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

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

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

Simone Calzolaio

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

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

1. Datificazione, intelligenza artificiale, *data dependence*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note

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

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

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

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

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

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

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

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

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

* * *

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

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

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