il loro territorio, raffor-

[21] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202302854*.

[22] C. MILLARD, *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, in *IEEE Cloud Computing* 2(2), 2015, p. 10 ss.; ID., *Cloud Computing Law*, 2nd ed., Oxford, 2021.

zando così la loro posizione strategica sulla rete internet. Tuttavia, queste misure sono state oggetto di numerose critiche, in quanto si ritiene che le argomentazioni utilizzate siano strumentali e che altri sistemi, come un più ampio uso di tecniche crittografiche, potrebbero raggiungere più efficacemente la protezione dei dati personali.

La pratica della localizzazione dei dati ha certamente un impatto significativo su vari aspetti, tra cui il commercio globale, l'innovazione e la sicurezza delle informazioni. Questa restrizione ha effetti negativi sul commercio globale, poiché impedisce la libera circolazione dei dati tra Stato e pone ulteriori ostacoli e restrizioni alle aziende che cercano di accedere ai mercati stranieri. Vi è un impatto dannoso anche sull'innovazione, poiché limita lo scambio di conoscenze e informazioni, ostacolando la collaborazione internazionale nei settori ad alta tecnologia. È stato osservato, inoltre, sotto il profilo della sicurezza dei dati, come la localizzazione dei dati possa aumentare il rischio di accesso non autorizzato o violazioni dei dati. Quando i dati sono concentrati in un'unica giurisdizione, diventano un bersaglio attraente per i cybercriminali, che possono concentrare i loro sforzi per accedere a specifici centri dati. Allo stesso tempo, questa pratica può portare a una maggiore dipendenza dall'infrastruttura di sicurezza informatica di un singolo Paese, rendendo più difficile la difesa contro attacchi informatici sofisticati[23].

[23] V. L.R. SHEPPARD, E. YAYBOKE, C.G. RAMOS, *The Real National Security Concerns over Data Localization*, Center for Strategic and International Studies, CSIS Briefs, July 2021, *https://www.csis.org/analysis/real-national-security-concerns-over-data-localization*.