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

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. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

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