LA CO-REGOLAZIONE DELLE NUOVE TECNOLOGIE, TRA RISCHI E TUTELA DEI DIRITTI FONDAMENTALI*

GIUSEPPE MOBILIO**

Sommario

Abstract

The issue at the basis of this paper is whether, and how, the protection of fundamental rights conditions legal regulation, and in particular the openness or otherwise of private involvement in regulation. The aim is to investigate whether, and in what terms, recourse to co-regulation depends on the impact of the technologies to be regulated on the fundamental rights at stake.

Suggerimento di citazione

G. MOBILIO, *La co-regolazione delle nuove tecnologie, tra rischi e tutela dei diritti fondamentali,* in *Osservatorio sulle fonti,* n. 1/2024. Disponibile in: http://www.osservatoriosullefonti.it

* Il presente contributo costituisce la rielaborazione della relazione preparata per il Convegno finale del Progetto PRIN 2017 S*elf- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law* (SE.CO.R.E TECH) tenutosi a Firenze l'8 e 9 febbraio 2024 e organizzato dal Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze.

** Ricercatore t.d. b) di Diritto costituzionale nell'Università degli Studi di Firenze.
Contatto: giuseppe.mobilio@unifi.it

Registrazione presso il Tribunale di Firenze n. 5626 del 24 dicembre 2007
Rivista inclusa nella classe A delle Riviste scientifiche di Area 12 – Direttore Prof. Paolo Caretti
ISSN 2038-5633

1. Introduzione

È un dato comunemente acquisito che dalle fonti del diritto dipenda la garanzia e la definizione dei limiti dei diritti fondamentali, la partecipazione democratica e il buon funzionamento delle istituzioni[1]. Oggi occorre quindi interrogarsi su quali siano le fonti e le tecniche di regolazione che si rivolgono alle nuove tecnologie, perché è proprio dagli strumenti tecnologici che dipende non solo l'esercizio di molte libertà, ma anche la minaccia alle stesse[2].

Per affrontare efficacemente il problema della disciplina del fenomeno tecnologico, tuttavia, lo sguardo deve assumere una portata più ampia e non limitarsi solamente al diritto, rivolgendosi invece alla "regolazione". Per comprendere l'impatto sulle libertà, non è possibile limitare l'attenzione alle tradizionali fonti normative, poiché, come efficacemente chiarito da Lawrence Lessig, il diritto costituisce solo una delle modalità per regolare lo spazio reale o il cyberspazio, in concorrenza con le norme sociali, il mercato, l'architettura o il codice[3]. Più in generale, la regolazione può assumere accezioni più o meno ristrette[4], a seconda che venga intesa solamente come l'attività volta a influenzare direttamente il comportamento di qualcuno[5], oppure consideri esplicitamente anche lo scopo o i risultati che ambisce ad ottenere[6], potendosi allargare anche alla platea variegata dei soggetti regolati, al soggetto responsabile della "direzione" da impartire con la regolazione, ai diversi soggetti coinvolti nei processi di regolazione (anche non pubblici)[7].

La scelta su come regolare le nuove tecnologie diviene quindi essenziale. E siccome non esiste una soluzione "one-size-fits-all"[8], le autorità pubbliche

[1] Come è altrettanto pacifico che in assenza di tale sistema «si riafferma pericolosamente il mero potere dei diversi soggetti politici, sociali od economici comunque dominanti»; cfr. U. DE SIERVO, *Perché occuparsi ancora delle fonti del diritto?*, in *Osservatorio sulle fonti*, 1, 2015, 3. Osserva A. SIMONCINI, *1998-2008: la fine della legge?*, in *Osservatorio sulle fonti*, 2, 2009, come anche dai principi costituzionali di natura organizzativa dipendano tali aspetti.

[2] Cfr. L. ALEXANDRE, *La guerra delle intelligenze. Intelligenza artificiale contro intelligenza umana*, EDT, Torino, 2018.

[3] Cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 113, 1999, 501 ss.

[4] R. BROWNSWORD, *Law, Technology and Society. Re-Imagining the Regulatory Environment*, Routledge, New York, 2019, 44 s.

[5] B.-J. KOOPS, *Ten dimensions of technology regulation. FINDING your bearings in the research space of an emerging discipline*, in M.E.A. GOODWIN, B.-J. KOOPS, R.E. LEENES (a cura di), *Dimensions of technology regulation*, Nijmegen, Wolf Legal Publishers, 2010, 309 ss.

[6] Cfr. J. BLACK, *Critical Reflections on Regulation*, in *Australian Journal of Law and Philosophy*, 1, 27, 2002, 26, che sottolinea come i risultati possono rigaurdare «mechanisms of standard-setting, information-gathering and behaviour-modification».

[7] K. YEUNG, *Algorithmic Regulation: A Critical Interrogation*, in *Regulation & Governance*, 12, 2018, 507.

[8] R. BROWNSWORD, *Law, Technology and Society*, cit., 43.

sono chiamate a reinventare come regolare al meglio le tecnologie, assumendo a monte scelte di politica regolatoria che considerino i diversi strumenti regolatori a disposizione e molteplici variabili in gioco. Basti pensare alla scelta circa l'oggetto di disciplina, ovvero se la regolazione debba rivolgersi direttamente alle tecnologie oppure ai possibili usi che di esse viene fatto[9], se debba riguardare le tecnologie in generale o le loro applicazioni settoriali[10], se debba essere prodotta a livello nazionale o internazionale[11]. Gli studi "socio-tecnologici" – che guardano alle dinamiche tra gli agenti umani, le tecnologie e le norme organizzative – pongono sempre più l'accento sulla iterazione tra persone e tecnologie, ovvero sul modo con cui tecnologie e contesti sociali sono "co-prodotti", influenzandosi reciprocamente[12]. Tra le variabili della regolazione da considerare, dunque, vi è anche il tipo di coinvolgimento dei privati che costituiscono i destinatari della disciplina giuridica, aprendo al fenomeno che – come si vedrà – prende il nome di "co-regolazione".

L'interrogativo alla base della presente riflessione è se, e come, la tutela dei diritti fondamentali condizioni la regolazione giuridica, e in particolare l'apertura o meno al coinvolgimento dei privati nell'attività regolatoria. Detto diversamente, si vuole indagare se, e in quali termini, il ricorso alla co-regolazione dipenda dall'impatto che le tecnologie da regolare producono sui diritti fondamentali in gioco. Per cercare di offrire qualche spunto a questo scopo, l'analisi offrirà alcuni chiarimenti su cosa si intenda per "co-regolazione", richiamando punti di forza e limiti di una tecnica che, in ambito di disciplina delle tecnologie, è sempre più diffusa, oltre che di "nuove tecnologie" (par. 2). Successivamente ci si addentrerà nell'analisi di una delle più recenti impostazioni con cui la legislazione dell'UE intende disciplinare le tecnologie, ovvero la "regolazione del rischio", per sottolineare come in larga parte essa faccia uso di tecniche di co-regolazione e come vi siano alcuni principi che valgono ad indirizzare questo tipo di regolazione verso la tutela dei diritti fondamentali (par. 3). Volendo quindi ammettere questa funzionalizzazione della co-regolazione verso la tutela dei diritti fondamentali, occorrerà interrogarsi su quale sia il ruolo del decisore pubblico e come vengano condizionati i margini a disposizione dei privati (par. 4). In conclusione (par. 5), si indicheranno alcuni limiti dell'impostazione emergente

[9] L. BENNETT MOSES, *Regulating in the Face of Sociotechnical Change*, in R. BROWNSWORD, E. SCOTFORD, K. YEUNG (a cura di), *The Oxford Handbook of Law, Regulation, and Technology*, OUP, Oxford, 2017, 584.

[10] J.D. LOHR, W.J. MAXWELL, P. WATTS, *Legal Practitioners' Approach to Regulating AI Risks*, in K. YEUNG, M. LODGE (a cura di), *Algorithmic Regulation*, OUP, Oxford, 2019, 242 ss.

[11] Ivi, 245.

[12] K. YEUNG, M. LODGE, *Algorithmic Regulation: An Introduction*, in K. YEUNG, M. LODGE (a cura di), *Algorithmic Regulation*, cit., 7 s.

dall'analisi, i quali comunque non impediscono di individuare un *trend* verso cui le politiche regolative delle nuove tecnologie si stanno muovendo.

2. Cosa significa "co-regolare" le "nuove tecnologie"

La tecnica regolatoria che verrà presa qui in considerazione è la "co-regolazione". Quest'ultima si pone a metà strada tra il paradigma tradizionale della "hard law", o "hard-regulation", e la "self regulation". La *hard-regulation* può essere intesa come regolamentazione ispirata allo schema delle imposizioni assistite da sanzioni ("command and control"), che segue una traiettoria di eteronomia ("top-down"), in cui il destinatario delle norme si vede calata dall'alto una disciplina che potrebbe anche risultare estranea e inadatta alle esigenze sue o del settore[13]. Pretendere di applicare alle tecnologie questa impostazione espone al rischio di una *disruption* della regolamentazione giuridica, che può divenire non solo ineffettiva, ma anche superata e sostituita da altri metodi di regolazione, quali il mercato o la tecnica, con conseguenti problemi in termini di legittimazione democratica, responsabilità (politica e giuridica), capacità di tutela[14].

All'opposto, la *self-regulation* consiste in una regolazione adottata dal soggetto destinatario della stessa, la quale può variare a seconda di elementi come l'adozione delle regole su base volontaria, il loro grado di cogenza, il loro contenuto tecnico, il coinvolgimento delle istituzioni pubbliche nella loro formazione, il ruolo dei destinatari[15]. Si tratta di un approccio *bottom-up*, espressione di una diversa concezione nei rapporti tra soggetto regolatore e soggetti regolati.

Ai fini della presente indagine, non è possibile operare una distinzione netta tra queste due versioni di regolazione *top-down* e *bottom-up*, poiché bisogna considerare soprattutto il ruolo giocato dalle autorità pubbliche, le quali ad esempio possono definire una cornice normativa riempita dai privati, oppure approvare le norme autoprodotte, o imporne di fatto l'elaborazione[16]. In generale, mediante la co-regolazione si assegna alla decisione di matrice pubblica il compito di fissare i valori e gli obiettivi generali, coinvolgendo invece nella fase di esecuzione-attuazione i destinatari delle

[13] R. BROWNSWORD, Law, Technology and Society, cit., 37 ss.

[14] G. MOBILIO, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal*, 2, 2020, 401 ss.

[15] J. BLACK, *Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a 'Post-regulatory' World*, in *Current Legal Problems*, 54, 1, 2001, 121, che sottolinea come si varia tra le più varie tipologie di regole, linee guida o standard, adottate dalle singole imprese, da più imprese in accordo, dalle loro forme associative o da partnership pubblico-private.

[16] Così nella sistinzione in EAD., *Constitutionalising Self-Regulation*, in *Modern Law Review*, 59, 1, 1996, 27 s., che parla di "mandated", "sanctioned", "coerced" e "voluntary" self-regulation.

norme[17]. La co-regolazione può quindi variare dalla responsabilizzazione dei privati nell'implementazione delle norme formulando scelte organizzative che esprimono una valenza normativa, ovvero facilitano o meno il raggiungimento di certi obiettivi[18], fino ad espressioni che più si avvicinano alla produzione di fonti del diritto. Quest'ultimo è il caso, ad esempio, dei codici di condotta contenenti regole sostanzialmente generali e astratte, i quali attualmente non rispondono ad un modello unitario[19], ma sono comunque impiegati – come si vedrà – da numerose normative in ambito tecnologico.

La co-regolazione è uno strumento chiave della *Better Regulation Strategy* dell'UE[20], che attualmente, nel suo *Better Regulation Toolbox*[21], richiama la "co-regulation" come uno dei *policy instruments* a disposizione in alternativa alle "hard, legally binding rules" e rientranti nella "soft regulation", assieme alla "self-regulation", i "technical standards"[22], le "raccomandazioni" delle istituzioni europee e gli "open method of coordination"[23].

Le cause che giustificano un sempre più ampio ricorso all'opzione della co-regolazione sono profonde e guardano a fenomeni di cambiamento della società e della funzione di governo, a partire dalla frammentazione della conoscenza e delle informazioni, intesa non solo come asimmetria informativa tra regolatori e regolati, ma anche come l'impossibilità che un solo soggetto possieda tutte le informazioni necessarie a risolvere problemi complessi come quelli legati alle tecnologie[24].

La co-regolazione porta con sé diversi vantaggi, fra cui la possibilità di coniugare la flessibilità della *self-regulation* con la supervisione dell'autorità

[17] A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 2022, 1032.

[18] Sul modello della "management-based regulation", su cui v. C. COGLIANESE, J. NASH, *Management-Based Strategies for Improving Private Sector Environmental Performance*, in *Faculty Scholarship*. Paper 105, 2005, 5 ss.

[19] C.V. MAELEN, *Hardly law or hard law? Investigating the dimensions of functionality and legalisation of codes of conduct in recent EU legislation and the normative repercussions thereof*, in *European Law Review*, 47, 6, 2022, 57.

[20] Cfr. più ampiamente S. GARBEN, I. GOVAERE, *The EU Better Regulation Agenda: A critical assessment*, Hart Publishing, 2 Oxford, 018.

[21] Cfr. TOOL #17. Più ampiamente sul tema, H. XANTHAKI, *European Union Legislative Quality After the Lisbon Treaty: The Challenges of Smart Regulation*, in *Statute Law Review*, 1, 2013, 66 ss.; S. TOMBS, *Making better regulation, making regulation better?*, in *Policy Studies*, 4, 2016, 332 ss.

[22] Su cui v. *infra*.

[23] Quale metodo intergovernativo in cui, sotto la supervisione della Commissione, gli Stati cooperano e si valutano reciprocamente in una logica orizzontale per raggiungere obiettivi comuni.

[24] Cfr. J. BLACK, *Decentring Regulation*, cit.., 105 ss., che parla anche di complessità delle interazioni tra attori sociali; frammentazione dell'esercizio del potere e controllo, condivisa da attori sociali e da essi e lo Stato; crescente autonomia degli attori sociali, sempre più capaci di impiegare potere e risorse per le loro azioni e perciò sempre più refrattari ad un intervento regolatorio esterno; il venir meno della distinzione tra pubblico e privato in termini socio-politici.

pubblica; di indirizzare i privati (comprese le imprese) verso interessi pubblici e protezione dei diritti; di porre regole condivise e più sostenibili dal punto di vista dei costi; di indurre un maggior senso di responsabilità verso regole concordate, con costi reputazionali in caso di mancato rispetto[25]. Di contro, la co-regolazione può rivelarsi un fallimento se incapace di indirizzare i privati verso obiettivi di interesse generale, o se i privati decidono di non rivelare le informazioni a disposizione per produrre la regolazione, oppure può dare origine a forme di negoziazione opache che si risolvono a vantaggio delle parti private, secondo il fenomeno di "cattura del regolatore"[26].

La stessa Unione Europea ha dimostrato di aver ben presenti i pericoli sottesi alla "remissività" verso la regolamentazione privata, tant'è che nell'accordo interistituzionale del 2003 sul «Legiferare meglio», pur incentivando queste forme di regolazione, ne ha scoraggiato l'applicazione laddove siano «in gioco i diritti fondamentali o scelte politiche importanti»[27].

La co-regolazione, come anticipato, ha ad oggetto le "nuove tecnologie", ovvero tecnologie innovative che aprono a nuove potenziali conseguenze irreversibili (in termini di danni fisici e non solo). Di conseguenza, si avverte la necessità di una regolazione per prevenire il compimento di determinate pratiche tecnologiche o la creazione e il possesso di particolari prodotti tecnologici[28]. Esempio paradigmatico di questo tipo di tecnologie sono i sistemi di intelligenza artificiale (IA), oramai diffusi in ogni ambito e attività delle nostre società, dai quali dipendiamo e difficilmente potremmo emanciparci[29].

Volendoci collocare nel solco del costituzionalismo liberal-democratico[30], la co-regolazione si dimostra compatibile con gli ordinamenti giuridici contemporanei solo se rispetta la condizione di incrementare e non indebolire la tutela dei diritti fondamentali. Diversamente, occorrerebbe ritornare alla "classica" ipotesi della regolazione panpubblicistica, ammesso che questa sia una soluzione percorribile e non esponga invece a maggiori rischi per i diritti a causa della sua inefficacia od obsolescenza. Per stabilire se questa condi-

[25] D. HIRSCH, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, in *Seattle University Law Review*, 34, 2011, 466 ss.

[26] Ivi, 468 ss.

[27] Progetto interistituzionale "Legiferare meglio" (2003/C 321/01), p. 17. Osserva N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Osservatorio sulle fonti*, 3, 2022, 70, come analoga statuizione non è stata replicata nel successivo accordo interistituzionale del 2015.

[28] L. BENNETT MOSES, *Regulating in the Face of Sociotechnical Change*, cit., 576 ss.

[29] Sul punto J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Faculty Scholarship Series*, 2017, 1219, fa riferimento alla "Algorithmic Society", ovvero «a society organized around social and economic decision-making by algorithms, robots, and Al agents, who not only make the decisions but also, in some cases, carry them out».

[30] A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T.E. FROSINI, O. POLLICINO, E. APA, M. BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier, Firenze, 2017, 26 ss.

zione viene rispettata può essere utile verificare come si comporti la normativa che più di recente è stata adottata per impostare la regolazione delle nuove tecnologie e, in particolare, regolare, direttamente o indirettamente, i sistemi di IA.

3. Nuovi approcci regolatori per nuove tecnologie: la "risk-based regulation" a tutela dei diritti e l'emergere dei principi di precauzione e proporzionalità

Gli studi sociologici hanno messo in luce da tempo come lo sviluppo di nuove tecnologie, che producono conseguenze difficilmente prevedibili a lungo termine, sia uno dei fattori principali che hanno contribuito a strutturare la "società del rischio"[31]. Il rischio, nelle società altamente tecnologizzate, è una componente che non è pensabile possa essere neutralizzata, ma che può essere conosciuta e al limite minimizzata o distribuita nei suoi effetti collaterali[32]. Da qui il diffondersi di un nuovo paradigma di "regolazione del rischio", intesa come categoria eterogenea che racchiude il tentativo delle autorità pubbliche di interferire con i processi sociali e di mercato per controllare conseguenze potenzialmente avverse contro i diritti[33]. Le nuove tecnologie, tuttavia, non sono solamente uno strumento attraverso cui "governare" il rischio, ma sono esse stesse fonte di conseguenze impreviste da cui bisogna tutelarsi[34]. Questo fattore contribuisce a spiegare perché la regolazione del rischio – come si vedrà – si sia oramai affermata come la nuova frontiera per la regolazione delle tecnologie, quantomeno in ambito europeo.

Ai fini della presente analisi, con regolazione del rischio non si intende una regolazione in cui il rischio è direttamente l'oggetto della regolazione, quanto piuttosto una regolazione "basata sul rischio" (RBR), in cui cioè il rischio è un fattore impiegato per calibrare l'attuazione della normativa a partire dai rischi che concretamente assumono rilevanza[35]. Il rischio, quindi, acquisisce una valenza metodologica per impostare la regolazione, stabilire

[31] Cfr. U. BECK, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2013. ma si vedano anche le riflessioni in N. LUHMANN, *Sociologia del rischio*, Mondadori, Milano, 1996, spec. 98 ss., a proposito di come il "rischio" sia inevitabilmente insito nella "tecnica". Sulle diverse definizioni di rischio, v. P. TAYLOR-GOOBY, J.O. ZINN, *The Current Significance of Risk*, in P. TAYLOR-GOOBY, J.O. ZINN (a cura di), *Risk in social science*, Oxford, 2006, 3 ss.

[32] U. BECK, *La società del rischio*, cit., pp. 25. Vi anche Z. BAUMAN, *La società dell'incertezza*, Il Mulino, Bologna, 1999.

[33] C. HOOD, H. ROTHSTEIN, R. BALDWIN, *The government of risk: Understanding risk regulation regimes*, Oxford, 2001, 3 ss.

[34] E. LONGO, *La disciplina del "rischio digitale"*, in F. PIZZETTI (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, 58

[35] G. DE GREGORIO, P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2, 2022, 475.

regimi giuridici diversificati, disciplinare le condizioni di sviluppo e uso di una certa tecnologia, graduare gli oneri e imporre soluzioni organizzative a carico dei soggetti coinvolti[36].

RBR e co-regolazione risultano non solo strettamente legate. Dall'analisi della normativa più recente risulta infatti che vi siano due principi richiamati dalla RBR che valgono a calibrare il ricorso alla co-regolazione, ovvero il coinvolgimento dei privati, e si tratta di principi finalizzati proprio alla tutela dei diritti. In particolare, si ha riguardo al principio di precauzione e al principio di proporzionalità.

Il principio di precauzione – come noto – si impone nei documenti internazionali per offrire risposta al problema della valutazione e gestione dei rischi per i diritti, a partire dalla salute, o per l'ambiente, quando la scienza non è in grado di fornire delle certezze riguardo ai pericoli, agli oneri e agli effetti collaterali connessi ad una determinata attività[37]. Il principio precauzionale interviene dunque nelle situazioni di incertezza scientifica e viene intimamente connesso al concetto di "rischio", con il quale condividono la stessa matrice "prudenziale" poiché tesi ad anticipare la soglia di rilevanza di fenomeni lesivi, traducendosi nell'esigenza di rappresentare anticipatamente, e quindi di scongiurare preventivamente, eventi potenzialmente dannosi[38].

Nel caso delle tecnologie siamo di fronte ai rischi, attualmente non valutabili con certezza, che dalla loro diffusione possa derivare un danno per l'essere umano e le società, che lo sviluppo possa avvenire in maniera incontrollata, ma soprattutto che sistemi efficaci di regolamentazione non siano

[36] Incrociando così alcune dei ruoli giocati dal rischio nella regolazione esplicitate da J. BLACK, *The role of risk in regulatory processes*, in R. BALDWIN, M. CAVE, M. LODGE (a cura di), *The Oxford Handbook of Regulation*, Oxford, 2010, 302 ss., che parla di rischio come oggetto, come giustificazione, come ruolo organizzativo e procedurale, come ruolo di valutazione e responsabilità.

[37] Cfr. A. ZEI, *Principio di precauzione*, in *Dig. disc. pubbl.*, Agg. III, II, 2008, 670. Più di recente, v. R. TITOMANLIO, *Il principio di precauzione fra ordinamento europeo e ordinamento italiano*, Giappichelli, Torino, 2018. Uno dei principali documenti istituzionali che offrono una cornice organica a questo principio è la comunicazione europea sul principio di precauzione, risalente al 2000 (COMMISSIONE DELLE CE, Comunicazione della Commissione sul principio di precauzione, COM(2000) 1 final, 2 febbraio 2000). Oggi tale principio è presente all'art. 191 TFUE. Sulle declinazioni di tale principio in materia ambientale, v. S. GRASSI, *Prime osservazioni sul "principio di precauzione" come norma di diritto positivo*, in *Dir. gest. amb.*, 1, 2001, 45 s.

[38] M.C. TALLACCHINI, *Ambiente e diritto della scienza incerta*, in S. GRASSI, M. CECCHETTI, A. ANDRONIO, *Ambiente e diritto*, I, Olschi, Firenze, 1999, 81. La regolazione sarà dunque chiamata a compiere scelte in cui entrano in gioco valutazioni di natura politica, tecnico-scientifica ed economica, come osservato in L. BUFFONI, A. CARDONE, *Il procedimento normativo precauzionale come caso paradigmatico del ravvicinamento "formale-procedurale" delle "fonti" del diritto*, in *Osservatorio sulle fonti*, 3, 2012, 2.

stati ancora elaborati contro queste evenienze[39]. A fronte di questi timori, il principio di precauzione può essere declinato in una duplice accezione, ovvero "forte" o "debole"[40]: nei suoi significati "forti", il principio in questione opera come "regola per decidere", postulando un obbligo di cautela, di adozione di misure preventive, al limite di astensione dalle attività di cui siano ignoti i potenziali effetti negativi; nei suoi significati "deboli", invece, il principio di precauzione opererebbe come "regola per procedere", che impone un obbligo di presa in considerazione dell'incertezza scientifica, nell'ambito di una analisi costi/benefici in cui pesano anche i costi dei margini di errore non prevedibili[41].

Il principio di proporzionalità, invece, offre il criterio per trovare il giusto bilanciamento tra gli obiettivi perseguibili, con una certa disciplina legislativa o l'uso di una tecnologia, e il conseguente sacrificio dei diritti. Si tratta di un principio sviluppato dalla giurisprudenza[42], che oggi costituisce una condizione per valutare la legittimità delle misure limitative dei diritti fondamentali ai sensi dell'art. 52, par. 1 CDFUE.

Per svolgere questo tipo di giudizio, giurisprudenza e dottrina hanno elaborato un test di proporzionalità articolato al suo interno in tre sottotest[43], che guardano: alla "idoneità" del mezzo impiegato a perseguire gli obiettivi; alla "necessità" di tale mezzo, intesa come "essenzialità" della misura per raggiungere gli obiettivi perseguiti e come esigenza che sia la "meno invasiva" per i diritti implicati; alla "proporzionalità in senso stretto", che implica una più ampia comparazione tra costi, intesi come intensità dell'interferenza con i diritti, e benefici, intesi come importanza degli obiettivi.

Come si vedrà, nell'ambito della RBR, entrambi questi principi entrano in gioco sia nella scelta dello strumento regolatorio, in particolare tra *co-regulation* e *hard-regulation*, sia nella valutazione e mitigazione concreta dei rischi emergenti da una certa tecnologia, l'uso che se ne può fare e i soggetti che possono impiegarla.

[39] Cfr. S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, 403; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 86 s.

[40] M. AHTEENSUU, P. SANDIN, *The Precautionary Principle*, in S. ROESER, R. HILLERBRAND, P. SANDIN, M. PETERSON (a cura di), *Handbook of Risk Theory*, Springer, 2012, 970.

[41] Cfr. P. ZUDDAS, *Pregiudizi digitali e principio di precauzione*, in *Consulta online*, 2, 2020, 420.

[42] T. TRIDIMAS, *The Principle of Proportionality*, in R. SCHU□TZE, T. TRIDIMAS (a cura di), *Oxford Principles of European Union Law*, Oxford University Press, Oxford, 2018, 243.

[43] In dottrina, v. G. DE BÚRCA, *The Principle of Proportionality and Its Application in EC Law*, in *Yearbook of European Law 1993*, 13, 1993, 113; A. BARAK, *Proportionality: Constitutional Rights and Their Limitations*, Cambridge University Press, Cambridge, 2012, 243 ss. Sulla giurisprudenza della CGUE, v., da ultimo, L. DALLA CORTE, *On proportionality in the data protection jurisprudence of the CJEU*, in *International Data Privacy Law*, 12, 4, 2022, 259 ss.

La pregnanza dei principi di precauzione e proporzionalità e dei due profili appena citati verrà misurata concentrando l'attenzione su tre atti normativi complessi elaborati a livello di Unione Europea e chiamati a regolare le nuove tecnologie. Ciascuno di questi atti adotta un approccio basato sul rischio, ma con una significativa diversità sia di impostazioni e finalità di partenza, sia di soluzioni concretamente previste. Si tratta del Regolamento (UE) 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (c.d. General Data Protection Regulation – GDPR), il Regolamento (UE) 2022/2065 "relativo a un mercato unico dei servizi digitali" (Digital Services Act – DSA) e il regolamento "che stabilisce regole armonizzate sull'intelligenza artificiale" (c.d. AI Act), attualmente nella fase conclusiva del procedimento di adozione[44].

3.1 La disciplina in vigore a tutela dei dati personali processati dalle nuove tecnologie: il GDPR

La prima disciplina rilevante per le nuove tecnologie che si basano su IA, e già in vigore da tempo, è quella sui dati personali, ovvero il GDPR. È una disciplina che si rivolge alle nuove tecnologie solo indirettamente, ma che costituisce un riferimento imprescindibile nella misura in cui sono i dati personali ad essere trattati dai sistemi di IA o nell'ambito delle *big data analytics*.

Il nuovo regolamento mira a porre rimedio ai limiti manifestati dalla direttiva 95/46/CE e alla frammentazione della protezione dei dati all'interno dell'UE che ne è scaturita[45]. Anche il nuovo regolamento tenta inoltre di coniugare le ragioni della tutela dei diritti fondamentali con quelle, di indole economica, dirette a favorire la circolazione dei dati e la costruzione del mercato unico[46].

Tra le più significative novità del GDPR è quella di adottare un approccio diretto ad anticipare la protezione ad un momento precedente al trattamento per prevenire così le potenziali lesioni, con una approccio marcata-

[44] Nel testo si farà riferimento alla versione finale approvata dal Parlamento europeo in 13 marzo 2024 e in attesa dell'approvazione finale del Consiglio: il testo è disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html#title2

[45] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22, 2018, 3.

[46] S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. Disc. Pubbl.*, Agg., 2017, 618 ss.; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, 87.

mente basato sul rischio[47]. Il GDPR, in particolare, rimette al titolare del trattamento il compito di valutare e decidere come affrontare i rischi per i diritti[48], guidato dai citati principi di precauzione (nel suo significato "debole"), specie per quanto riguarda tecnologie ad esempio ancora non applicate su vasta scala, e di proporzionalità.

A livello normativo, questa impostazione si sostanzia innanzitutto in una valorizzazione del principio di "responsabilizzazione" (*accountability*), da cui scaturisce l'obbligo per il titolare del trattamento tanto di conformarsi alla normativa a protezione dei dati tramite procedure e misure tecniche e organizzative, quanto di dover essere in grado di dimostrare tale conformità[49]. Questo compito è modulato su una serie di parametri che rendono più dinamica e concreta la protezione dei dati, che va calibrata a seconda «della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche»[50]. Il criterio con cui il titolare del trattamento deve compiere le proprie valutazioni è proprio il principio di proporzionalità[51], dal momento che il rigore di queste misure varia in proporzione alla gravità dei rischi, ovvero la probabilità che i diritti e queste regole possano essere violati[52].

A fianco del principio di *accountability* si aggiungono i principi di *privacy by design* e *by default*[53], o il principio di sicurezza del trattamento[54], che si

[47] G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver–Cedam, Milano, 2016, 55 ss.; A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Zanichelli, Bologna, 2019, 473 ss.; 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, 3, 2018, 502 ss.; R. GELLERT, *The risk-based approach to data protection*, Oxford, 2020.

[48] G. DE GREGORIO, P. DUNN, *The European risk-based approaches*, cit., 478 ss., parlano di un approccio bottom-up.

[49] Art. 5, par. 2, e art. 24 GDPR. V. anche GRUPPO DI LAVORO ARTICOLO 29, *Parere 3/2010 sul principio di responsabilità*, WP 173, 13 luglio 2010.

[50] Art. 24 GDPR. Più ampiamente, cfr. K. DEMETZOU, *GDPR and the concept of risk: The role of risk, the scope of risk and the technology involved*, in E. KOSTA e al. (a cura di), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Cham, 2019, 137 ss.

[51] A. GUINCHARD, *Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law*, in *European Law Journal*, 24, 6, 2018, 434 ss.

[52] K. YEUNG, L.A. BYGRAVE, *Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship*, in *Regulation & Governance*, 16, 2022, 146.

[53] In base all'art 25, par. 1 del GDPR, occorre «mette[re] in atto misure tecniche e organizzative adeguate [...] volte ad attuare in modo efficace i principi di protezione dei dati [...] e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti [normativi] e tutelare i diritti

basano su valutazioni ispirate a canoni analoghi. Merita specifica menzione, inoltre, lo strumento della "valutazione d'impatto sulla protezione dei dati"[55], volta ad identificare, valutare e gestire i "rischi elevati" per i diritti e le libertà prima che vanga effettuato il trattamento dei dati[56]. Tale analisi, fra l'altro, deve comprendere espressamente «una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità»[57].

Alla luce di queste previsioni, che implicano un diretto coinvolgimento dei destinatari della regolazione, si potrebbe sostenere che il GDPR sposi un approccio basato sul rischio associabile alla categoria della "meta risk-management"[58], quale forma di co-regolazione che, nel suo significato più ampio, sprona i destinatari delle norme a scegliere le soluzioni organizzative e di *governance* più adatte per affrontare e gestire i rischi, sotto il controllo delle autorità pubbliche regolatrici che verificano se gli obiettivi prefissi dalla normativa sono stati raggiunti. Questa impostazione non esprime l'unica forma di co-regolazione valorizzata dal GDPR – sui codici di condotta si dirà *infra* al par. 4 –, ma ne rappresenta certamente l'ispirazione di fondo.

3.2 La recente disciplina sui servizi di intermediazione e le piattaforme online: il DSA

Il secondo atto normativo che nel futuro sarà chiamato a regolare nuove tecnologie aventi un impatto diretto sulle società e decisive per la tutela di diritti, libertà e valori democratici è il DSA. Questo regolamento offre una complessa disciplina volta a disciplinare il ruolo di intermediari e piattaforme online in relazione alle attività e ai contenuti digitali veicolati, secondo

degli interessati», «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso»; cfr. D. WIESE SCHARTUM, *Making privacy by design operative*, in *International Journal of Law and Information Technology*, 24, 2, 2016, 151 ss.

[54] In base all'art. 32 del GDPR, occorre mettere in atto «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio», tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Più ampiamente, v. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione. Pseudonimizzazione. Sicurezza*, Giappichelli, Torino, 2017.

[55] Art. 35 GDPR.

[56] Cfr. R. BINNS, *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law*, 7, 1, 2017, 22 ss.; A. YORDANOV, *Nature and Ideal Steps of the Data Protection Impact Assessment Under the General Data Protection Regulation*, in *European Data Protection Law Review*, 3, 4, 2017, 486 ss.

[57] Art. 35, par. 7, lett. b, GDPR.

[58] N. GUNNINGHAM, *Enforcement and Compliance Strategies*, in R. BALDWIN, M. CAVE, M. LODGE (a cura di), *The Oxford Handbook of Regulation*, cit., 135 ss.

una impostazione orizzontale e non settoriale[59]. L'obiettivo dichiarato è quello di garantire «un ambiente online sicuro, prevedibile e affidabile in cui i diritti fondamentali [...] siano efficacemente tutelati e l'innovazione sia agevolata»[60].

Dal punto di vista che qui interessa maggiormente, il DSA risente di una tensione nel tentativo di bilanciare interessi che potrebbero entrare in conflitto in relazione al ruolo delle piattaforme, che da un lato favoriscono o abilitano l'esercizio dei diritti, come quelli legati alla libertà di espressione, e la costruzione dello spazio democratico, attraverso l'informazione o il dialogo all'interno della comunità; ma dall'altro offrono nuove opportunità per comportamenti potenzialmente lesivi per i diritti, come accade con la disinformazione o la diffusione di contenuti illeciti[61].

A differenza della normativa fin qui richiamata, il DSA adotta un approccio basato sul rischio in relazione al soggetto da cui dipende favorire l'esercizio, o la lesione, dei diritti. Vengono infatti definite diverse categorie di prestatori di servizi intermediari e per ciascuna di esse, secondo un ordine crescente, si fissano condizioni e obblighi diversificati che ciascuno dei soggetti sottoposti alla disciplina è chiamato ad assolvere, con un margine di autonomia e coinvolgimento che esprime diverse forme di co-regolazione[62].

Il DSA, a questo proposito, prevede una impostazione a "piramide rovesciata" o "asimmetrica"[63], con la quale di distingue tra prestatori di servizi di memorizzazione (artt. 16-18); piattaforme online (artt. 19-28), le quali non solo memorizzano le informazioni fornite da un destinatario del servizio, ma su richiesta diffondono le informazioni al pubblico[64]; piattaforme e motori di ricerca online di dimensioni molto grandi (VLOPs e VLOSEs) (artt. 33-43), che offrono i propri servizi ad un numero medio mensile di destinatari pari o superiore a 45 milioni. Sulla base di questa distinzione, il DSA stabilisce diversi regimi in proporzione ai rischi che potenzialmente derivano dai servizi offerti.

Di regola viene prevista l'esenzione dalla responsabilità dei prestatori di servizi intermediari in relazione alle informazioni fornite, ma questa è condi-

[59] Per una panoramica sui contenuti, v. F. G'SELL, *The Digital Services Act (DSA): A General Assessment*, in ANTJE VON UNGERN-STERNBERG (a cura di), *Content Regulation in the European Union – The Digital Services Act,* Trier Studies on Digital Law, 1, Verein für Recht und Digitalisierung e.V., Institute for Digital Law (IRDT), 3 aprile 2023; L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital Services Act* e *Digital Markets Act*, GFL, Milano, 2023.

[60] Cons. 9 DSA

[61] S. DEL GATTO, *Il* Digital Services Act*: un'introduzione*, in *Giornale di diritto amministrativo*, 6, 2023, 725.

[62] G. DE GREGORIO, P. DUNN, *The European risk-based approaches*, cit., 483 ss.

[63] F. G'SELL, *The Digital Services Act (DSA): A General Assessment*, cit.

[64] Art. 3, par. 1, lett. i DSA.

zionata al rispetto di un'ampia serie di regole di *due diligence*. Si tratta, ad esempio, di obblighi di trasparenza, concernenti i sistemi di raccomandazione o le pratiche pubblicitarie[65]. Oppure di predisporre specifiche procedure, come i "meccanismi di segnalazione e azione" per i prestatori di servizi di memorizzazione, che consentono agli utenti di notificare contenuti presumibilmente illegali facendo così venire meno l'esenzione di responsabilità[66], o i "sistemi interni di gestione dei reclami" da parte delle piattaforme[67]. Così facendo si intende mettere in atto «garanzie adeguate, proporzionate ed efficaci» contro gli abusi consistenti nella diffusione di contenuti manifestamente illegali[68].

Ancora più onerosi sono gli obblighi specifici per le VLOPs e VLOSEs, che devono «essere soggetti agli obblighi più stringenti in materia di dovere di diligenza, proporzionati al loro impatto per la società»[69]. Tra questi obblighi, essi particolare attenzione va prestata ai «rischi sistemici»[70], che devono essere oggetto di valutazione da parte di questi soggetti non solo in quanto derivanti da possibili abusi, ma soprattutto «dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi»[71]. Tale valutazione deve essere condotta in relazione alla specificità dei servizi e «proporzionata ai rischi sistemici»[72]. VLOPs e VLOSEs, inoltre, devono adottare misure di attenuazione di questi rischi sistemici, definite in modo che siano «ragionevoli, proporzionate ed efficaci»[73]. Infine, ulteriore novità è offerta dalle forme di controllo cui questi giganti del web devono sottostare, che si sostanziano nell'obbligo di sottoposizione ad "audit indipendenti"[74], ma anche di garantire l'accesso ai propri dati, non solo a beneficio dei Coordinatori di servizi digitali o della Commissione europea, ma anche di ricercatori abilitati che

[65] Artt. 26 e 27 per le online platforms e artt. 38 e 39 per i VLOPs e VLOSEs.

[66] Art. 16 DSA.

[67] Art. 20 DSA, ovvero forma di reclamo contro la decisione a seguito delle segnalazione o, ad esempio, di rimozione di una informazione.

[68] Cons. 63 DSA.

[69] Cons. 76 DSA.

[70] I "rischi sistemici" vengono considerati come diffusione di contenuti illegali; eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali; analoghi effetti sul dibattito civico, sui processi elettorali, sulla sicurezza pubblica; analoghi effetti in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori, alle gravi conseguenze negative per il benessere fisico e mentale della persona (art. 34, par. 1 DSA).

[71] Art. 34, par. 1 DSA.

[72] Ivi.

[73] Art. 35 DSA.

[74] Art. 37 DSA.

contribuiscano «al rilevamento, all'individuazione e alla comprensione dei rischi sistemici»[75].

In definitiva, e a differenza del GDPR, il DSA in parte distingue direttamente le categorie di intermediari su cui gravano obblighi diversificati, individuate sulla base di una valutazione di proporzionalità rispetto ai rischi per i diritti che possono derivare dalla loro attività, in parte rimette agli intermediari il compito di predisporre meccanismi – come è evidente nel caso dei *top players* – sempre in ossequio al canone di proporzionalità e di precauzione in senso "debole", allo scopo di adempiere e realizzare le finalità imposte a livello normativo, con specifico riguardo alla valutazione e gestione dei rischi o misure di trasparenza e controllo. Anche in questo caso non si tratta delle uniche forme di co-regolazione fatte proprie dal regolamento – sui codici di condotta e i protocolli di crisi v. *infra* par. 4 –, ma si tratta di previsioni rivelatrici dell'ispirazione di fondo di questa disciplina.

3.3 La futura disciplina generale sui sistemi di IA: l'AI Act

Infine, il terzo *corpus* normativo chiamato a regolare le nuove tecnologie è l'AI Act, ovvero il regolamento, non ancora entrato in vigore al momento in cui si scrive, che per la prima volta in Europa mira a disciplinare direttamente i sistemi di intelligenza artificiale secondo una impostazione anche qui non settoriale, bensì orizzontale, che investe tutti i prodotti e i possibili usi di queste tecnologie[76].

Lo sforzo dell'UE è quello di sviluppare un approccio regolativo coordinato, che tenga conto delle implicazioni umane ed etiche dell'IA mediante un quadro giuridico volto ad affrontare i rischi associati a determinati usi dell'IA. Le istituzioni dell'UE hanno preparato il terreno con diversi documenti, come gli "Orientamenti etici per un'IA affidabile", prodotte dal Gruppo di esperti ad alto livello sull'IA nel 2019, o il "Libro bianco" sull'IA pubblicato nel 2021 dalla Commissione europea, che hanno posto le basi per un approccio "umano-centrico"[77]. Tuttavia, nonostante questa esplicita attenzione alle implicazioni etiche e giuridiche, questo regolamento – come si chiarirà meglio a breve – non nasce con una impostazione immediatamente funzionale a tutelare i diritti, bensì volta a garantire la sicurezza dei pro-

[75] Art. 40 DSA. Sottolinea la novità di questi profili anche E. LONGO, *Libertà di informazione e lotta alla disinformazione nel* Digital Services Act, in *Giornale di diritto amministrativo*, 6, 2023, 741 ss.

[76] G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf. inform.*, 2, 2022, 310.

[77] L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 34, 2021, 215 ss.

dotti[78]. Non è un caso che la base giuridica di questo regolamento si rintraccia espressamente nell'art. 114 TFUE, relativo alla costruzione del mercato interno, realizzata mediante la definizione di regole armonizzate per quanto concerne lo sviluppo, l'immissione sul mercato dell'UE e l'utilizzo di sistemi di IA. Queste due anime convivono all'interno della disciplina, sebbene durante l'iter di approvazione si sia cercato, soprattutto da parte del Parlamento europeo, di spingere esplicitamente nella direzione della tutela dei diritti.

Sulla scia dei due documenti preparatori citati sopra, l'AI Act adotta una impostazione che coniuga una RBR con i due principi di proporzionalità e precauzione. Come chiarisce il considerando 26, «al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro». Questo approccio adatta «la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA». Sulla base di questo presupposto, l'AI Act individua espressamente diverse categorie di rischio in relazione alle tecnologie di IA e all'uso che se ne può fare, distinguendo tra usi dell'IA che creano "rischi inaccettabili", sistemi di IA "ad alto rischio" e ulteriori sistemi di IA associati a obblighi di trasparenza, ciascuno correlato a diverse condizioni, obblighi e gradi di responsabilità.

Nella prima categoria rientrano i sistemi che pongono "rischi inaccettabili", e che pertanto sono proibiti. Il regolamento, all'art. 5, si riferisce ai sistemi che utilizzano «tecniche subliminali» che agiscono su persone inconsapevoli, o che sfruttano «le vulnerabilità di uno specifico gruppo di persone», al fine di distorcerne il comportamento con la possibilità di provocare loro danni; sistemi di «classificazione dell'affidabilità delle persone» che possano provocare loro trattamenti pregiudizievoli o sfavorevoli; «l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto», salvo rispettare le condizioni previste – invero molto ampie – che ne giustificano l'impiego[79]. Per questi sistemi vale una presunzione assoluta di lesività nei confronti dei diritti fondamentali che di fatto si basa su un giudizio precauzionale nel suo significato "forte", anche perché si tratta di tecnologie ancora non sviluppate o che presuppongono infrastrutture ancora non realizzate, oppure un giudizio di assoluta disproporzionalità, alla luce del bilanciamento tra mezzi impiegati e l'impatto, giudicato eccessivo, sui diritti.

[78] G. MAZZINI, S. SCALZO, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza Artificiale*, Cedam, Milano, 2023, 21 ss.

[79] G. MOBILIO, *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, in *Internet Policy Review*, 12, 1, 2023.

Nella categoria dei sistemi ad "alto rischio" rientrano invece i sistemi di IA che, come elementi indipendenti o come componenti di un prodotto, risultano disciplinati dalla normativa di armonizzazione dell'UE elencata nell'allegato II oppure sono fra quelli indicati dall'allegato III[80]. Per questi sistemi vale una disciplina ispirata al c.d. New Legislative Framework, volto – come accennato poc'anzi – a garantire la sicurezza dei prodotti immessi sul mercato, di cui la marcatura CE è garanzia, e istituire un sistema di sorveglianza del mercato[81]. In questa parte, l'AI Act indica numerose condizioni che gravano su tutti i partecipanti alla catena del valore e che tendono a responsabilizzarli lasciando loro un margine significativo di valutazione e gestione dei rischi. In particolare, i fornitori, a livello organizzativo, devono disporre di un "sistema di gestione della qualità"[82] per garantire il rispetto delle nuove prescrizioni del regolamento, nonché di un "sistema di gestione dei rischi"[83], compresi quelli riferiti ai diritti fondamentali[84]. In aggiunta, prima di poter immettere queste tecnologie sul mercato, i fornitori devono dimostrare il rispetto di tutti gli obblighi previsti sottoponendo i prodotti a una "valutazione della conformità", quale verifica interna che, una volta superata, consente di apporre il marchio CE ai sistemi di IA ad alto rischio[85]. A differenza di quanto avviene per gli usi proibiti, in cui è lo stesso regolamento a esprimere una valutazione, per la categoria dei sistemi ad "alto rischio" vengono responsabilizzati i soggetti destinatari della regolazione[86].

I sistemi di IA associati ad obblighi di trasparenza sono invece quelli «destinati a interagire con le persone fisiche», per i quali occorre informare le persone del fatto che si stanno interfacciando con una macchina; oppure i sistemi di IA, come quelli per finalità generali, che generano contenuti audio-video, i quali devono indicare che il prodotto è prodotto artificialmente;

[80] Nel quale vengono indicate certe applicazioni rientranti in settori come istruzione, occupazione, accesso a servizi pubblici essenziali, attività di polizia.

[81] In particolare, sul pacchetto di riforme del 2008, v. più ampiamente EUROPEAN COMMISSION, *Supporting study for the evaluation of certain aspects of the New Legislative Framework (Decision No 768/2008/EC and Regulation (EC) No 765/2008)*, SWD(2022) 364 final/2, 16 novembre 2022.

[82] Art. 18 AI Act.

[83] Art. 9 AI Act.

[84] Tale sistema è volto a identificare e analizzare i rischi noti e ragionevolmente prevedibili qualora il sistema di IA sia utilizzato conformemente alla sua finalità prevista, in condizioni di uso improprio ragionevolmente prevedibile, nonché alla luce dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato, allo scopo di adottare misure di gestione di tali rischi. Più ampiamente, v. J. SCHUETT, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023, 1 ss.

[85] Art. 43 AI Act.

[86] T. MAHLER, *Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal*, in *The Swedish Law and Informatics Research Institute*, 2022, 1, 251 ss.

oppure, nel caso di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica, occorre fornire informazioni sul loro funzionamento[87]. Nulla toglie che un sistema ad "alto rischio" possa essere sottoposto anche a tali obblighi di trasparenza.

Per i sistemi di IA non ad alto rischio, che ipoteticamente non dovrebbero mettere a repentaglio i diritti fondamentali, l'AI Act prevede la possibilità di adottare "codici di condotta" volti a promuovere l'applicazione volontaria dei requisiti previsti per i sistemi di IA ad alto rischio[88]. Tali codici volontari, in particolare, sono volti ad attuare i principi definiti dall'AI HLEG nel 2019, favorire la sostenibilità ambientale, promuovere l'alfabetizzazione in materia di IA, facilitare la progettazione inclusiva e diversificata dei sistemi di IA, valutare e prevenire l'impatto negativo dei sistemi di IA sulle persone vulnerabili[89]. L'ufficio per l'IA e gli Stati membri incoraggiano e agevolano l'elaborazione di tali codici, anche con il supporto del Comitato europeo per l'intelligenza artificiale[90].

L'AI Act, in definitiva, opera una classificazione degli usi di queste tecnologie, associando a ciascuna di esse un determinato regime sulla base dei rischi che possono generare[91], declinando ancora diversamente i principi di precauzione e proporzionalità. Per le ipotesi di rischio inaccettabile questi principi spingono verso un divieto *tout court* (salvo eccezioni) disposto dallo stesso regolamento. Per i sistemi ad alto rischio questi principi valgono a guidare l'attività valutativa e gli adempimenti da parte dei soggetti coinvolti nella catena di valore, declinando così una forma di co-regolazione simile a quella che sta alla base del GDPR. Per i sistemi non ad alto rischio, infine, l'AI Act richiama una forma di co-regolazione intesa come co-produzione di regole generali e astratte che diviene la fonte "preferenziale" per la disciplina dei sistemi di IA che pongono solo limitatamente a repentaglio i diritti fondamentali[92]. Su quest'ultimo profilo occorre però osservare che durante i lavori preparatori, accanto ai codici di condotta, è stata introdotta – come si vedrà meglio nel par. 4 – l'ulteriore figura dei codici di buone pratiche, che, sulla scia di una impostazione che chiama più da vicino il DSA, interessano altre applicazioni di IA che potenzialmente impattano in maniera considerevole sui diritti.

[87] Art. 50 AI Act. In ogni caso sono previste eccezioni per la finalità di contrasto.

[88] Cons. 165 AI Act.

[89] Art. 95 AI Act.

[90] Art. 65 AI Act.

[91] G. DE GREGORIO, P. DUNN, *The European risk-based approaches*, cit., 488, che parlano di un approccio top-down.

[92] A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, cit., 1044.

4. Pubblico e privato nella co-regolazione delle nuove tecnologie

Una volta verificata questa diversità di approcci alla co-regolazione, strettamente legata alla regolazione basata sul rischio e guidata dai principi di precauzione e proporzionalità con l'obiettivo di funzionalizzarla, o quanto meno renderla più sensibile alla tutela dei diritti, occorre interrogarsi sul ruolo svolto dalle autorità pubbliche. In particolare, una volta colto il legame tra co-regolazione e tutela dei diritti, occorre osservare più da vicino come venga dosato lo spazio concesso ai privati e come si atteggi l'intervengo dell'autorità pubblica. Per sottolineare una tendenza comune che attraversa questi recenti strumenti di regolazione si limiterà lo sguardo alle forme di co-regolazione che si concretizzano nella produzione di regole generali e astratte che, nella sostanza, hanno una valenza normativa.

La prima, e forse più nota, di queste forme di co-regolazione è data dai "codici di condotta" previsti dalla disciplina sulla protezione dei dati personali. Il GDPR prevede questi atti come finalizzati a «contribuire alla corretta applicazione del [...] regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese»[93]. Lo scopo è appunto quello di «precisare l'applicazione» del GDPR[94] e non integrarlo nelle sue previsioni[95].

Rispetto a quanto previsto dalla precedente direttiva 46/95, il nuovo regolamento segna un passo in avanti[96]. La direttiva, infatti, prevedeva la "possibilità" di sottoporre i codici di condotta elaborati dalle associazioni rappresentative dei responsabili del trattamento all'approvazione dell'autorità di controllo o del Gruppo di lavoro ex Articolo 29[97]. Oggi, invece, gli organismi rappresentativi delle categorie dei titolari o responsabili che intendano elaborare, modificare o prorogare un codice di condotta devono sottoporlo all'autorità di controllo ai fini della relativa "approvazione"[98]. Viene inoltre ammessa la possibilità che, tramite atti di esecuzione, la Commissione attribuisca a tali codici validità generale all'interno dell'UE[99].

[93] Art. 40.1 GDPR.

[94] Art. 40.2 GDPR.

[95] EDPB, *Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679*, 2.0, 4 giugno 2019, p. 36 ss.

[96] N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, cit., 85. Sul punto anche M.C. CAUSARANO, *GDPR e forme di autoregolamentazione privata: continuità e discontinuità nella disciplina dei codici di condotta*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, PUP, Pisa, 2018, 249.

[97] art. 27.2 direttiva 46/95

[98] Art. 40.5 GDPR.

[99] Art. 40.9 GDPR.

Il GDPR, inoltre, prevede che l'adesione ad un codice di condotta valga ai fini di dimostrare il rispetto degli obblighi del titolare del trattamento[100]. La stessa adesione può anche essere presa in considerazione dall'autorità di controllo nel momento in cui deve commisurare una sanzione amministrative pecuniaria[101].

La disciplina sulla protezione dei dati personali attualmente vigente, dunque, prevede in ruolo più attivo delle autorità (pubbliche) di controllo e della Commissione, oltre che una valenza scusante, o quantomeno di riduzione della responsabilità, in caso di esercizio o adesione al prodotto della co-regolazione.

Anche il DSA prevede forme di co-regolazione intesa come co-produzione sostanziale di norme. È il caso, anche qui, dei "codici di condotta", quali strumenti, formalmente «volontari», che assumono una portata a livello di UE e che hanno lo scopo di «contribuire alla corretta applicazione» del regolamento, anche per affrontare le «sfide specifiche connesse alla lotta ai diversi tipi di contenuti illegali e ai rischi sistemici»[102].

Da una parte, vale sempre la funzione promozionale con cui la Commissione e il Comitato europeo per i servizi digitali[103] «incoraggiano e agevolano» i VLOPs e VLOSEs nell'elaborare tali codici[104]. Dall'altra, nella situazione in cui «emerga un rischio sistemico significativo», la Commissione assume un ruolo più proattivo[105], poiché «può invitare» questi soggetti o altri fornitori a partecipare all'elaborazione dei codici di condotta, assieme ad altri stakeholders rilevanti e alle autorità nazionali; può arrivare a stabilire «impegni ad adottare misure specifiche di attenuazione dei rischi»[106]; si adopera affinché i codici stabiliscano «obiettivi specifici», «indicatori chiave di prestazione per misurare il conseguimento di tali obiettivi», e «tengano debitamente conto delle esigenze e degli interessi di tutte le parti interessate, in particolare dei cittadini»[107]. Rimane fermo che la Commissione «può emanare orientamenti» per definire misure di attenuazione dei rischi sistemici[108].

[100] Art. 24.3 GDPR.
[101] Art.83.2.j GDPR.
[102] Art. 45.1 DSA.
[103] Organo consultivo indipendente composto dai coordinatori dei servizi digitali per la vigilanza sui prestatori di servizi intermediari (artt. 61 ss. DSA).
[104] Art. 45.1 DSA.
[105] N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, cit., 86; A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, cit., 1042.
[106] Art. 45.2 DSA.
[107] Art. 45.3 DSA.
[108] Art. 35.3 DSA.

In base a questa architettura e alla possibilità per la Commissione di condizionare la partecipazione e i contenuti di un codice, questi ultimi, al di là di quanto stabilito formalmente, acquistano di fatto carattere vincolante[109]. Va considerato, inoltre, che il rifiuto all'invito da parte della Commissione a conformarsi ad un codice può pesare al momento della valutazione circa il mancato rispetto della normativa[110], mentre tra le misure necessarie a porre fine o rimedio ad una violazione del regolamento possono comprendere l'impegno a rispettare un codice[111]. Si registra quindi un ruolo più incisivo della Commissione, la quale risulta ancor più protagonista rispetto alle autorità amministrative indipendenti nel caso del GDPR[112].

Accanto ai codici di condotta, già conosciuti dall'ordinamento, il DSA introduce inoltre i "protocolli di crisi", ovvero protocolli «volontari» con i quali affrontare situazioni di crisi «strettamente limitate a circostanze straordinarie che incidono sulla sicurezza pubblica o sulla salute pubblica»[113]. Anche in questo caso la Commissione «incoraggia e facilita», anche su suggerimento del Comitato europeo per i servizi digitali, i VLOPs e VLOSEs e, ove necessario, gli altri fornitori, a partecipare alla elaborazione, sperimentazione e applicazione di tali protocolli[114]. Si tratta, anche in questa ipotesi, di atti di co-regolazione "atipici"[115], per i quali occorrerà attendere la prassi applicativa per chiarire in cosa effettivamente consistano.

Da ultimo bisogna osservare come l'AI Act faccia un ampio uso della co-regolazione in una delle forme richiamate dalla Strategia di *Better Regulation* dell'UE, ovvero il rinvio a standard o norme tecniche. In particolare, si tratta delle norme armonizzate adottate da organizzazioni europee di normazione su richiesta della Commissione, come definite all'art. 2, p. 1, lett. c), del regolamento (UE) n. 1025/2012[116].

[109] R. GRIFFIN, C. VANDER MAELEN, *Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges*, 30 maggio 2023, disponibile su SSRN: https://ssrn.com/abstract=4463874.

[110] In base al cons. 104, l'adesione a un determinato codice di condotta e il suo rispetto da parte di una VLOP e VLOSE «possono essere ritenuti una misura di attenuazione dei rischi adeguata». Il fatto poi che «un fornitore di una piattaforma online o di un motore di ricerca online rifiuti, senza adeguate spiegazioni, l'invito della Commissione a partecipare all'applicazione di un tale codice di condotta potrebbe essere preso in considerazione, se del caso, nel determinare se la piattaforma online o il motore di ricerca online abbia violato gli obblighi stabiliti nel presente regolamento».

[111] Art. 75 DSA.

[112] A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, cit., 1042.

[113] Art. 48.1 DSA.

[114] Art. 48.2 DSA.

[115] A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, cit., 1039 s.

[116] Cfr. A. IANNUZZI, *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, cit., 49 ss. Tali organizzazioni sono Comitato europeo di normazione (CEN), Comitato euro-

L'importanza di questo strumento regolatorio si comprende se si considera che i fornitori che rispettano tali standards possono invocare la presunzione di conformità agli obblighi dell'AI Act per i sistemi ad alto rischio, per quelli sottoposi ai soli obblighi di trasparenza, o per i modelli di IA per finalità generali[117]. Inoltre, in presenza di una norma armonizzata, il fornitore può svolgere una valutazione della conformità sulla base del controllo interno, senza doversi avvalere di un organismo notificato esterno alla propria organizzazione[118].

In generale il regolamento esprime che «le norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA [...] dovrebbero facilitare l'efficace attuazione e consentire l'esercizio dei diritti degli interessati e di altri mezzi di ricorso garantiti dal diritto dell'Unione in materia di protezione dei dati personali nonché degli altri diritti fondamentali» (cons. 10). Sono note, tuttavia, le critiche secondo cui tali norme rimangono formalmente volontarie e non pongono regole giuridicamente vincolanti, ma di fatto assumono valenza vincolante per via delle barriere all'accesso dei mercati e i costi derivanti dalla ricerca di soluzioni alternative[119]. Gli organismi di standardizzazione, inoltre, hanno una legittimazione che deriva dalle conoscenze tecnico-scientifiche in loro possesso, ma rimangono pur sempre organismi privati, i cui relativi procedimenti decisionali vengono criticati per mancanza di trasparenza, inclusività, responsabilità e controllo giurisdizionale[120].

Anche su questo punto l'AI Act, però, introduce una novità significativa. Nel richiamare le norme armonizzate per i sistemi di IA ad alto rischio, stabilisce tuttavia che laddove tali norme non vengano adottate, o siano insufficienti, o «non tengono sufficientemente conto delle preoccupazioni in materia di diritti fondamentali», la Commissione può intervenire mediante atti di esecuzione definendo essa stessa le "specifiche comuni" attuative dei requisiti di cui al capo II del regolamento[121]. In questo modo, e in va astratta, si fa

peo di normazione elettrotecnica (Cenelec), Istituto europeo per le norme di telecomunicazione (ETSI).

[117] Art. 40 e cons. 117 AI Act.

[118] art. 43 AI Act.

[119] F. CAFAGGI, *New foundation of transnational private regulation*, in *Journal of Law and Society*, 38, 1, 2011, 20 ss.; E. FOSCH VILLARONGA, A. JR GOLIA, *Robots, standards and the law: Rivalries between private standards and public policymaking for robot governance*, in *Computer Law & Security Review*, 35, 2, 2019, 131 ss.

[120] M. EBERS, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in L.A. DIMATTEO, M. CANNARSA, C. PONCIBÒ (a cura di), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, 2022, 321 ss.

[121] Art. 41.1.a.iii AI Act. Come osservato in N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, cit., 87 s. Secondo il cons. 121, le

salva la possibilità che la Commissione (autorità pubblica) intervenga qualora l'operato degli organismi di standardizzazione (soggetti privati) non sia adeguato alla tutela dei diritti fondamentali in gioco.

A conferma di questo ruolo "tutorio" dei soggetti pubblici, inoltre, merita ricordare come l'AI Act faccia utilizzo di un ulteriore strumento di co-regolazione che richiama da vicino i codici di condotta del DSA, ovvero i "codici di buone pratiche". La previsione di questi codici è stata introdotta dal Coreper nel gennaio 2024, e va ad affiancare i "codici di condotta" per i sistemi IA non ad alto rischio presenti fin dalla proposta della Commissione del novembre 2021. A differenza di questi ultimi, i codici di buone pratiche si rivolgono ad applicazioni di IA che potenzialmente impattano in maniera considerevole con i diritti, perché coinvolgono principalmente i modelli di IA per finalità generali[122], o sono diretti a facilitare l'attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente[123]. In particolare, tali codici consentono ai fornitori di questi modelli di IA di dimostrare la *compliance* con gli obblighi previsti dal regolamento, «finché non è pubblicata una norma armonizzata»[124]. Analoga possibilità è offerta ai fornitori di modelli di IA per finalità generali con rischio sistemico[125], le cui misure di gestione devono essere «proporzionate» ai rischi[126]. Le norme tecniche armonizzate, dunque, possono sopperire ai limiti del codice di buona pratica, ma rimane sempre ferma – come visto sopra – la possibilità per la Commissione di adottare specifiche comuni.

Inoltre, in analogia allo schema (già in vigore) che si ritrova nel DSA, cambia anche il ruolo dell'autorità pubblica. È l'ufficio per l'IA, infatti, che «incoraggia e agevola» l'elaborazione di codici di buone pratiche a livello di UE al fine di contribuire alla corretta applicazione del regolamento, tenendo conto degli approcci internazionali[127], e assieme al Comitato europeo per l'intelligenza artificiale monitora e valuta periodicamente il conseguimento degli obiettivi dei codici di buone pratiche[128]. L'ufficio per l'IA, inoltre, «può invitare» tutti i fornitori di modelli di IA per finalità generali, nonché le autorità nazionali competenti, a «partecipare» all'elaborazione dei codici

specifiche comuni «dovrebbe costituire una soluzione eccezionale di ripiego per agevolare l'obbligo del fornitore di conformarsi ai requisiti del presente regolamento».

[122] Ovvero i sistemi caratterizzati da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti (art. 3.1.63 AI Act).

[123] Art. 50.7 AI Act.

[124] Art. 53.4 AI Act.

[125] Art. 55 AI Act.

[126] Art. 56.2.d AI Act.

[127] Art. 56.1 AI Act.

[128] Art. 56.6 AI Act.

di buone pratiche o ad «aderire» ad essi[129]. La Commissione, inoltre, può approvare un codice di buone pratiche per conferire ad esso una validità generale all'interno dell'UE[130], e può tener conto dell'adesione ad un codice nel commisurare una sanzione per violazione del regolamento da parte dei fornitori di modelli di IA per finalità generali[131]. Anche in questo caso, dunque, l'autorità pubblica (ufficio per l'IA o Commissione) svolge un ruolo più incisivo nell'indurre a fare ricorso alla co-regolazione, condizionarne i contenuti e vigilare sul rispetto di quanto prodotto.

5. Spunti conclusivi

L'analisi dei più recenti atti europei che disciplinano le nuove tecnologie testimonia, da una parte, una ampia diffusione della co-regolazione e, dall'altra, una specificazione articolata di forme e moduli di coinvolgimento dei privati. Lì dove questi atti seguono un approccio basato sul rischio, la tutela dei diritti fondamentali per il tramite dei principi di precauzione e di proporzionalità diviene un canone che condiziona la scelta su quale tipo di co-regolazione impiegare e su come calibrare gli obblighi in capo ai destinatari.

Il GDPR, in vigore fin dal 2018 e promosso dalla Commissione presieduta da Juncker, non opera direttamente qualificazioni di tecnologie o soggetti in base al rischio, ma affida al titolare del trattamento il compito di affrontare i rischi, sulla base di valutazioni e decisioni guidate dai due citati principi.

Il DSA, in vigore dal 2024 e promosso invece dalla Commissione presieduta da von der Leyen, si discosta da tale approccio perché va a qualificare direttamente a livello normativo, e quindi di *hard law*, diverse categorie di soggetti in proporzione ai rischi per i diritti che possono generare con le proprie attività, per poi graduare la disciplina per ciascuno di essi con oneri di tutela proporzionati e calibrati in termini precauzionali.

L'AI Act, non ancora in vigore, distingue invece i rischi in base agli impieghi dei sistemi di IA e, guidato dai due principi citati, sceglie lo strumento regolatorio per fronteggiarli, variando tra *hard law* (usi proibiti) e diverse forme di co-regolazione (per i sistemi "ad alto rischio" o gravati da obblighi di trasparenza).

Benché, dunque, si tratti di discipline che si discostano l'una dall'altra per approcci regolatori (declinazioni della *hard* e *co-regulation*), per attori politici e periodi di gestazione (Commissioni promotrici ed entrata in vigore), nonché per finalità perseguite (tutela dei dati personali; regolazione dei

[129] Art. 56.3 e c. 6 AI Act.
[130] Art. 56.6 AI Act.
[131] Art. 101.1 AI Act.

prestatori di servizi intermediari; disciplina dei prodotti basati su IA), sembrerebbe di poter ritracciare una comune tendenza a garantire la tutela dei diritti grazie ad una regolazione basata sul rischio e ai due principi di precauzione e di proporzionalità.

L'ipotesi della co-produzione normativa, inoltre, sembrerebbe dimostrare che ove ci sia la tutela dei diritti in gioco, lì l'intervento delle autorità pubbliche si faccia più marcato, allo scopo di guidare e vigilare sull'operato dei destinatari della regolazione. Si ha così la riprova di come l'UE non rinunci alla collaborazione con i privati, al loro patrimonio di conoscenze, alla condivisione degli obiettivi e alla loro responsabilizzazione, nell'intento di rendere la disciplina giuridica più effettiva. Le autorità pubbliche, inoltre, sembrano assumere un ruolo di garanzia preventiva e più marcata, a tutela dell'interesse pubblico, in particolare laddove i rischi riguardino una categoria di soggetti o attività (come nell'ipotesi dei codici di condotta del GDPR), oppure interessi generali, siano essi qualificati come "rischi sistemici" su diritti e sistemi democratici prodotti da piattaforme o motori di ricerca di dimensioni molto grandi (mediante i codici di condotta o i protocolli di crisi del DSA), o "alti rischi" derivanti da sistemi di IA (mediante le "specifiche comuni" o i "codici di buone pratiche" per i modelli di IA per finalità generali dell'AI Act)[132].

Certamente, sono comunque presenti delle contraddizioni nelle impostazioni adottate da questi atti. Basti pensare, ad esempio, a come l'AI Act faccia ricorso alla co-produzione di regole sostanzialmente normative in parte per i sistemi di IA meno impattanti sui diritti, come nel caso dei codici di condotta per i sistemi gravati da obblighi di trasparenza, in parte per tecnologie destinate a generare crescenti preoccupazioni, come nel caso dei codici di buone pratiche per modelli di IA per finalità generali – non a caso inseriti successivamente nell'articolato in corrispondenza all'esplodere del fenomeno di Chat GPT.

Nella co-regolazione, inoltre, il coinvolgimento dei destinatari della regolazione rappresenta un punto di forza e, allo stesso tempo, un elemento di debolezza. Queste normative, infatti, rimettono la loro effettiva implementazione al coinvolgimento attivo dei privati, come nel caso della predisposizione di procedure e misure tecniche e organizzative del GDPR, o delle forme di autovalutazione per i sistemi di IA ad alto rischio dell'AI Act. In questi casi, diverse analisi riportano come sia ben possibile che la disciplina rimanga inattuata e, di conseguenza, il ruolo della *hard law* e delle istituzioni pub-

[132] In parte analogamente N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, cit., 88.

bliche ne esca ridimensionato[133]. Questa ipotesi risulta ancor più plausibile quando i soggetti gravati sono le *Big Tech*, come nel caso del DSA, che possono riuscire a "catturare il regolatore" facendo leva sul proprio potere di mercato e sulla capacità di influenzare le decisioni politiche[134].

In definitiva, non siamo in presenza di trend univoci, pienamente coerenti e privi di limiti. Si tratta comunque di segnali significativi nelle politiche regolatorie sulle nuove tecnologie, con il tentativo da parte dei soggetti pubblici di coniugare la tutela dei diritti con le logiche di mercato e di profitto dei privati. Una innovazione regolatoria che cerca di tenere il passo con una innovazione tecnologica sempre più incessante, in un confronto al quale gli ordinamenti giuridici non possono sottrarsi.

[133] NOYB – EUROPEAN CENTER FOR DIGITAL RIGHTS, *GDPR: a culture of non-compliance? Numbers of evidence-based enforcement efforts*, gennaio 2024, disponibile su: https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf.

[134] J. LAUX, S. WACHTER, B. MITTELSTADT, *Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA*, in *Computer law & Security review*, 43, 2021.