Rischio e costituzionalismo digitale

di Pietro Dunn[1] e Giovanni De Gregorio[2]

Abstract: Il contributo investiga il rapporto tra politiche digitali dell'Unione Europea e approccio regolativo basato sul rischio (*risk-based approach*). Si osserva come, sebbene il rischio sia diventato una costante della normativa europea in materia, tale approccio sia declinato secondo forme diverse. In particolare, se il GDPR si caratterizza quindi per una prospettiva più prettamente *bottom-up*, alcune recenti proposte (DSA, AI Act) segnalano un progressivo spostamento nella direzione di un sistema *top-down*. A fronte di tale apparente contraddizione, l'elemento comune di tali atti legislativi sembra essere l'obiettivo della costruzione di un sistema basato sulla proporzionalità: in tal senso, proporzionalità e bilanciamento degli interessi, quali espressione di un costituzionalismo digitale in divenire, sembrano essere la cifra capace di riportare a unità il rapporto tra rischio e regolazione.

1. Introduzione: l'approccio basato sul rischio

Il ventunesimo secolo ha visto un notevole incremento del ricorso al "*risk-based approach*" nella maggioranza dei sistemi giuridici occidentali[3], quale risposta all'emersione di quella che Beck definiva, già negli anni '80, una "società del rischio"[4]. Il modello dell'approccio basato sul rischio è stato ben presto adottato dalla stessa Unione Europea[5] con riferimento inizialmente al diritto dell'ambiente e alla tutela della salute umana, per poi approdare, in un secondo momento, alla regolazione delle tecnologie digitali. A partire dalla pubblicazione della Strategia per il mercato unico digitale in Europa[6], le istituzioni dell'Unione hanno infatti fatto sempre più ricorso allo strumento del rischio per incentivare una maggiore assunzione di responsabilità (*accountability*) da parte degli attori, pubblici e privati, per i potenziali effetti collaterali legati all'utilizzo di tali tecnologie e al processamento di dati personali.

L'approccio basato sul rischio si fonda essenzialmente sull'istituzione di un quadro normativo ove obblighi e doveri delle parti tutelate vengono graduati e adattati al concreto

[1] Dottorando di ricerca presso l'Alma Mater Studiorum – Università di Bologna e l'Università del Lussemburgo. E-mail: pietro.dunn2@unibo.it.
[2] Assegnista di ricerca presso il Centre for Socio-Legal Studies dell'Università di Oxford. E-mail: giovanni.degregorio@csls.ox.ac.uk
[3] J. Van der Heijden, *Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda*, in *Sage Open*, 11-3, 2021, 1 ss.; J. Black, *The Emergence of Risk-Based Regulation and the New Public Risk-Management in the United Kingdom*, in *Public Law*, 2005, 510 ss.
[4] U. Beck, *Risk Society. Towards a New Modernity* (tr. M. Ritter), Londra, 1986.
[5] Cfr. H.W. Micklitz – T. Tridimas (a cura di), *Risk and EU Law*, Cheltenham, 2015.
[6] COM(2015)192 final, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni*.

rischio connesso alle attività poste in essere: viene superata la logica binaria dell'adempimento per realizzare una forma di «*compliance* 2.0» ove gli obblighi sono cuciti direttamente addosso ai destinatari della regolazione[7]. La modalità più tipica del *risk-based approach*, caratterizzante per esempio il GDPR, prevede che la valutazione del rischio e l'individuazione delle misure di mitigazione adeguate siano condotte direttamente dai soggetti destinatari della regolazione. Tale metodologia, che definiamo "bottom-up", non è peraltro l'unica possibile, in quanto testi successivi hanno posto in essere modalità che potremmo definire "*top-down*". Il riferimento è, nello specifico, alla proposta di Regolamento per il *Digital Services Act* e, in misura maggiore, alla proposto di Regolamento per l'AI Act.

2. Diritto dell'UE e *risk-based approach* nella regolazione della società algoritmica

Il Regolamento (UE) 2016/679 (GDPR)[8], come è noto, è nel suo complesso informato dal principio di *accountability*[9]. Tale principio è declinato in pratica anche attraverso il ricorso a un sistema regolativo basato sul rischio, in base al quale titolare e responsabile del trattamento sono tenuti a predisporre le misure tecnico-organizzative necessarie ad assicurare che i principi del Regolamento siano rispettati. Laddove tali attori non siano in grado di provare la predisposizione di tali misure, saranno soggetti a responsabilità per i danni prodotti a carico dei soggetti interessati[10]. Di conseguenza, titolare e responsabile dovranno operare una valutazione di impatto delle loro attività e, sulla base di tale valutazione, elaborare la strategia migliore per ridurre i rischi di violazione dei diritti individuali.

Anche la più recente proposta di regolamento sul *Digital Services Act* (DSA) contiene un approccio alla moderazione dei contenuti online che si fonda sulla categoria del rischio: essa introdurrebbe una serie di obblighi a carico dei *service provider* volti a incentivare, da un lato, una riduzione di contenuti illeciti nell'ambiente digitale e, dall'altro lato, modalità più trasparenti e garantistiche delle attività di moderazione stessa. A differenza del GDPR, il DSA individua direttamente quattro livelli di rischio, sulla base dei quali vengono assegnati obblighi e doveri differenti[11]. Se nel GDPR vi è dunque una delegazione completa, secondo un modello *bottom-up*, dei doveri di valutazione e mitigazione, il DSA si discosta da tale sistema, individuando i criteri oggettivi di classificazione dei *provider*. Tuttavia, questo passaggio da una logica *bottom-up* a una logica *top-down* non è ancora completo: soprattutto nel caso delle piattaforme online di dimensioni molto grandi, infatti, un ampio margine di

[7] C. Quelle, *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach*, in *European Journal of Risk Regulation*, 9, 2018, 502 ss.
[8] R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020.
[9] Art. 5(2) GDPR.
[10] Si vedano in tal senso gli artt. 24 e 25 GDPR.
[11] I nuovi obblighi si applicano infatti a: tutti i fornitori di servizi di intermediazione; i soli fornitori di servizi di hosting; le sole piattaforme online; le sole piattaforme online di dimensioni molto grandi.

discrezionalità è comunque previsto per la mitigazione di rischi sistemici connessi alle loro attività[12].

Nell'AI Act, il passaggio da un modello *bottom-up* a un modello *top-down* è ancor più marcato[13]. Anche in questo caso la proposta di regolamento prevede quattro categorie di rischio per i sistemi di intelligenza artificiale: sistemi a rischio inaccettabile; sistemi ad alto rischio; sistemi a rischio limitato; sistemi a rischio minimo. I sistemi del primo gruppo sono in linea generale vietati[14], mentre quelli del secondo gruppo sono sottoposti a una lunga lista di requisiti di qualità e trasparenza, nonché a un regime di controllo da parte di fornitori e utenti[15]. Infine, i sistemi a rischio limitato (per esempio *chatbot*) sono soggetti a semplici requisiti di trasparenza[16], mentre per tutti i restanti sistemi di IA non è previsto alcun obbligo[17]. Nel caso dell'AI Act, dunque, l'individuazione delle categorie di rischio e la predisposizione di meccanismi di mitigazione del rischio sono attività che non sono più affidate alla discrezione dei destinatari del regolamento. Al contrario, l'ascrizione all'uno o all'altro livello avviene sulla base di un automatismo imposto dall'alto (*top-down*), così come è regolata dall'alto la disciplina dei livelli stessi. In effetti, sebbene la Commissione sostenga, nell'*explanatory memorandum* della proposta, di aver incentrato il testo dell'AI Act «su un approccio normativo ben definito basato sul rischio che non crea restrizioni inutili al commercio», vi è chi, in letteratura, ha posto in dubbio la sussistenza effettiva di un vero e proprio *risk-based approach*[18].

La prospettiva adottata dall'AI Act sembra quindi essere per certi versi opposta a quella del GDPR. Se nel GDPR la valutazione del rischio e la predisposizione di misure atte a tutelare i diritti individuali alla riservatezza e protezione dei dati erano attività delegate direttamente al titolare e al responsabile del trattamento dati, nel caso dell'AI Act la prospettiva è rovesciata: è il regolamento stesso a operare tale attività. In effetti, se è vero che è presente, con riferimento ai sistemi di IA ad alto rischio, la previsione dell'obbligo di istituire, attuare, documentare e mantenere un sistema di gestione dei rischi[19], è altresì vero che nell'ecosistema del Regolamento tale norma sembra avere un carattere per lo più residuale.

3. Il rischio quale cifra del costituzionalismo digitale europeo?

[12] Artt. 26-27.
[13] Cfr. O. Pollicino – G. De Gregorio – F. Bavetta – F. Paolucci, *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, in *agendadigitale.eu*, 21 maggio 2021.
[14] Art. 5.
[15] Artt. 8 ss.
[16] Art. 52.
[17] Resta salva la possibilità di incentivare l'adozione di codici su base volontaria (art. 69).
[18] L. Edwards, *Regulating AI in Europe: four problems and four solutions*, in *adalovelaceinstitute.org*, 31 marzo 2022.
[19] Art. 9.

A fronte di tali rilievi appare quanto meno essenziale interrogarsi in merito alla linearità dell'approccio normativo adottato dalla Commissione con riferimento al *risk-based approach* nella regolazione delle tecnologie informatico-digitali. Invero, l'adozione da parte dell'AI Act di un modello *top-down*, apparentemente agli antipodi rispetto al modello proposto pochi anni fa attraverso il GDPR, pone non pochi dubbi a livello di coerenza sistematica.

Nonostante ciò, sembra tuttavia potersi individuare quanto meno un elemento caratterizzante sia il GDPR, sia il DSA, sia l'AI Act. Tutti e tre gli atti normativi mirano infatti a realizzare, attraverso il concetto di "rischio", un bilanciamento tra gli interessi in gioco: da un lato, l'interesse, di matrice economica, all'innovazione e allo sviluppo di un mercato unico digitale competitivo sul piano internazionale; dall'altro lato, l'interesse, sovente opposto, alla tutela dei valori democratici e dei diritti e delle libertà fondamentali degli individui[20]. Il rischio funge, in altre, parole, da *proxy* per un'attività, quella del bilanciamento, strettamente connessa a una dimensione costituzionale[21].

L'apparente incoerenza dei tre atti normativi, pertanto, può essere ricondotta a unità attraverso l'adozione di una prospettiva costituzionalmente orientata al rischio, che veda nello stesso non solo un semplice modello normativo quanto, piuttosto, uno strumento atto a garantire un sistema giuridico bilanciato e a tutelare in egual misura tutti gli interessi in gioco. In altre parole, sebbene le modalità siano diverse, e diversa sia la declinazione del *risk-based approach*, il fine pare essere in ultima analisi univoco: la tutela dei valori fondanti del costituzionalismo digitale europeo[22].

[20] Sul crescente ruolo ricoperto dai diritti fondamentali e dai valori democratici all'interno della strategia normativa europea in ambito di tecnologie digitali, si veda in particolare G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 19-1, 2021, 41 ss.

[21] Cfr. A. Stone Sweet – J. Mathews, Proportionality Balancing and Global Constitutionalism, in Columbia Journal of Transnational Law, 47, 2008, 72 ss.

[22] Sul tema si veda, più ampiamente, G. De Gregorio – P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 59-2, 2022.