ISTITUTO ITALIANO PER LA PRIVACY E LA VALORIZZAZIONE DEI DATI

LE "TENTAZIONI" DEL CLOUD EUROPEO E NAZIONALE: TRA SEMPLIFICAZIONE POLITICA E CRITICA GIURIDICA

25 settembre 2020

Uno studio di Luca Bolognini* ed Enrico Pelino**

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Indice generale

Abstract

La corsa alla creazione di soluzioni cloud locali è ormai una costante nei piani di sviluppo digitale degli Stati membri. L'Italia promuove la costituzione del cd. "cloud nazionale", la Germania e la Francia lavorano da tempo alla definizione del progetto Gaia-X. A livello istituzionale dell'Unione Europea, il potenziamento del cloud computing occupa il ruolo di tematica strategica per l'immediato futuro. L'obiettivo dichiarato è quello di realizzare un affrancamento dalle soluzioni che oggi poggiano quasi integralmente su infrastrutture messe a disposizione da fornitori internazionali. Concorrono – più per sovrapposizione che per composizione – ragioni in senso lato geopolitiche, aspirazioni alla preminenza tecnologica internazionale, preoccupazioni connesse con la protezione dei dati personali rispetto a paventate ingerenze terze dovute all'applicazione extraterritoriale di atti normativi stranieri. La recente pronuncia cd. "Schrems II" della Corte di Giustizia Europea e, in precedenza, sia pure con inferiore perimetro di interesse per il vasto pubblico, i risultati dello studio congiunto EDPB-EDPS sul Cloud Act statunitense hanno posto con forza il problema dell'acquisizione internazionale di flussi di dati personali (e non personali, potremmo aggiungere) e delle connesse garanzie.

Il presente studio intende avviare un'analisi della tematica, volta innanzitutto a districare i molteplici piani di questioni sollevate, che toccano non solo temi giuridici ma anche politici, e si propone di fare un primissimo ragionato censimento dei vari corpi di fonti normative applicabili. Al di là di dichiarazioni a effetto, occorre determinare fino a che punto sia realmente possibile e auspicabile l'indipendenza di un cloud locale europeo rispetto ai fornitori extra UE e, più concretamente, fino a che punto una soluzione autarchica sia economicamente e tecnologicamente praticabile rispetto a servizi oggi essenziali, per gli Stati, o abilitativi dell'esercizio di altri diritti e libertà fondamentali, per gli individui, dunque non suscettibili di menomazione o di interruzione. Va altresì compreso fino a che punto sia anche opportuna sul versante della sicurezza, ancorché ciò di primo acchito possa apparire controintuitivo. Occorre infatti includere, quantomeno nella valutazione complessiva, gli alti

livelli qualitativi di stabilità dei servizi e di sussistenza di misure ad elevato coefficiente tecnologico nel contrasto al *cybercrime*, oggi garantiti dai maggiori provider internazionali, livelli di cui non sarebbe raccomandabile privarsi ove se ne possano conservare i benefici, riducendone sensibilmente i connessi rischi. La tutela dei dati trattati da ingerenze terze deve, infatti, essere misurata anche sul piano, certamente diverso da quello della minaccia "extraterritoriale", ma comunque rilevante, rappresentato dagli illeciti e dagli incidenti di sicurezza. Si deve inoltre tenere in considerazione la disponibilità, già perfettamente attuale e "nelle mani" degli utilizzatori, di soluzioni immediatamente tutelanti, come la cifratura o la segregazione di set di dati strategici. In altre parole, se sono possibili misure di significativo depotenziamento del rischio extraterritoriale, che facciano salvi i vantaggi in termini di contrasto al *cybercrime*, esse vanno debitamente incluse nella valutazione complessiva.

L'analisi non nasconderà altresì incongruenze nella tutela interna all'Unione Europea e disallineamenti tra spinte nazionali alla localizzazione e principio della libera circolazione dei dati. In breve, si vuole proporre un quadro più articolato e meno ovvio dei temi trattati, che non possono essere ridotti, se non al prezzo di una eccessiva semplificazione, a una contrapposizione binaria UE *versus* extra UE, ma rivelano sinergie trasversali e disallineamenti reciproci su fronti apparentemente unitari; è utile ragionare, piuttosto, in termini di creazione di un ecosistema condiviso che tragga i maggiori vantaggi dalle soluzioni oggi disponibili e riconosca l'esigenza di adottare forme di tutela sostanziali. Non si tratta in alcun modo di eludere le serie, ma non immediatamente risolvibili, questioni connesse all'extraterritorialità, bensì di utilizzarle, semmai, come leva per ottenere un ripensamento critico su lacune e disarmonie giuridiche che emergono anche all'interno dell'Unione Europea. Neppure si tratta di avventurarsi sulla strada di soluzioni domestiche poco tutelanti, o meno tutelanti di quelle attuali, ma di preservare livelli elevati di protezione da illeciti, dunque di disporre delle soluzioni tecnologiche più avanzate al momento, e allo stesso tempo di trovare strumenti giuridici che garantiscano un maggiore controllo nazionale delle infrastrutture e dei dati e una mitigazione del rischio a un livello che lo renda giuridicamente accettabile.

Il contesto – Verso la realizzazione di cloud nazionali

Nel febbraio 2020, la Ministra italiana per l'Innovazione, Paola Pisano, dando seguito ad anticipazioni del novembre precedente[1], annunciava in un'intervista al quotidiano "Il Sole 24 Ore" l'avvio del progetto di costituzione di un cloud nazionale, in fase ancora di studio, da gestirsi verosimilmente attraverso una joint venture tra Stato e privati in quota di minoranza, selezionati attraverso gara pubblica. L'obiettivo dichiarato rimandava innanzitutto a considerazioni di natura geopolitica: evitare interruzioni di servizio o ingerenze indebite dovute a tensioni internazionali, anche non direttamente coinvolgenti l'Italia o l'Unione europea, ma tali da colpire potenzialmente i fornitori internazionali di tecnologia cloud o le stesse infrastrutture fisiche[2]. Il modello prospettato non prevede la gestione della totalità del patrimonio informativo pubblico, ma postula una selezione a monte: in particolare, secondo le dichiarazioni rese, "*il Polo si occuperà solo dei dati critici, quelli che rientrano nel perimetro di sicurezza nazionale, e comunque, per i diversi profili di competenza, sarà vigilato dalle varie Authority di regolamentazione esistenti*".

Il 23 giugno 2020, l'*ex* Presidente dell'Autorità Garante per la protezione dei dati personali italiana, Antonello Soro, nel contesto del tradizionale discorso al Parlamento e al Governo sollevava a sua volta la questione, di squisita politica normativa, della creazione di un'infrastruttura cloud di Stato, in connessione con obiettivi di sicurezza nazionale e di sovranità digitale. Veniva così a registrarsi un'ulteriore convergenza istituzionale sul tema. Il ragionamento, in particolare, prendeva le mosse dall'esame dei rischi connessi ai *data breach* o quantomeno a una certa tipologia di essi. Indicava infatti il Presidente: "*Le implicazioni, in termini di sicurezza nazionale, di alcuni data breach dimostrano anche come*

1 F. Me., *Pisano: "Serve un cloud italiano contro i rischi geopolitici"*, in *Corriere delle comunicazioni – CorCom*, 27 novembre 2019, https://www.corrierecomunicazioni.it/digital-economy/pisano-serve-un-cloud-italiano-contro-i-rischi-geopolitici.

2 F. Me., *Pisano: "Joint venture Stato-privati per il cloud nazionale"*, in *Corriere delle comunicazioni – CorCom*, 20 febbraio 2020, https://www.corrierecomunicazioni.it/pa-digitale/pisano-joint-venture-stato-privati-per-il-cloud-nazionale/

la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e 'canali' induca a ripensare il concetto di sovranità digitale.

E di fronte alla delocalizzazione in cloud di attività rilevantissime chiediamo al Parlamento e al Governo se non si debba investire in un'infrastruttura cloud pubblica, con stringenti requisiti di protezione, per riversarvi con adeguata sicurezza dati di tale importanza.

In un contesto in cui le tecnologie ICT sono divenute - sempre più chiaramente con la pandemia - la principale infrastruttura di ciascun Paese, assicurarne una regolazione sostenibile e adeguata, tale da garantire sicurezza, indipendenza dai poteri privati, soggezione alla giurisdizione interna, diviene un obiettivo non più eludibile" (cfr. GPDP, Relazione annuale 2019, discorso del presidente, doc. web n. 9428327). Come si nota, sono in definitiva toccati due poli concettuali, sia pure non necessariamente connessi: quello della sicurezza informatica e quello della giurisdizione applicabile, sui quali si tornerà più avanti.

Allargando a questo punto in uno *zoom out* il campo visuale dall'Italia all'Unione europea, va necessariamente preso atto di un complessivo e ampio sviluppo di iniziative dirette alla creazione di infrastrutture cloud locali, a conferma di un marcato, riconoscibile e condiviso indirizzo politico. La più visibile di queste iniziative è probabilmente costituita dal progetto denominato "Gaia-X"[3], di aspirazione europea, presentato dal governo tedesco il 29 ottobre 2019 e al momento a guida e composizione quasi esclusivamente franco-tedesca, che vede attualmente la partecipazione di oltre venti grandi gruppi europei principalmente del settore Telco e IT[4]. La piattaforma non esclude, esattamente come il progetto di cloud nazionale italiano, sopra richiamato, la partecipazione dei grandi provider internazionali, in particolare di quelli statunitensi, a condizione dell'osservanza di un codice di regole[5].

3 Cfr. data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

4 Si tratta per esempio dei seguenti: Amadeus, Atos, Beckhoff, Bosch, BMW, DE-CIX, Deutsche Telekom, Docaposte, EDF, Fraunhofer, German Edge Cloud, Institut Mines Telecom, International Data Spaces Association, Orange, 3DS Outscale, OVHcloud, PlusServer, Safran, SAP, Scaleway, Siemens. Cfr. L. Tung, *Meet GAIA-X: This is Europe's bid to get cloud independence from US and China giants*, in *ZDNet*, 8 giugno 2020, *https://zd.net/3iq6qpk.*

5 Cfr. art. ult. cit.

Attualmente, non è del tutto chiara la relazione tra il progetto italiano e la piattaforma franco-tedesca in fase di realizzazione, e in particolare se, e in quali termini, in futuro l'Italia ritenga di aderirvi, al di là di generali manifestazioni di interesse[6], tanto più se si tiene conto del fatto che scelte iniziali di impostazione, se non coordinate tra i due modelli, potrebbero produrre nel prosieguo sviluppi divergenti. In proposito, sarebbe auspicabile opportuna chiarezza sulle intenzioni e sulle eventuali ragioni di autoesclusione da un progetto che si presenta in fase più avanzata di quello italiano, si pone un orizzonte ambizioso e rivela apporti economici e tecnologici di rilievo. La pur legittima scelta di fare parte a sé rappresenta infatti una decisione di peso e produttiva di conseguenze: sembra dunque corretto parteciparne le motivazioni.

Allargando la visuale in un ulteriore livello di *zoom out*, deve notarsi che le direttrici verso la creazione di piattaforme cloud europee vanno idealmente collocate entro la cornice comune delle iniziative programmate dalla Commissione europea, e ad essa dovranno aderire. Esse devono dunque svilupparsi come parti di un ecosistema sviluppato secondo le linee strategiche progettate in sede istituzionale europea. Proprio su questo aspetto, giova menzionare il documento dal titolo *Una strategia europea per i dati*[7]. Costituiscono elementi chiave di questa strategia anche la creazione di una *European federation of cloud infrastructures and services*, di uno *European marketplace for cloud services*, di una *governance framework and an EU Cloud Rulebook*[8].

Questo dunque il contesto della presente analisi. Potrebbe essere arricchito con la menzione di percorsi analoghi in ambito europeo, ma crediamo sufficienti queste coordinate.

6 Luigi Garofalo, *Pisano: "Definire le regole per il cloud europeo, ma non è possibile escludere le Big Tech dalla Pa"*, in *Key4Biz.it*, 5 agosto 2020, *key4biz.it/pisano-definire-le-regole-per-il-cloud-europeo-ma-non-e-possibile-escludere-le-big-tech-dalla-pa/317590*.

7 Commissione europea, 19 febbraio 2020, COM(2020) 66 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066_20_283.

8 Cfr., per es., https://ec.europa.eu/digital-single-market/en/cloud.

Il complesso coordinamento delle fonti

Va subito chiarito che le tematiche sollevate presentano profili di non semplice lettura. Riguardano infatti la sfera degli obiettivi politici e non soltanto quella propriamente giuridica, o meglio toccano i rapporti reciproci di interazione e limitazione tra i due ambiti. Inoltre coinvolgono, a vario titolo e in misura diversa, un complesso di aree del diritto, almeno le seguenti:

- normativa sulla protezione dei dati personali – reg. (UE) 2016/679 (cd. "RGPD"), dir. 2002/58 (cd. direttiva "ePrivacy"), e a livello nazionale d.lgs. 30 giugno 2003, n. 196 ("codice privacy") e normativa secondaria collegata;
- normativa specifica di bilanciamento tra protezione dei dati personali e repressione dei reati – dir. (UE) 2016/680, d.lgs. 15 maggio 2018, n. 51;
- normativa extra UE in materia di sorveglianza per finalità di *intelligence*: in particolare, più avanti si farà riferimento alla disciplina nordamericana, soprattutto alla Section 702 del FISA;
- normativa in materia di *e-evidence*: dunque, Cloud Act statunitense e strumenti normativi ancora in via di approvazione in ambito europeo, ossia la proposta di regolamento COM/2018/225 final – 2018/0108 e la proposta di direttiva COM/2018/226 final - 2018/0107;
- normativa sui dati non personali, ossia reg. (UE) 2018/1807;
- normativa in materia di infrastrutture strategiche – dir. (UE) 2016/1148, e a livello nazionale il d.lgs. 18 marzo 2018, n. 65
- normativa in materia di cloud nella PA – d.lgs. 7 marzo 2005, n. 82 (cd. "CAD") e relativa normativa secondaria (es. Linee Guida AGID), d.l. 18 ottobre 2012, n. 179, come modificato dal d.l. 16 luglio 2020, n. 76

Una compiuta tessitura delle reciproche implicazioni tra questi diversi corpi normativi risulterebbe troppo articolata e prematura in questa prima fase di analisi: obiettivo del presente lavoro non è tanto quello di fornire un compiuto vaglio delle interazioni normative, ma quello di presentare uno strumento agile che prepari il campo a un più articolato dibattito. Il focus maggiore riguarderà comunque la normativa sulla protezione dei dati personali, in consonanza con la vocazione dell'Istituto. Si tratta di area giuridica ampiamente assorbente, se si tiene conto della nozione per così dire "agglutinante" di dato personale e del dinamismo insito nell'applicazione concreta del concetto di reidentificazione. In altre parole, a meno di non essere assolutamente certi che i set di dati trattati siano non personali, occorre prudenzialmente considerarli tali (personali), applicando di conseguenza lo standard di tutela più rigoroso. Giova inoltre rilevare che in questa materia è di recente intervenuta la sentenza cd. "Schrems II" della Corte di giustizia dell'Unione europea, ossia decisione CGUE, 16 luglio 2020, C-311/18, il cui impatto, tuttora in fase di elaborazione, non può essere trascurato anche in uno studio sul cloud computing locale e globale. Dunque, sceglieremo di affrontare il tema posto considerando innanzitutto dal punto prospettico di osservazione della normativa sulla protezione dei dati personali.

La dipendenza della PA dai fornitori extra UE

Attualmente, il mercato mondiale dei principali fornitori di infrastrutture cloud è dominato da cinque gruppi societari, quattro dei quali (Amazon, Microsoft, Google, IBM) hanno la sede principale negli Stati Uniti, il quinto, Alibaba, in Cina. Quote residuali del mercato sono distribuite tra ulteriori gruppi, prevalentemente con base nordamericana (es. Cisco Systems, Salesforce, Oracle) esclusi alcuni gruppi europei[9]. Questa situazione dipende principalmente – per quanto è possibile apprezzare – da dinamiche di mercato e di libera

9 Cfr. per una disamina più approfondita, L. Dignan, *Top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players*, in *ZDNet*, 11 maggio 2020, https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/

concorrenza, dalle capacità economiche, dagli investimenti sostenuti per la realizzazione delle infrastrutture e per la ricerca e lo sviluppo, dalla dotazione tecnologica di partenza dei fornitori. Il rilievo ha un suo significato, perché eventuali investimenti governativi diretti alla costruzione di un cloud nazionale non possono non tenere conto di fattori economici e di sostenibilità nel tempo e non possono sottrarsi al necessario confronto con parametri di efficienza imposti dal mercato.

L'attuale situazione dell'offerta di soluzioni cloud costituisce dunque un elemento di fatto, da assumere come tale. Determina ben precise implicazioni giuridiche. In Italia, ad esempio, è infatti ormai da tempo operativo il principio del "**cloud first**", confermato da ultimo nel Piano Triennale per l'Informatica 2019 – 2021, ossia l'obbligo per la Pubblica Amministrazione di definire nuovi progetti o sviluppare nuovi servizi adottando, in via prioritaria, soluzioni in cloud, privilegiando in particolare il modello SaaS, prima di qualsiasi altra opzione tecnologica e, più in generale, di ricorrere al cloud nel momento in cui intende *"acquisire sul mercato nuove soluzioni e servizi ICT per la realizzazione di un nuovo progetto o nuovi servizi destinati a cittadini, imprese o utenti interni alla PA*"[10].

La *ratio* è evidente e condivisibile: il cloud è lo standard più affermato e permette vantaggi riconosciuti in termini di efficienza, scalabilità, economicità e resilienza rispetto a modelli IT tradizionali, quali l'*housing* e l'*hosting*[11].

La combinazione di questi due elementi, ossia la situazione attuale di mercato e il principio "cloud first", determina quale conseguenza che la Pubblica Amministrazione tenda in larga misura a dipendere, nella sua operatività essenziale, e quantomeno in contesti di

10 Cfr. *Il modello cloud nella PA*, 13 febbraio 2020, § 4.1, in https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/index.html

11 Giova notare che tale indicazione riceve pieno avallo a livello di Unione europea, cfr. Commissione UE, *Una strategia digitale europea cit.*, p. 11, ove, nel quadro di una ancora insufficiente adozione di piattaforme cloud da parte delle pubbliche amministrazioni nel complesso degli Stati membri, si rileva quanto segue: "*L'adozione del cloud è limitata, in particolare, nel settore pubblico europeo; ciò può comportare una minore efficienza dei servizi pubblici digitali, non solo a causa del potenziale evidente in termini di riduzione dei costi informatici garantito dall'adozione del cloud, ma anche a causa del fatto che le pubbliche amministrazioni necessitano della scalabilità del cloud computing per la diffusione di tecnologie quali l'intelligenza artificiale*".

cloud pubblico, da infrastrutture che rimandano a qualcuno dei provider internazionali sopra indicati[12], e ciò o in via diretta oppure in via indiretta, attraverso intermediari. È dunque proprio all'interno di questo scenario che viene a collocarsi il progetto della costituzione di un cloud nazionale.

Analoghe considerazioni sono espresse nella già citata *strategia europea per i dati* della Commissione europea, cfr. in particolare pag. 10: "*I fornitori di servizi cloud basati nell'UE dispongono soltanto di una piccola quota del mercato del cloud, il che rende l'UE estremamente dipendente dai fornitori esterni, vulnerabile alle minacce esterne a livello di dati e soggetta a una perdita di potenziale d'investimento per l'industria digitale europea nel mercato dell'elaborazione dati*".

Così impostati i punti essenziali del tema, occorre valutare se realmente l'attuale situazione di dipendenza da grandi fornitori non nazionali possa integrare, fino a che punto, e comunque per quali ragioni, un fattore di rischio, in quale modo la realizzazione di soluzioni domestiche sia idonea a contenere il suddetto rischio, e in ogni caso se e in quale misura alcune delle criticità generalmente paventate nel dibattito pubblico possano essere sciolte a fronte di una disamina più granulare.

Il modello tripartito – disponibilità, riservatezza, integrità (DRI)

Al fine di individuare la tipologia di rischio e studiare misure di contenimento, l'approccio più immediato e consolidato appare quello offerto dal classico modello tripartito che interpreta il rischio in base a tre parametri: perdita della disponibilità dei dati (*availability*), della loro riservatezza (*confidentiality*), della loro integrità (*integrity*), eventualmente in cumulo tra loro.

12 Secondo indicazioni fornite dalla Ministra italiana per l'innovazione "*Oggi noi ci approvvigioniamo di risorse di cloud per l'80% da extra Ue*", cfr. Fabio Savelli, La battaglia per la (nostra) sovranità digitale: la corsa al cloud nazionale, in Corriere della sera, ed. online, 6 luglio 2020, https://bit.ly/32nyAf3

Il modello ha del resto il pregio di essere applicabile sia a dati personali sia a dati non personali. Applicazioni più dettagliate del modello potrebbero includere l'attribuzione di coefficienti numerici ai diversi fattori di rischio per stimarne gravità e probabilità, ma per il momento è difficile ravvisare elementi, adatti allo specifico e assai peculiare contesto di riferimento, che permettano di determinarli.

Rischi connessi con eventi di *data breach*

Una prima tematica da affrontare, anche per la rispettosa considerazione dovuta all'istituzione che l'ha espressa, concerne il rapporto tra incidenza dei *data breach* e sicurezza nazionale/sovranità digitale. Qui il riferimento al modello DRI appare perfino scontato, manifestandosi le violazioni di dati (personali[13]), per definizione, secondo una tipologia di eventi articolati nella distruzione, perdita, modifica, divulgazione e accesso non autorizzati (cfr. art. 4, par. 1, n. 12 RGPD).

Il cuore concettuale della nozione di *data breach* è il verificarsi di una violazione di sicurezza informatica od organizzativa. Tuttavia, per questa stessa ragione, non appare immediatamente comprensibile il rapporto postulato dalla Presidenza dell'Autorità Garante per la protezione dei dati personali italiana, tra nazionalizzazione delle infrastrutture ed eventi di *data breach*, almeno non senza ulteriori elementi e apporti di chiarificazione in tal senso. Detto altrimenti, gli incidenti di sicurezza hanno, in ultima analisi, origine in condotte malevole oppure negligenti, dunque rimandano all'ambito della qualità delle misure organizzative e tecnologiche adottate, alla correttezza delle valutazioni di rischio, al continuo aggiornamento degli standard, all'effettuazione di verifiche periodiche (*audit*), in breve a un complesso di regole che si collocano su di un piano completamente indipendente e trasversale rispetto a questioni di nazionalità o internazionalità del fornitore. Le regole di

13 Le considerazioni esposte possono tuttavia essere estese al trattamento dei dati non personali.

cybersicurezza, una volta definite, implementate e garantite, sono cioè tali a qualsiasi latitudine.

Vero che nelle considerazioni riportate in apertura è contenuto un rimando anche a profili attinenti alla giurisdizione, che, se ben comprendiamo, potrebbero alludere a difficoltà di comunicazione e collaborazione rilevate nella relazione tra fornitori *extra* UE e Autorità di controllo europee e/o a insufficiente riscontro agli interessati, ossia in altre parole all'osservanza effettiva delle previsioni del RGPD (reg. UE 2016/679). Non siamo, tuttavia, al corrente di attività sanzionatoria dell'Autorità Garante italiana chiaramente correlata a siffatte situazioni; dunque, ogni ragionamento volto a individuare con maggiore precisione le ragioni di insoddisfazione e il collegamento con l'esortazione alla costruzione di un cloud nazionale resta confinato nella sfera delle ipotesi e non può contare purtroppo su concreti punti di appoggio per essere sviluppato.

L'applicazione extraterritoriale della normativa di Paesi terzi

Il tema della giurisdizione e dell'applicazione di normativa dei Paesi terzi è comunque argomento centrale e si presta a essere esplorato a prescindere dalle considerazioni svolte nella parte conclusiva del paragrafo precedente. Sotto un certo punto di vista, esso costituisce – almeno in prospettiva giuridica, meno in chiave politica – il cuore stesso della questione, come dimostra il rilievo che normalmente assume nel dibattito sviluppato attorno a piattaforme cloud riconducibili a fornitori extra UE.

Possiamo, in maniera grossolana, scindere i problemi che possono prospettarsi entro due macro-categorie:

- criticità connesse ad attività di trattamento da parte di Autorità straniere, svolte per finalità di *intelligence*, difesa e sicurezza nazionale, in conformità con la normativa di diritto pubblico del Paese terzo;

- criticità connesse a richieste di dati personali promosse da Autorità giurisdizionali/amministrative di Paesi terzi.

Va rilevato che la distinzione proposta è solo orientativa e sono possibili sovrapposizioni, nel senso che anche trattamenti per finalità di *intelligence* possono trovare fasi di verifica giurisprudenziale, anche se sovente attraverso tribunali speciali[14].

Intelligence, difesa e sicurezza nazionale di Paesi terzi

Procedendo nell'ordine posto, è la prima macro-categoria quella sulla quale è stata costruita la decisione Schrems II (e altresì, in realtà, la precedente Schrems I, ossia CGUE, 6 ottobre 2015, C-362/14). Naturalmente, l'esame della normativa statunitense costituisce, in tal senso, solo un pratico *case study*, in quanto già oggetto di compiute riflessioni, ma va da sé che la stessa impostazione di metodo deve essere applicata ed estesa a qualsivoglia Paese terzo, dunque, e a titolo di esempio, alla Cina e alla normativa cinese, nel caso si ponga la questione della fornitura di piattaforma cloud cinese o di utilizzo di infrastrutture cinesi[15].

Venendo comunque al contesto statunitense, la Corte di Giustizia UE nella pronuncia richiamata si sofferma soprattutto su due fonti normative, la *Section* 702 del Foreign Intelligence Surveillance Act (FISA) e l'E.O. 12333 (cfr. sentenza cit., § 60 e ss.). Vale la pena citare qualche estratto della pronuncia, per una più chiara contestualizzazione.

La prima disposizione, rileva il giudice europeo, "*consente al procuratore generale e al direttore dell'intelligence nazionale di autorizzare congiuntamente, previa approvazione*

14 Per es., la e *Foreign Intelligence Surveillance Court* (FISC) rispetto al FISA.

15 Cfr. la posizione critica recentemente espressa dalla Commissione in *Una Strategia europea per i dati*, p. 4: "*In Cina si assiste a una combinazione tra sorveglianza governativa e forte controllo delle imprese Big Tech su massicce quantità di dati, senza sufficienti garanzie per i cittadini*". Cfr. altresì, in senso più generale, p. 10: "*I fornitori di servizi che operano nell'UE possono altresì essere soggetti alla legislazione di Paesi terzi, con il rischio che le giurisdizioni di tali paesi che non sono conformi alla normativa dell'UE in materia di protezione dei dati abbiano accesso ai dati dei cittadini e delle imprese dell'UE; è stata in particolare espressa preoccupazione in merito ad alcune leggi cinesi relative alla cibersicurezza e all'intelligence nazionale*".

della Corte FISA, la sorveglianza di cittadini ***stranieri*** *che si trovano al di fuori del territorio degli Stati Uniti e serve, in particolare, quale fondamento dei programmi di sorveglianza PRISM e UPSTREAM. Nell'ambito del programma PRISM,* ***i fornitori di servizi Internet*** *sono tenuti, secondo le constatazioni di tale giudice, a fornire alla NSA tutte le comunicazioni inviate e ricevute da un «selettore»*[16]*, e parte di esse è trasmessa anche allo FBI e alla Central Intelligence Agency (CIA) (agenzia centrale per l'intelligence). Per quanto riguarda il programma UPSTREAM, detto giudice ha constatato che, nell'ambito di tale programma, le imprese di telecomunicazioni che gestiscono la* ***«dorsale» di Internet*** *– vale a dire la rete di cavi, commutatori e router – sono costrette a consentire alla NSA di copiare e filtrare i flussi di traffico Internet al fine di raccogliere comunicazioni inviate da, dirette a o riguardanti il cittadino straniero interessato da un «selettore». Nell'ambito di tale programma, la NSA, secondo le constatazioni del medesimo giudice, ha accesso tanto ai metadati quanto al contenuto delle comunicazioni interessate*" (§§ 61-62).

Prosegue la Corte: "*Per quanto riguarda l'E.O. 12333, il giudice del rinvio constata che esso consente alla NSA di accedere a dati «in transito» verso gli Stati Uniti, accedendo ai cavi sottomarini posti sul fondale dell'Atlantico, nonché di raccogliere e conservare tali dati prima che essi giungano negli Stati Uniti e siano ivi soggetti alle disposizioni del FISA. Esso precisa che le attività fondate sull'E.O. 12333 non sono disciplinate dalla legge*" (§ 63).

In linea generale, i fornitori statunitensi di tecnologia cloud possono essere considerati soggetti alla citata disposizione del FISA in quanto "*electronic communication service providers*".

16 Cfr. altresì *The FISA Amendments Act: Q&A*, unclassified, 18 aprile 2017, p. 2: "*Section 702 permits the government to target for surveillance foreign persons located outside the United States for the purpose of acquiring foreign intelligence information (with the compelled assistance of electronic communication service providers) while also providing a comprehensive oversight regime by all three branches of government to protect the constitutional and privacy interests of any U.S. person whose information may be incidentally acquired during the collection activity*", https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

La tipologia di rischio individuata in base al modello DRI è qui essenzialmente quella della perdita di riservatezza, con le conseguenze che ne derivano per l'interessato, venendo in considerazione l'ambito dell'*intelligence* e, a seconda dei casi, dell'antiterrorismo.

Rispetto alle fonti richiamate, la sentenza Schrems II ha ritenuto che la sorveglianza fosse massiva e che il livello di protezione per i cittadini europei, derivante da tale quadro normativo, fosse incompatibile con la Carta dei diritti fondamentali dell'Unione e con il RGPD.

Fotografato in tal modo il contesto normativo, ci si deve domandare se sia solo il trasferimento di dati personali verso gli Stati Uniti a porsi in contrasto con la struttura di tutele vigente nell'Unione e se, pertanto, la localizzazione delle infrastrutture cloud nella UE possa costituire un rimedio. Sotto questo profilo, giova positivamente notare che da tempo alcuni provider extra europei hanno creato *data center* nell'Unione Europea e garantiscono, spesso attraverso società controllate, una circolazione delle informazioni esclusivamente all'interno della "bolla" territoriale dell'Unione: in altre parole esiste già un cloud "europeo", sia pure non gestito da società europee o partecipato da Stati membri. Occorre, tuttavia, comprendere se anche alle controllate UE di fornitori di cloud statunitensi sia comunque applicabile la *Section* 702 FISA, e dunque se la localizzazione europea perda, sotto tale profilo, rilevanza sostanziale.

Va ad ogni modo tenuto conto che la responsabilità di garantire la conformità della piattaforma al RGPD e alla Carta dei diritti fondamentali dell'Unione Europea - ossia, rispetto all'ipotesi esaminata, l'assenza di flussi informativi carenti di base giuridica e requisiti di liceità verso autorità statunitensi - grava innanzitutto proprio sulle controllate UE dei suddetti fornitori. È infatti pacifica, da un lato, l'applicazione dell'art. 3 RGPD e dall'altro la piena inclusione dei trattamenti per ragioni di sicurezza nazionale di Paese terzo entro il perimetro applicativo del Regolamento[17]. Tale profilo di responsabilità potrà dunque essere ben

17 Cfr. CGUE *cit.* § 81: "*A tal riguardo, occorre anzitutto rilevare che la disposizione contenuta nell'articolo 4, paragrafo 2, TUE, secondo la quale all'interno dell'Unione la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro, riguarda esclusivamente gli Stati membri dell'Unione. Di conseguenza, tale disposizione*

declinato nella richiesta di idonee garanzie e di richieste di chiarimento legale da parte dei committenti che affidano in cloud i dati, facendo evidentemente privilegiare i fornitori in grado di fornire tali garanzie.

Va anche considerato, sotto un profilo del tutto diverso, che una misura pratica di contenimento del rischio di applicazione della citata *Section* 702 FISA può essere ravvisata nell'utilizzo di tecniche robuste di **cifratura**, direttamente e autonomamente attivabili dagli utenti del servizio cloud. In tal modo – fatte salve vulnerabilità sconosciute nei protocolli o l'utilizzo di computer quantistici per decifratura – si viene infatti a contrastare il rischio di perdita di riservatezza (*confidentiality*) dei dati, ossia il fattore di rischio appunto ravvisato in applicazione del modello DRI, collocando così a monte, cioè al livello del committente/utente, il livello dell'accesso in chiaro alle informazioni. Non a caso, la cifratura costituisce una misura validamente contemplata nelle Linee guida europee sul *data breach* proprio in relazione al rischio di perdita di riservatezza[18]. Le stesse considerazioni non possono, dunque, che essere trasposte anche nel contesto qui esaminato.

La localizzazione delle infrastrutture cloud nel territorio dell'Unione Europea permette invece e unicamente di far fronte, nei limiti in cui si accompagni a forme di effettivo controllo della continuità operativa del cloud da parte degli Stati membri, al diverso rischio (pur talvolta paventato) costituito da interruzioni di servizio collegate a ipotetiche tensioni internazionali. Lo scenario è ovviamente diverso dalla tematica finora considerata della sorveglianza a fini di *intelligence* e non appare formulato rispetto a specifici Paesi terzi, ma esaminato solo quale mera eventualità geopolitica. In questo caso, la tipologia di rischio che viene in considerazione in un modello DRI è quella della disponibilità dei dati ed, eventualmente (a seconda dei casi), altresì dell'integrità, ma tale rischio si presta appunto a essere contenuto attraverso la fisica collocazione delle infrastrutture nell'Unione.

---

non è pertinente, nel caso di specie, ai fini dell'interpretazione dell'articolo 2, paragrafo 1, e dell'articolo 2, paragrafo 2, lettere a), b) e d), del RGPD".

18 Cfr. WP29/EDPB, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, WP250 rev. 01.

Richieste promosse da Autorità giurisdizionali di Paese terzo

Venendo alla seconda macro-categoria di criticità connesse con l'applicazione della normativa di Paese terzo, essa riguarda gli ordini di esibizione di dati formulate da autorità giudiziarie o amministrative straniere. Anche qui il caso di studio più ricco per l'analisi giuridica è fornito dal contesto normativo nordamericano, e anche qui vale il principio che la valutazione deve essere naturalmente condotta in generale rispetto a qualsiasi autorità richiedente di qualsiasi Paese terzo. La tipologia di rischio in base al modello DRI è quella di una perdita di riservatezza dell'informazione.

Dal punto di vista normativo, è necessario ricordare che, qualora sussista un trattamento di dati personali, l'art. 48 RGPD impone come condizione necessaria, ai fini della liceità della comunicazione, la sussistenza di "*un accordo internazionale in vigore tra il Paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria*". Un_accordo di questo genere è stato sottoscritto nel 2003[19] (in un contesto, però, oggi in parte insoddisfacente rispetto ad alcune attuali esigenze di cooperazione giudiziaria). Concretamente, un'ipotesi di ordine diretto, a prescindere cioè dal citato accordo bilaterale, si è posta nel 2016 in occasione della controversia Microsoft Ireland c. Stati Uniti, decisa dalla Suprema corte il 17 aprile 2018, concernente un ordine giudiziale di accesso a dati collocati su server irlandesi, formulato da un'Autorità giudiziaria statunitense e opposto in giudizio dalla controllata europea della società americana.

Successivamente, il 23 marzo 2018, è entrato in vigore il Cloud Act, che ha emendato lo Stored Communications Act (SCA) del 1986. La novella normativa risulta applicabile ai soggetti di diritto statunitense e, a secondo lo studio congiunto, sia pure preliminare, condotto nel 2019 dal Comitato Europeo per la Protezione dei Dati (EDPB) e dall'Autorità di controllo delle istituzioni dell'Unione (EDPS) con dell'EDPB-EDPS, è probabile che scavalchi

19 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22003A0719(02)&from=EN.

l'attuale accordo bilaterale esistente tra Unione europea e Stati Uniti[20]. Dunque, il Cloud Act pone, sotto tale profilo, una tendenziale criticità rispetto all'art. 48 RGPD e richiederebbe un nuovo accordo tra Stati membri e/o Unione Europea e USA in tali ambiti (strumento, peraltro, previsto dallo stesso Cloud Act).

Il lavoro evidenzia altresì che elemento portante dell'atto normativo in commento è l'irrilevanza del luogo in cui si trovano i dati oggetto dell'ordine. In questo rispetto, dunque, eventuali scelte di localizzazione nel territorio dell'Unione Europea si rivelano inefficaci rispetto alla portata normativa, ove il fornitore del servizio di cloud computing risulti essere una società di diritto statunitense o comunque una sua controllata.

In verità, la portata territoriale del Cloud Act ha diramazioni giuridiche tutte da accertare. Nello studio congiunto viene per esempio notato: "*Other questions regarding the scope of application of the US CLOUD Act remain to be resolved, (e.g. whether it applies to* ***EU operators*** *with some "presence" in the US, and how the concept of "control" is to be interpreted in practice, in particular with regard to* ***affiliated companies*** *of US based companies, established in the EU)*"[21]. Se queste ipotesi dovessero trovare conferma, la situazione di alcuni fornitori europei sarebbe cioè assimilabile a quella delle società statunitensi, venendo meno sostanziali differenze giuridiche.

Anche in questo caso, possono ripetersi considerazioni già formulate rispetto ad attività di sorveglianza extra UE per finalità di *intelligence*, ossia che è responsabilità della società potenzialmente soggetta al Cloud Act dare sufficienti garanzie circa la conformità del trattamento al RGPD. Sotto tale profilo, la massa economica del fornitore costituisce in linea generale un elemento di affidabilità, poiché, opportunamente valorizzato, si pone come

20 Cfr. EDPB e EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, 10 luglio 2019, pag. 1: "*By choosing to create a legal avenue under US law for US law enforcement authorities to require disclosure of personal data directly from service providers who fall under US jurisdiction, irrespective of where the data is stored, the US Congress enacts into US law a practice of US governmental entities likely to bypass the Mutual legal assistance in criminal matters treaty (MLAT) in force between the European Union and the United States of America*".

21 Ivi, p. 2.

fattore di resilienza giuridica a richieste contrastanti con l'art. 48 RGPD e alle altre disposizioni del Regolamento europeo, laddove di converso è prevedibile che soggetti giuridici con scarsa massa economica rischino di essere travolti.

Fatte queste osservazioni, occorre in ogni caso contestualizzare la casistica dei flussi di dati per ordine di autorità giudiziarie o amministrative rispetto a quelli connessi a finalità di sorveglianza massiva per attività di *intelligence*. Nella prima ipotesi, vengono di regola in considerazione richieste mirate, non esplorative, basate su *fumus* di evidenza e assistite dalle garanzie di un processo ordinario, sia pure con tutte le limitazioni di tutela che riguardano i cittadini non statunitensi avanti a Corti statunitensi.

Come in precedenza, una misura di contrasto al rischio consistente nella perdita di riservatezza (*confidentiality*) dei dati personali oggetto di ordini giudiziari o amministrativi può essere ravvisata nella cifratura degli stessi da parte dei committenti/utenti stessi del servizio cloud.

Infine, occorre tenere presenti considerazioni di reciprocità. Infatti, in maniera speculare, anche le autorità giudiziarie europee hanno pieno interesse ad accedere per attività giudiziaria e di indagine a evidenze informatiche conservate presso società con sede negli Stati Uniti: si pensi al *vulnus* che potrebbe derivarne rispetto a indagini relative a fenomeni di criminalità organizzata. In altre parole, la materia della collaborazione giudiziaria è intrinsecamente multilaterale, e il rischio posto da brusche interruzioni andrebbe complessivamente valutato alla luce della potenziale perdita di occasioni di reciprocità. Sul punto, giova ricordare che la stessa Unione europea si sta dotando di una normativa in materia di *e-evidence*, al momento in attesa di approvazione, e sta avviando apposite interlocuzioni con gli Stati Uniti[22] per il raggiungimento di un accordo di collaborazione in regime di reciprocità con il Cloud Act.

22 Cfr. Commissione UE, *Una strategia europea per i dati*, *cit.*, pp. 10-11: "*Sebbene la legislazione dei Paesi terzi, quale il CLOUD Act degli Stati Uniti, si fondi su obiettivi di ordine pubblico come l'accesso delle autorità di contrasto ai dati per lo svolgimento di indagini giudiziarie, l'applicazione della legislazione di giurisdizioni straniere solleva preoccupazioni legittime per le imprese, i cittadini e le autorità pubbliche europee in merito all'incertezza giuridica*

Due connotati emergenti del progetto del cloud nazionale

Gli elementi di perplessità rapidamente analizzati in rapporto alle attività di sorveglianza per finalità di *intelligence* e di ordini amministrativi/giudiziari rivelano, in definiva, il loro aspetto più delicato in profili di natura giurisdizionale, profili che, cioè, riguardano l'ampio raggio applicativo di alcuni atti normativi vigenti in ambito extra UE. Realisticamente, non è agevole individuare soluzioni immediate, stante l'evidente impraticabilità dell'idea di soppiantare all'improvviso fornitori all'avanguardia tecnologica, saldamente confermati dal mercato, abilitanti servizi pubblici essenziali o comunque l'esercizio di diritti e libertà fondamentali anche per i cittadini dell'Unione Europea. Si potrebbero, al più, nell'immediato, studiare forme giuridiche di inquadramento societario eventualmente in grado di sottrarsi, ammesso che sia possibile, al raggio applicativo della normativa estera. Altra soluzione pragmatica è quella, già più volte considerata, di far adottare ai committenti/utenti tecniche robuste di cifratura delle informazioni, che le rendano non intelligibili ai provider e con ciò alle autorità terze richiedenti.

Calando a questo punto l'analisi sul progetto di cloud nazionale nel caso italiano, giova sottolineare che il modello in fase di elaborazione da parte del Governo non esclude una partecipazione all'infrastruttura dei grandi fornitori extra UE. Sotto questo rispetto, il progetto, come già indicato in apertura di questo lavoro, appare piuttosto costruito su una ripartizione di rilevanza strategica delle informazioni trattate in cloud, il che appare corretto, e sulla mera valorizzazione di una coordinata spaziale (la localizzazione nazionale, cfr. in proposito anche art. 35, co. 1, lett. a), D.L. 16 luglio 2020, n. 76, ved. appresso), ma non anche di una coordinata giurisdizionale (la legge estera applicabile al fornitore)[23].

---

e alla conformità al diritto applicabile dell'UE, quale la normativa in materia di protezione dei dati. L'UE sta operando per attenuare tali preoccupazioni mediante una cooperazione internazionale reciprocamente vantaggiosa, ad esempio la proposta di un accordo UE-USA per facilitare l'accesso transfrontaliero alle prove elettroniche, che attenui il rischio di conflitto di leggi e stabilisca chiare tutele per i dati dei cittadini e delle imprese dell'UE. L'UE sta inoltre lavorando a livello multilaterale, anche nel contesto del Consiglio d'Europa, per elaborare norme comuni sull'accesso alle prove elettroniche, basate su un elevato livello di protezione dei diritti fondamentali e procedurali".

23 Cfr. Lugi Garofalo, *Cloud nazionale, Pisano non esclude le big tech Usa*, in *Key4Biz.it*, 4 settembre 2020, https://www.key4biz.it/cloud-nazionale-pisano-non-esclude-le-big-tech-usa/319717/. Per analoghe considerazioni,

Le ragioni del coinvolgimento dei provider extra UE appaiono sostanzialmente pragmatiche e riflettono la difficoltà percepita di sostituire le prestazioni già fornite con altre soluzioni nazionali, come si evince anche dalle dichiarazioni rese dalla Ministra per l'innovazione italiana a proposito dei lineamenti del nuovo assetto di fornitura: "*La nostra strategia per il cloud e per le infrastrutture digitali non può rinunciare a fare i conti con la realtà. Perciò prevede l'utilizzo di soluzioni già esistenti nella Pubblica amministrazione, di infrastrutture che attualmente possono fornirci soltanto gruppi stranieri*"[24]. Ciò che sembrerebbe nuovo è il "contenitore" giuridico e il rafforzato controllo pubblico sul profilo decisorio e gestionale. Non è possibile, al momento, valutare se e in che termini questa diversa impostazione, insieme legale e di struttura, sia in grado di mitigare l'applicazione della portata extraterritoriale della giurisdizione straniera, non essendo stati resi pubblici, diversamente dall'omologo Gaia-X, documenti che descrivano le specifiche del progetto, la cui conoscenza è dunque limitata ai cenni forniti dalla Ministra in interviste e dichiarazioni. Ciò non rende possibile valutare, ancora, in termini concreti il reale apporto di novità.

L'erogazione del supporto tecnologico-infrastrutturale essenziale da parte dei fornitori di cloud extra EU costituisce finora un dato pacifico e prescinde perfino dalla necessità che il fornitore abbia una rappresentanza in Italia. Si vedano, in proposito, l'art. 5 circolare 3/2018 e l'art. 5 circolare 2/2018 estero dell'Agenzia per l'Italia Digitale (AgID): "*Nel caso in cui un fornitore non abbia alcuna rappresentanza diretta o indiretta in Italia, AgID su segnalazione di un'amministrazione proponente, acquisisce le informazioni necessarie alla qualificazione e potrà avviare d'ufficio la procedura mediante la piattaforma AgID dedicata alla qualificazione, secondo le modalità pubblicate sul sito Cloud Italia all'indirizzo: https://cloud.italia.it/*".

cfr. altresì Luigi Garofalo, *Pisano: "Definire le regole per il cloud europeo, ma non è possibile escludere le Big Tech dalla Pa", in Key4Biz.it*, 5 agosto 2020, https://www.key4biz.it/pisano-definire-le-regole-per-il-cloud-europeo-ma-non-e-possibile-escludere-le-big-tech-dalla-pa/317590/.

24 Cfr. ult. loc. cit.

Conflitti tra obblighi di localizzazione e disciplina eurounitaria

Aprendo un diverso fronte di analisi, ossia quello del rapporto giuridico tra cloud nazionale (o più in generale soluzioni di localizzazione) e normativa dell'Unione Europea, devono segnalarsi alcuni profili di attenzione rispetto al Regolamento europeo sul trattamento dei dati non personali. Il Regolamento, ai sensi dell'art. 2, si applica alle "*attività di trattamento elettronico di dati elettronici diversi dai dati personali nell'Unione che: a) sono fornite come servizio ad utenti residenti o stabiliti nell'Unione, indipendentemente dal fatto che il fornitore di servizi sia o non sia stabilito nell'Unione; b) sono effettuate da una persona fisica o giuridica residente o stabilito nell'Unione per le proprie esigenze*". Per "user" si intende "*una persona fisica o giuridica, compreso un'autorità pubblica e un organismo di diritto pubblico, che utilizza o richiede servizi di trattamento di dati*". Tale regolamento appare dunque applicabile anche ai servizi cloud della Pubblica Amministrazione.

In particolare, con riferimento al caso italiano, andranno presi in considerazione, ai fini dell'analisi, qui possibile in termini necessariamente sintetici, gli obblighi di localizzazione emergenti dall'art. 9, co. 2 DPCM 3 dicembre 2013, recante "*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*", e il disposto dell'art. 33-*septies*, co. 1 D.L. 18 ottobre 2012, n. 179, come modificato dall'art. 35, co. 1, lett. a), D.L. 16 luglio 2020, n. 76.

Seguendo l'ordine, la prima disposizione indica: "*Fatto salvo quanto previsto dal decreto legislativo 22 gennaio 2004, n. 42, in ordine alla tutela, da parte del Ministero dei beni e delle attività culturali e del turismo, sugli archivi e sui singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico, i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul*

territorio nazionale e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle stabilite dal presente decreto".

La seconda disposizione prevede: "*La Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) definiti al comma 2, destinata a tutte le pubbliche amministrazioni*". L'infrastruttura nazionale è progettata al fine di garantire un approdo sicuro di migrazione a centri per l'elaborazione delle informazioni sprovvisti dei requisiti di sicurezza fissati da AgID secondo quanto previsto dal comma quarto dell'articolo in esame. In alternativa, potrà essere adottata la soluzione di cui al comma 4-*ter* oppure la migrazione potrà avvenire verso eventuali CED propri conformi ai già cennati requisiti oppure infine, e per quanto qui maggiormente interessa, la migrazione verso soluzioni cloud in linea con i suddetti requisiti previsti da AgID. Siamo dunque dinanzi a un quadro di possibilità costruito su una pluralità di alternative.

Fermo restando che dalla complessiva formulazione non pare desumersi l'introduzione di un vincolo di localizzazione nazionale, nel senso proprio di questo termine, giova, prima di formulare ulteriori considerazioni, ricostruire brevemente il quadro normativo introdotto con il citato reg. (UE) 2018/1807 sul trattamento di dati non personali e la *ratio* ad esso sottesa. Pietra angolare della disciplina eurounitaria è l'art. 4, par. 1 del Regolamento in questione, che dispone espressamente il divieto di "obblighi di localizzazione di dati", salvo eccezioni (ved. prossimo paragrafo). Per "obbligo di localizzazione", come chiarito all'art. 3, par. 1, n. 5), si intende "*qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro*".

La *ratio* è meglio chiarita dai considerando. Ad esempio, il secondo reca: "*Il funzionamento efficace ed efficiente del trattamento di dati costituisce un elemento fondamentale di qualsiasi catena del valore dei dati. Eppure, tale trattamento di dati efficace ed efficiente e l'evoluzione dell'economia dei dati nell'Unione sono compromessi principalmente da due tipi di ostacoli relativi alla mobilità dei dati e al mercato interno: gli obblighi in materia di localizzazione dei dati posti in essere dalle autorità degli Stati membri e pratiche di «vendor lock-in» nel settore privato*". Medesime considerazioni sono sviluppate ai successivi considerando 3 e 4. Il considerando 6 collega poi espressamente al settore del *cloud computing* (cfr. anche cons. 17) i due ostacoli predetti e quelli ulteriori connessi a profili giuridici contrattuali e tecnici che impongono limitazioni (così al precedente cons. 5), evocando, in diretta connessione con tali ostacoli, due ordini di pregiudizi:

- alla libertà di concorrenza, richiamata espressamente anche al cons. 18;
- al progresso della ricerca e sviluppo.

Sostanzialmente – sia permessa una sintesi grezza – la localizzazione obbligatoria è equiparata, *mutatis mutandis*, a una sorta di *vendor lock-in* di matrice pubblicistica.

Vale la pena riportare il considerando 6, che illustra chiaramente la *ratio* dell'impostazione eurounitaria: "*La combinazione di tali ostacoli ha determinato una mancanza di concorrenza tra i fornitori di servizi cloud nell'Unione, diversi problemi di «vendor lock-in» e gravi carenze in termini di mobilità dei dati. Analogamente, le politiche di localizzazione dei dati hanno compromesso la capacità delle aziende di ricerca e sviluppo di agevolare la collaborazione tra imprese, università e altre organizzazioni di ricerca allo scopo di sostenere l'innovazione*".

Il cons. 13 del reg. (UE) 2018/1807 invita le autorità e gli organismi di diritto pubblico ad astenersi dall'applicare limitazioni restrittive attraverso localizzazioni ("*refrain from making data localisation restrictions*"[25]).

25 Si riporta il testo nella versione inglese, essendo qui errata la traduzione ufficiale italiana.

In senso ancora più chiaro il cons. 18, che conviene riportare per intero: "*Gli obblighi di localizzazione dei dati costituiscono un chiaro ostacolo alla libera prestazione di servizi di trattamento di dati in tutta l'Unione e al mercato interno. In quanto tali, dovrebbero essere vietati tranne quando siano giustificati da motivi di pubblica sicurezza, ai sensi del diritto dell'Unione, in particolare ai sensi dell'articolo 52 TFUE, e soddisfino il principio di proporzionalità sancito dall'articolo 5 TUE. Al fine di dare concreta attuazione al principio della libera circolazione transfrontaliera dei dati non personali, assicurare la rapida rimozione degli obblighi di localizzazione dei dati esistenti e consentire, per motivi operativi, il trattamento di dati in più località distribuite nel territorio dell'Unione, e atteso che il presente regolamento prevede misure per garantire la disponibilità dei dati ai fini del controllo di regolamentazione, è opportuno che gli Stati membri possano invocare unicamente la sicurezza pubblica come giustificazione per gli obblighi di localizzazione dei dati*".

È utile notare che ai sensi dall'art. 4, co. 2 (cfr. anche cons. 20) gli Stati membri devono comunicare immediatamente alla Commissione qualsiasi progetto di atto che introduca un nuovo obbligo di localizzazione dei dati o ne modifichi uno esistente, conformemente agli artt. 5-7 direttiva (UE) 2015/1535. Quanto invece agli obblighi preesistenti al regolamento, essi vanno rimossi entro il 30 maggio 2021, come dispone il comma 3, a meno di giustificazione idonea che sarà sottoposta al vaglio della Commissione.

Riassunti dunque i lineamenti essenziali del quadro normativo introdotto dal regolamento (UE) 2018/1807, e riprese le due disposizioni nazionali richiamate in apertura, possono formularsi fondate perplessità sulla compatibilità con il nuovo quadro europeo della prima di esse, ossia l'art. 9, co. 2 DPCM 3 dicembre 2013 in materia di conservazione dei documenti informatici. Giova del resto constatare la sussistenza di un convincente argomento di conferma *a contrario*, la constatazione cioè che le Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici adottate ai sensi dell'art. 71 del D.lgs. 82/2005 (Codice dell'amministrazione digitale, CAD) nella versione anteriore alle

osservazioni critiche formulate dalla Commissione europea[26] riproducevano, al par. 4.9, primo periodo formulazione ricalcante, nella sostanza[27], proprio quella del DPCM citato, laddove la nuova formulazione, che recepisce le osservazioni della Commissione, reca espressamente: "*Fatto salvo quanto previsto dal Codice dei beni culturali, nel rispetto del principio di libera circolazione dei dati all'interno dell'Unione europea, si sottolinea l'obbligo, in capo al fornitore del servizio di conservazione, di conservare e rendere disponibili* ***le descrizioni del sistema di conservazione*** [non più *"la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale"*, nda] *all'interno del territorio nazionale"*. Il testo reca altresì nota che giova riportare: "Reg. (UE) 2018/1807 all'articolo 4, paragrafo 1 recita: "Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. In definitiva, le ipotesi di localizzazione territoriale dei servizi di conservazione dei documenti informatici, lungi dal costituire una regola, sono ora ricondotte alle sole (poche) eccezioni consentite dal reg. (UE) 2018/1807."

Deve ritenersi che pertanto l'Italia dovrà procedere a riformulare altresì l'art. 9, co. 2 DPCM cit. entro il termine massimo consentito del **30 maggio 2021**: tale data pare, infatti, solo parzialmente compatibile con la perdita di efficacia del succitato DPCM, una volta entrate in piena efficacia le nuove Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici (cosa che avverrà il 9 giugno 2021, considerando l'iter approvativo a norma e tempistiche comportate dall'applicazione dell'art. 71 del Codice dell'amministrazione digitale) come da previsione di cui all'art. 65 comma 10 del Decreto legislativo, 13/12/2017 n° 217 modificativo del CAD stesso.

Quanto all'altra disposizione, ossia quella del novellato 33-*septies*, co. 1 D.L. 18 ottobre 2012, n. 179, essa da un lato contempla alternative che ne limitano il profilo

26 La notizia è riportata sul sito AgID in data 1° aprile 2020 https://www.AgID.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/04/01/precisazioni-sulla-pubblicazione-nuove-linee-guida-sulla-formazione-gestione

27 "*Fatto salvo quanto previsto dal Codice dei beni culturali, i sistemi di conservazione delle Pubbliche Amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e garantiscono un accesso ai dati presso la sede del Titolare dell'oggetto di conservazione e misure di sicurezza conformi a quelle stabilite dalle presenti linee guida*".

vincolante, come già notato dall'altro potrebbe essere ricondotta a taluna delle eccezioni previste dal regolamento europeo in esame, ad esempio all'internalizzazione (organizzazione interna, ved. sotto).

Libera circolazione - Eccezioni della sicurezza pubblica e del trattamento interno

Conviene soffermarsi su due limiti all'applicazione della disciplina europea: quello che fa leva sull'organizzazione interna degli Stati membri e quello che fa leva su esigenze di sicurezza pubblica.

Quanto al primo, prevede l'ultimo capoverso dell'art. 2, par. 1 reg. cit.: "*Il presente regolamento fa salve le disposizioni legislative, regolamentari e amministrative relative all'**organizzazione interna** degli Stati membri che attribuiscono tra autorità pubbliche e organismi di diritto pubblico quali definiti all'articolo 2, paragrafo 1, punto 4 della direttiva 2014/24/UE poteri e responsabilità in materia di trattamento dei dati, senza remunerazione contrattuale di soggetti privati, nonché le disposizioni legislative, regolamentari e amministrative degli Stati membri che prevedono l'esercizio di tali poteri e responsabilità*". L'intelligenza della disposizione è meglio chiarita dal cons. 14, che giova riportare: "*Come la direttiva 2014/24/UE, il presente regolamento fa salve le disposizioni legislative, regolamentari e amministrative relative all'organizzazione interna degli Stati membri [...]. Mentre le autorità pubbliche e gli organismi di diritto pubblico sono incoraggiate a considerare i vantaggi economici e di altro tipo dell'esternalizzazione a fornitori esterni di servizi, essi potrebbero avere ragioni legittime per scegliere **l'autofornitura** di servizi o **l'internalizzazione**. Di conseguenza, il presente regolamento non obbliga in alcun modo gli Stati membri a subappaltare o esternalizzare la fornitura di servizi che essi intendono fornire direttamente o organizzare con mezzi diversi dagli appalti pubblici*". Come indicato nella citata *Guidance on the Regulation on a framework for the free flow of non-personal*

data in the European Union, rientra in tale ipotesi il caso di "*una agenzia IT centralizzata per fornire servizi di trattamento di dati per le istituzioni e gli enti pubblici*"[28], ipotesi che sembra inscriversi entro l'alveo dell'art. 33-*septies*, co. 1 sopra richiamato, almeno fino a quando non siano coinvolti soggetti privati con remunerazione contrattuale.

Quanto all'altro limite applicativo, costituito da trattamento connesso con ragioni di **sicurezza pubblica**, conformemente al disposto dell'art. 4 TUE, occorre notare che il concetto di "sicurezza pubblica" va adeguatamente definito e perimetrato, non tollera cioè una nozione lasca o generica, in applicazione dei citati artt. 52 TFUE e 5 TUE. Deve altresì essere interpretato entro stretti margini, al pari di tutte le norme eccezionali e limitative di diritti di portata generale (Carta UE 52, par. 1). Giova notare che il cons. 19 reg. (UE) 2018/1807 fornisce una definizione normativa di "sicurezza pubblica" aggiornata alla giurisprudenza della Corte di giustizia, che è opportuno riportare: "*La nozione di «pubblica sicurezza» ai sensi dell'articolo 52 TFUE, nell'interpretazione datane dalla Corte di giustizia, riguarda la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati. Presuppone l'esistenza di una minaccia* ***reale e sufficientemente grave*** *a uno degli interessi fondamentali della società, quale il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché all'incolumità della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari. Conformemente al principio di proporzionalità, gli obblighi di localizzazione dei dati giustificati da motivi imperativi di pubblica sicurezza dovrebbero essere* ***adatti*** *al raggiungimento dell'obiettivo perseguito e* ***limitarsi*** *a quanto è necessario per conseguire tale obiettivo*".

Non si ravvisano, invece, nel Regolamento generale sulla protezione dei dati personali (RGPD) analoghe considerazioni rispetto a obblighi di localizzazione, ancorché pure in tale ambito normativo il principio della libera circolazione dei dati trovi non soltanto

28 Ivi, pp. 17-18.

riconoscimento ma costituisca espressamente pilastro fondamentale della normativa, accanto naturalmente a quello della costruzione di un solido guscio di garanzie intorno a quei dati che si riferiscono appunto alle persone fisiche. I due poli concettuali – libera circolazione e tutela individuale – devono dialogare. A ben guardare, da un lato la stessa portata extraterritoriale di cui all'art. 3 RGPD e, dall'altro, le garanzie previste per i trasferimenti a Paesi terzi (Capo V) si prestano a essere lette in rapporto con il sottostante principio della libertà di circolazione (cfr. in proposito il cons. 6 RGPD: "*La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso Paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali*"). Impostato in questi termini il rapporto tra i due corpi normativi, ci si potrebbe effettivamente domandare quali ragioni giustifichino, sia pure in mancanza di espresso divieto, la liceità di obblighi di localizzazione rispetto al trattamento di dati personali, posto che la natura personale del dato sembra solo connessa con una esigenza di adeguata tutela e non anche con la collocazione fisica del *data center* entro uno specifico Stato membro, tenuto anche conto del fatto che il livello di garanzia è assunto con il RGPD *ex lege* come identico in ogni Stato membro[29].

Anche a prescindere da quanto sopra, devono poi rilevarsi le difficoltà pratiche di distinguere tra sistemi che trattano dati personali e non personali, considerato che, da un lato, sono facilmente configurabili situazioni miste e, dall'altro, che il concetto di dato "personale" è pervasivo e dinamico: per essere più chiari, se un set di dati non personali

29 Può essere utile riportare un estratto delle considerazioni espresse da Roberto Viola, direttore generale della DG Connect presso la Commissione europea, nell'imminenza dell'introduzione reg. (UE) 2018/1807, cfr. Id., *Free flow of data in the EU – a pathway into the cloud*, 12 novembre 2018, https://ec.europa.eu/digital-single-market/en/blogposts/free-flow-data-eu-pathway-cloud: "*Thanks to the new General Data Protection Regulation (GDPR), rules on the free movement of personal data in the European Union have been clarified and citizens' data is now guaranteed to be protected. Until recently however, there was no legislation dealing with the free flow of non-personal data in European legislation. At the same time, several Member States introduced legislation requiring certain data to be stored or processed within their national borders. These ""data localisation requirements"" were hindering the development of the EU data economy by stopping the emergence of data innovation ecosystems across European borders. They were also creating inefficiencies by requiring companies active in multiple Member States to duplicate IT infrastructure*".

può essere collegato a un certo punto a un set di dati personali diviene anch'esso un set di dati personali, e viceversa se un set di dati personali può essere a un certo punto privato della componente di collegamento anche indiretto a persone fisiche diviene un set di dati non personali. A fronte di questa mobilità di qualificazione, la localizzazione non appare altrettanto flessibile da consentire di accompagnarla.

L'ipotesi della sussistenza di insiemi misti di dati personali e non personali è in effetti considerata dal legislatore all'art. 2, par. 2 reg. (UE) 2018/1807, secondo il criterio così sintetizzato nella *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, p. 9[30]:

- *"il regolamento sulla libera circolazione dei dati non personali si applica alla parte dell'insieme contenente i dati non personali;*
- *la disposizione sulla libera circolazione dei dati del regolamento generale sulla protezione dei dati si applica alla parte dell'insieme contenente i dati personali;*
- *se le parti di dati personali e di dati non personali sono "indissolubilmente legate", i diritti e gli obblighi in materia di protezione dei dati derivanti dal regolamento generale sulla protezione dei dati si applicano pienamente all'insieme di dati misti, anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme di dati*".

È peraltro manifesto che, nonostante le precisazioni indicate, il livello di complessità postulato dalla sussistenza di trattamenti misti pone considerazioni che vanno attentamente esplorate, quali ad esempio la nozione di "indissolubilmente legato". Inoltre, l'approccio indicato non tiene conto della natura "agglutinante" del dato personale cui si è già avuto modo di accennare.

30 COM(2019) 250 final, 29 maggio 2019, *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52019DC0250&from=EN*

Doppio standard e approccio sostanziale

Si sono affrontate più sopra due questioni, oggetto di intenso dibattito, connesse con la portata extra-territoriale di una parte della normativa pubblicistica di Paesi terzi. Affinché esse siano debitamente apprezzate in tutte le loro implicazioni giuridiche, occorre altresì contestualizzarle adottando un rovesciamento di prospettiva. Sembra corretto prendere le mosse da una delle considerazioni portanti della sentenza Schrems II, espressa in vari punti della motivazione e sintetizzata al § 180, dove, richiamate le più ampie considerazioni sviluppate ai §§ 175 e 176, si trova enunciata la seguente massima: "*per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura e impongano requisiti minimi*". Il richiamo è, cioè, a un approccio sostanziale di osservanza dei diritti della persona, che è necessariamente trasversale: non può quindi essere circoscritto ai soli flussi di dati personali verso Paesi terzi. In altre parole: lo standard di garanzia dei diritti fondamentali della persona applicato nei confronti dei Paesi terzi dovrebbe valere in termini altrettanto rigorosi all'interno dell'Unione Europea. Orbene, si desidera portare l'attenzione al fatto che uno dei principali temi di dibattito, ossia l'ingerenza per ragioni di sorveglianza connessa con attività di *intelligence*, incontra, all'interno dell'Unione, un limite giuridico nell'art. 2, par. 2 RGPD[31]. Ciò evidentemente costituisce un paradosso di cui occorre essere consapevoli: ciò che non viene "lasciato passare" in deroga fuori dalla UE, si ammette in UE. Se la *ratio* dell'intera disciplina è, in ultima analisi, la tutela dei diritti fondamentali della persona fisica, non si può non notare che una parte delle stesse ragioni di insoddisfazione legittimamente espresse rispetto ai trattamenti per *intelligence* di Paesi terzi dovrebbero valere per trattamenti di *intelligence* svolti intra UE, sennonché in tale caso non trovano nel RGPD strumenti per essere azionate.

31 Del resto la disposizione citata è inevitabile poiché si inserisce nella stessa architettura del TUE e non può prescindere dall'osservanza del titolo V, capo 2.

Posta in questi termini la questione, emerge in definitiva un doppio standard ("due pesi e due misure"), sul quale si desidera richiamare l'attenzione nella complessiva valutazione giuridica, e che è solo mitigato dalla considerazione che può supplire, in parte, l'art. 8 CEDU, disposizione che non individua esclusioni aprioristiche di materie quanto piuttosto bilanciamenti tra interessi tutelati, che come tali presuppongono ragionamenti sul merito.

Inoltre, anche prescindendo dalle considerazioni espresse in relazione all'ambito materiale di applicazione del Regolamento, si registrano, nell'Unione, situazioni di ingerenza da parte di autorità pubbliche, di ingiustificata compressione dei diritti dell'interessato o perfino di vera sospensione dei diritti che meriterebbero di essere considerate con altrettanta attenzione. In altre parole, la preoccupazione verso quanto avviene nei trattamenti svolti da autorità di Paesi terzi è corretta e giustificata ma, si riconoscerà, affetta, nei termini attuali, da una manifesta forma di strabismo giuridico. Per citare l'ipotesi più vistosa: l'introduzione di limitazioni generali estese e penetranti nell'applicazione del Regolamento disposta dal governo ungherese con decreto 4 maggio 2020, n. 179 solleva perplessità altrettanto gravi rispetto all'attività di *intelligence* svolta da autorità extra-europee, perché avviene appunto, e in modo dirompente, all'interno dell'Unione, e perché riguarda l'applicabilità concreta dell'intero Regolamento. Non a caso, il Comitato Europeo per la Protezione dei Dati (EDPB) ha già preso posizione sulla vicenda nella sua tredicesima riunione plenaria[32].

Anche a prescindere dal caso eclatante appena ricordato, sussistono nello stesso assetto normativo italiano ampie ragioni di perplessità sulla compatibilità di varie limitazioni imposte ai diritti fondamentali dell'interessato nell'interazione con le autorità. Solo a titolo di esempio, si può citare la sussistenza, incredibile, di un obbligo di conservazione generalizzata ed *erga omnes* dei dati di traffico telefonico e telematico, al fine di contrasto del terrorismo anche internazionale, introdotto dall'art. 24 della l. 20 novembre 2017, n. 167,

32 Cfr. EDPB, *Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR*, in https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

norma che induce a un interessante confronto comparatistico con la *Section* 702 FISA, sennonché quest'ultima quantomeno prevede garanzie procedurali e offre tutele ai cittadini del paese che l'ha introdotta. Si attribuisce a Seneca la frase "*Aliena vitia in oculis habemus, a tergo nostra sunt*", i vizi altrui li abbiamo davanti agli occhi, i nostri alle spalle.

Si possono inoltre aggiungere, a titolo di ulteriore esempio per il caso italiano, le vaste prerogative sussistenti in ambito parlamentare per ragioni di autodichia, che riguardano altresì l'area giuridica tutelata dal RGPD, o la formulazione dell'art. 2-*duodecies* d.lgs. 196/03, che fa registrare, al pari del 2-*undecies*, sostanziali perplessità di compatibilità con l'art. 23 RGPD. Ugualmente, andrebbe verificata l'integrale coerenza dell'istituto delle intercettazioni preventive previsto dall'art. 226 delle disposizioni di attuazione del codice di procedura penale con l'assetto delle garanzie eurounitarie, ed eventualmente valutato, se ritenuto necessario ad esito del suddetto vaglio, un rafforzamento di salvaguardie.

Sia ben chiaro, le criticità del diritto nazionale e quelle strutturali nel diritto eurounitario (es. l'art. 2, par. 2 RGPD richiamato) non valgono a sanare eventuali trattamenti di dati non sufficientemente tutelanti i diritti fondamentali svolti da Paesi terzi; tali criticità europee e nazionali impongono, tuttavia, una lettura realistica e un'onesta presa d'atto: paradossalmente, a voler evitare attualmente l'applicazione di un immotivato doppio standard, non è escluso che si debba sospendere con effetto immediato anche attività di trattamento anche all'interno dell'Unione, con conseguenze paralizzanti, dunque impraticabili.

Pare corretto, in definitiva, contestualizzare la pronuncia Schrems II nel più vasto stato di cose che riguarda anche la situazione nazionale e dell'Unione Europea, e trarne conseguenze realistiche sulla necessità di progettare un percorso diretto al raggiungimento di un livello generale di tutela compatibile con la garanzia normativa.

Conclusioni

Il progetto di cloud nazionale nel caso italiano e il parallelo Gaia-X a guida franco-tedesca disegnano uno scenario nel quale emergono con chiarezza indicazioni di politica legislativa dirette alla creazione di infrastrutture cloud sotto il completo, o prevalente, controllo di Stati membri e, in via tendenziale, ma ad oggi solo futuribile, dell'Unione Europea. Riteniamo che questo sia dunque il punto d'ancoraggio. Va osservato che le ragioni nazionali ed europee sottese alle iniziative menzionate sembrano, anche dalle dichiarazioni che le accompagnano, riconducibili più a interessi strategici e politici di rafforzamento della sovranità digitale e di protezionismo di mercato, che ad autentiche preoccupazioni relative al livello di tutela dei diritti fondamentali all'interno dell'Unione.

Occorre notare, sotto quest'ultimo profilo, ossia quello appunto del livello effettivo di tutela giuridica, che le criticità rilevate nella pronuncia cd. "Schrems II" della Corte di giustizia dell'Unione Europea – che segna un approdo rispetto al quale ci può posizionare in senso adesivo o critico ma da cui non si può prescindere – non appaiono del tutto eliminabili attraverso una mera localizzazione intra UE delle infrastrutture, perché sono connesse in misura sostanziale alla portata extraterritoriale di norme di diritto pubblico dei Paesi terzi. Si può avviare un dialogo internazionale con tali Paesi, sperimentare forme di *soft suasion*, ma esse troveranno inevitabili limiti nelle altrui scelte di sovranità nazionale. Appare dunque, realisticamente, improbabile scongiurare la scelta secca alternativa se interrompere completamente i flussi extra UE di dati personali, ossia anche quelli essenziali e non rinunciabili poiché collegati con la stessa disponibilità delle odierne infrastrutture cloud (prendendo atto delle conseguenze enormi che ne deriverebbero) e all'abilitazione all'esercizio di diritti e libertà fondamentali – strada, questa, che apparirebbe in chiaro contrasto con il principio di proporzionalità ex art. 5 del Trattato sull'Unione Europea -, o se concentrare l'attenzione verso modelli di transizione più equilibrati e proporzionati, diretti a creare assetti infrastrutturali meno dipendenti dall'estero, ma pur sempre ecosistemici con l'estero, con tempistica e progettualità adeguate.

Nella fase di transizione che in tal modo viene ad aprirsi, appare ragionevole ricorrere a soluzioni pragmatiche e fare affidamento su fornitori in grado di offrire, per struttura e capitale, garanzie di resilienza giuridica a richieste di governi extra europei, di assicurare eventuali risarcimenti in caso di pregiudizio e di assumersi gli obblighi richiesti dalla normativa europea applicabile, in primo luogo dal RGPD.

Tra le soluzioni pragmatiche giova richiamare le tre seguenti: la segregazione di informazioni considerate maggiormente strategiche, l'applicazione di tecniche di cifratura direttamente attivabili dai committenti/utenti, lo studio di modelli di giuridici di gestione delle infrastrutture europee che garantiscano un maggiore controllo europeo, cercando di non privarsi dell'apporto tecnologico offerto dai fornitori extra UE selezionati dal mercato.

Nella complessiva valutazione delle tutele e in un'ottica di corretto e complessivo bilanciamento dei fattori di rischio, è opportuno non dimenticare, accanto al rischio per così dire "extraterritoriale" appena descritto, l'altro versante del rischio, ossia quello tipico rappresentato dalle violazioni della cybersicurezza, il cui impatto sui diritti fondamentali degli interessati risulta particolarmente intenso e pervasivo (anche perché include l'area degli attacchi governativi riconducibili a Paesi terzi svolti addirittura fuori da un quadro delle regole vigenti nel settore della sicurezza pubblica dei paesi attaccanti). Da questo punto di vista, la scelta del fornitore cloud va allora operata tenendo conto dell'effettivo livello di qualità che esso può offrire rispetto allo stato dell'arte e della tecnica, tenendo cioè in debita considerazione i precedenti di risposta a situazioni critiche, gli investimenti fatti in termini di continuo adeguamento tecnologico, le eventuali coperture assicurative che possono essere attivate in caso di risarcimento, gli SLA (*service level agreement*) e i PLA (*privacy level agreement*), la qualità e dalla frequenza delle verifiche interne e degli audit esterni anche rispetto alle misure organizzative e gli effettivi livelli di formazione applicati agli autorizzati al trattamento, non solo rispetto alla consapevolezza informatica (ivi incluso il contrasto a tecniche di *social engineering*), ma anche rispetto alla consapevolezza normativa.

AUTORI

*__Luca Bolognini__ (l.bolognini@istitutoprivacy.it) è Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati. Avvocato europeo dei dati, è founding partner dello Studio ICTLC - ICT Legal Consulting con sedi a Roma, Milano, Bologna, Amsterdam, Madrid, Helsinki e Melbourne. Ethics & Privacy Advisor per numerosi progetti di ricerca Horizon 2020. Saggista, negli ultimi 10 anni ha pubblicato libri per RCS Etas e Springer, e ha scritto con Enrico Pelino diversi volumi per Giuffrè Francis Lefebvre – tra i quali "Il Regolamento Privacy europeo", primo commentario italiano al GDPR (2016) e l'estesa opera "Codice della Disciplina Privacy" (2019). È stato, inoltre, autore dei pamphlet "Generazione Selfie" per il Corriere della Sera (2014) e "Follia Artificiale – Riflessioni per la resistenza dell'intelligenza umana" per Rubbettino (2018).

**__Enrico Pelino__ (avv.enricopelino@griecopelino.com), PhD in diritto dell'informatica presso l'Università di Bologna, è avvocato esperto in materia di protezione dei dati personali e privacy. Autore di numerosi articoli su riviste di diritto e di informatica, ha scritto con Luca Bolognini tre volumi sul GDPR e sul Codice privacy italiano per Giuffrè Francis Lefebvre. Relatore in conferenze e in master, è altresì Fellow dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati.

www.istitutoitalianoprivacy.it