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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0133 • articolo non sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Simone Calzolaio

La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale
Introduzione

L'Autore è professore associato di Diritto costituzionale presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

1. Che cosa resta dell'utopia di Internet? La rete Internet doveva renderci più liberi, più informati e più consapevoli, più uniti in un unico piccolo mondo, più tutelati e più sicuri rispetto agli altri umani, ai poteri pubblici e ai poteri privati. La rete Internet doveva essere il nuovo stadio e forse anche l'ulteriore inedito lascito delle liberaldemocrazie al mondo. Le cose stanno andando – come per tutte le utopie – molto diversamente. L'avvento e l'evoluzione della rete Internet sono ormai divenute il terreno di una nuova era della regolazione giuridica: l'esigenza di governo della sfuggente società dei dati. Proviamo, in questa sezione monografica della *Rivista italiana di informatica e diritto*, a passare in rassegna – con la piena consapevolezza che la materia di studio è più grande delle capacità di ciascuno – quali sono alcuni dei nuovi ambiti e dei nuovi strumenti di questa sfida regolatoria, da una prospettiva schiettamente liberaldemocratica.

2. La sezione trae spunto dal convegno ICON•S di Bologna su *Il Futuro dello Stato*[1] e dal panel che si è avuto l'opportunità di co-organizzare[2] in tale sede.

Nell'ambito della tematica del *Futuro dello Stato* ci era sembrato interessante porsi il problema – provocatoriamente – della fine della rete Internet così come l'avevamo conosciuta e delle sfide pressanti che l'avvento della società digitale comportava per la democrazia. Il titolo del panel era *La fine di Internet? vulnerabilità della democrazia e regolazione delle piattaforme*, mentre il titolo di questa pubblicazione collettanea non è più esclusivamente rivolto alla regolazione delle piattaforme, ma più ampiamente alle sfide della regolazione e gestione dello spazio digitale.

In effetti, la situazione e la condizione post-pandemica, insieme ai venti di guerra che avvolgono direttamente l'Europa, hanno manifestato l'esigenza di indagare sfide e piste meno battute di quelle della regolazione dei *bad guys* delle *big tech*. I contributi di questa sezione monografica rappresentano esattamente questa nuova dimensione.

3. Il primo aspetto di cui si avverte l'esigenza – a nostro sommesso avviso – è un quadro realistico delle vulnerabilità caratteristiche della società digitale e quindi indotte, specificamente, dal (mutevole) processo di datificazione. Proprio dall'indagine delle vulnerabilità si rendono manifeste le domande aperte ed i profili di tutela costituzionale a maggior rischio: la prima vulnerabilità della società digitale può consistere nella difficoltà ad identificare i caratteri specifici di un ordinamento dei dati (su questo aspetto si avventura il contributo *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*).

Si è ritenuto opportuno – grazie al lavoro di Camilla Lobascio – mettere a disposizione del lettore una tabella riassuntiva dell'evoluzione del diritto europeo dei dati e delle piattaforme, che senza pretesa di esaustività, al fine di agevolare lo studio e il reperimento di materiali normativi, elenca le principali disposizioni del diritto europeo dei dati e delle piattaforme digitali, vigente o ancora in fase di discussione, con specifico link al sito ufficiale dell'Unione europea, ove è possibile approfondire i lavori preparatori e reperire altro materiale ufficiale.

Un secondo aspetto – che emerse proprio grazie ad un puntuale intervento svolto oralmente da Federico Serini in occasione del panel e che contribuì a modificarne l'oggetto, così come descritto – concerne l'urgenza di qualificare e descrivere la più recente delle grandi vulnerabilità delle nostre democrazie: la dimensione della sicurezza cibernetica, in tutte le sue consistenti sfaccettature. Appare davvero meritorio il tentativo di Serini di spiegare, e con ciò legare, i modelli di sicurezza cibernetica al rilievo normativo assunto dalle pratiche di standardizzazione delle norme tecniche, e dei connessi modelli di certificazione, che di fatto rappresentano le vere e uniche regole cogenti della società digitale.

Il contributo di Angela Cossiri ci introduce al rilievo delle c.d. campagne di disinformazione ed alla vulnerabilità dei tessuti democratici – si direbbe dovuta proprio al fatto di essere tali – di fronte a queste vecchie armi della propaganda, sviluppate con gli strumenti tipici della società digitale. Si descrivono il fondamento e la dinamica della Decisione Pesc 2022/351 del Consiglio, peraltro non così chiaramente

1. V. il sito del Convegno ICONS•S.
2. … sempre grazie alla cordialità degli organizzatori di ICON•S e alla vivacità intellettuale di colleghe e colleghi: v. il programma del Convegno.

approfonditi finché non vennero esposti da Angela Cossiri durante il panel bolognese, riguardante le modalità con cui l'Unione europea si è difesa – adottando azioni e prassi istituzionali anch'esse sostanzialmente inedite – di fronte all'attacco informativo subito in concomitanza all'avvio della guerra russo-ucraina e ai suoi sviluppi in sede giurisdizionale, ove con motivazione interessante il provvedimento europeo è stato ritenuto legittimo.

Nel contributo di Arturo Di Corinto si descrivono le dinamiche e l'articolazione della vera e propria guerra cibernetica, che si sviluppa nel campo di battaglia della Rete, fiancheggiando le attività degli eserciti sul campo, per sostenere gli obiettivi strategici della propria parte e fiaccare le resistenze degli avversari: è l'infowar con i suoi soldati, gli hacktivisti. Il campo di battaglia – e di indagine – purtroppo è lo scenario del conflitto russo-ucraino.

Lasciando da parte le guerre vere e proprie, il contributo di Irene Sigismondi si occupa invece di descrivere come si possano evitare – grazie alla Rete – le guerre giudiziarie nelle aule di tribunale, per trasferirle nell'ambiente digitale della rete Internet, in particolare attraverso l'utilizzo delle online dispute resolution (ODR), ovvero delle piattaforme di risoluzione alternativa delle controversie: non è affatto irrilevante, e ci mostra come la fine dell'utopia di Internet investa proprio gli aspetti che ne rappresentavano l'iniziale ed intrinseco contenuto originario, che uno degli aspetti che mette a rischio l'utilizzo e lo sviluppo delle ODR, sia proprio la progressiva frammentazione della rete Internet.

Gli ultimi due contributi aprono il quadro di indagine agli sviluppi normativi più recenti ed alle dinamiche di cui si avverte maggiormente l'esigenza per consentire uno sviluppo pieno e sovrano della dimensione europea della società digitale. Elia Cremona espone chiaramente la sua tesi, secondo cui il Data Governance Act e il Data Act costituiscono un mutamento di paradigma dell'indirizzo normativo europeo: l'enfasi non è più solo sul profilo della protezione e del controllo, ma anche della condivisione. La parola d'ordine è il data sharing e gli strumenti sono – principalmente – l'intermediazione, l'altruismo, l'accessibilità. Il fine è riconoscere che i dati sono beni comuni del nostro tempo: la loro condivisione, specie dal settore privato a quello pubblico, può rappresentare un'opportunità per lo sviluppo di politiche pubbliche data-driven e, per le imprese, di contribuire al raggiungimento degli obiettivi di sostenibilità fissati dalla normativa ESG (Environmental, Social, Governance).

Stefano Torregiani si pone il problema dell'impatto della datificazione sulla sovranità dell'Unione europea e osserva – obiettivamente, a ragione – che dei dati europei non hanno beneficiato principalmente i cittadini europei. Si chiede quindi se il recente Data Act – con l'obiettivo dichiarato di consentire accesso e riuso dei dati – possa riportare l'Unione in una dimensione di maggior padronanza e sfruttamento delle sue risorse digitali: è forse il Data Act una forma di Data Nationalism europeo? E in tal caso, può rivelarsi una strategia efficace?

4. La pluralità e i differenti punti di vista dei contributi raccolti rendono necessaria una ritrovata visione unitaria, ma non asfittica, della dimensione costituzionale della società digitale: concludendo e commentando i lavori di questa sezione monografica Erik Longo mostra che riconoscere il data-centrismo non implica aderire ad una ideologia – ottimista o pessimista – dei dati e della loro funzione. Implica invece riconoscere nel nuovo contesto tecnologico e nei mutamenti antropologici in atto l'esigenza di porre la tecnologia a servizio delle esigenze umane di giustizia (giustizia dei dati), di conoscibilità e spiegabilità (trasparenza algoritmica) e di controllo della tecnologia (controllo umano).

This research was funded by the European Union – NextGenerationEU under the Italian Ministry of University and Research (MIUR), National Innovation Ecosystem grant ECS00000041-VITALITY-CUP D83C22000710005