

Papers di
**DIRITTO
EUROPEO**

www.papersdidirittoeuropeo.eu
ISSN 2038-0461

2026, n. 1

DIRETTORE RESPONSABILE

Maria Caterina Baruffi (Ordinario di Diritto internazionale, Università di Bergamo).

COMITATO DI DIREZIONE

Francesco Bestagno (Ordinario di Diritto dell'Unione europea, Università Cattolica del Sacro Cuore di Milano; Giudice del Tribunale dell'Unione europea); **Andrea Biondi** (Avvocato generale alla Corte di giustizia; Professor of European Law e Director of the Centre of European Law, King's College London); **Fausto Pocar** (Professore emerito, Università di Milano); **Lucia Serena Rossi** (Ordinario di Diritto dell'Unione europea, "Alma Mater Studiorum" Università di Bologna).

COMITATO SCIENTIFICO

Adelina Adinolfi (Ordinario di Diritto dell'Unione europea, Università di Firenze); **Elisabetta Bani** (Ordinario di Diritto dell'economia, Università di Bergamo); **Matteo Borzaga** (Ordinario di Diritto del lavoro, Università di Trento); **Susanna Cafaro** (Ordinario di Diritto dell'Unione europea, Università del Salento); **Laura Calafà** (Ordinario di Diritto del lavoro, Università di Verona); **Javier Carrascosa González** (Catedrático de Derecho Internacional Privado, Universidad de Murcia); **Luigi Daniele** (Ordinario di Diritto dell'Unione europea, Università di Roma "Tor Vergata"); **Angela Di Stasi** (Ordinario di Diritto internazionale, Università di Salerno); **Davide Diverio** (Ordinario di Diritto dell'Unione europea, Università di Milano); **Franco Ferrari** (Professor of Law e Director of the Center for Transnational Litigation, Arbitration, and Commercial Law, New York University); **Costanza Honorati** (Ordinario di Diritto dell'Unione europea, Università di Milano-Bicocca); **Paola Mori** (Ordinario f.r. di Diritto dell'Unione europea, Università "Magna Graecia" di Catanzaro); **Matteo Ortino** (Associato di Diritto dell'economia, Università di Verona); **Carmela Panella** (Ordinario f.r. di Diritto internazionale, Università di Messina); **Lorenzo Schiano di Pepe** (Ordinario di Diritto dell'Unione europea, Università di Genova); **Alessandra Silveira** (Profesora Associada e Diretora do Centro de Estudos em Direito da União Europeia, Universidade do Minho); **Eleanor Spaventa** (Ordinario di Diritto dell'Unione europea, Università "Bocconi" di Milano); **Stefano Troiano** (Ordinario di Diritto privato, Università di Verona); **Michele Vellano** (Ordinario di Diritto dell'Unione europea, Università di Torino).
Segretario: **Caterina Fratea** (Associato di Diritto dell'Unione europea, Università di Verona).

COMITATO DEI REVISORI

Stefano Amadeo (Ordinario di Diritto dell'Unione europea, Università di Trieste); **Bruno Barel** (Associato f.r. di Diritto dell'Unione europea, Università di Padova); **Silvia Borelli** (Associato di Diritto del lavoro, Università di Ferrara); **Laura Carpaneto** (Ordinario di Diritto dell'Unione europea, Università di Genova); **Marina Castellaneta** (Ordinario di Diritto internazionale, Università di Bari "Aldo Moro"); **Federico Casolari** (Ordinario di Diritto dell'Unione europea, "Alma Mater Studiorum" Università di Bologna); **Gianluca Contaldi** (Ordinario di Diritto dell'Unione europea, Università di Macerata); **Matteo De Poli** (Ordinario di Diritto dell'economia, Università di Padova); **Giacomo di Federico** (Ordinario di Diritto dell'Unione europea, "Alma Mater Studiorum" Università di Bologna); **Fabio Ferraro** (Ordinario di Diritto dell'Unione europea, Università di Napoli "Federico II"); **Daniele Gallo** (Ordinario di Diritto dell'Unione europea, LUISS Guido Carli); **Pietro Manzini** (Ordinario di Diritto dell'Unione europea, "Alma Mater Studiorum" Università di Bologna); **Simone Marinai** (Associato di Diritto dell'Unione europea, Università di Pisa); **Silvia Marino** (Ordinario di Diritto dell'Unione europea, Università dell'Insubria); **Emanuela Pistoia** (Ordinario di Diritto dell'Unione europea, Università di Teramo); **Francesca Ragno** (Ordinario di Diritto internazionale, "Alma Mater Studiorum" Università di Bologna); **Carola Ricci** (Associato di Diritto internazionale, Università di Pavia); **Giulia Rossolillo** (Ordinario di Diritto dell'Unione europea, Università di Pavia); **Vincenzo Salvatore** (Ordinario di Diritto dell'Unione europea, Università dell'Insubria); **Andrea Santini** (Ordinario di Diritto dell'Unione europea, Università Cattolica del Sacro Cuore di Milano); **Cristina Schepisi** (Ordinario di Diritto dell'Unione europea, Università di Roma "Tor Vergata"); **Martin Schmidt-Kessel** (Lehrstuhl für Deutsches und Europäisches Verbraucherrecht und Privatrecht sowie Rechtsvergleichung, Universität Bayreuth); **Chiara Enrica Tuo** (Ordinario di Diritto dell'Unione europea, Università di Genova).

COMITATO EDITORIALE

Diletta Danieli (Associato di Diritto dell'Unione europea, Università di Verona); **Teresa Maria Moschetta** (Associato di Diritto dell'Unione europea, Università di Roma Tre); **Rossana Palladino** (Associato di Diritto dell'Unione europea, Università di Salerno); **Cinzia Peraro** (Associato di Diritto dell'Unione europea, Università di Bergamo); **Federica Persano** (Ricercatore di Diritto internazionale, Università di Bergamo); **Angela Maria Romito** (Associato di Diritto dell'Unione europea, Università di Bari "Aldo Moro"); **Sandra Winkler** (Straordinario di Diritto della famiglia, Università di Rijeka).

Responsabile di redazione: **Isolde Quadranti** (Documentalista, Centro di documentazione europea, Università di Verona).

I contributi sono sottoposti ad un procedimento di revisione tra pari a doppio cieco (*double-blind peer review*).

Non sono sottoposti a referaggio esclusivamente i contributi di professori emeriti, di professori ordinari in quiescenza e di giudici di giurisdizioni superiori e internazionali.

Fascicolo 2026, n. 1

INDICE

Ruggiero Cafari Panico <i>In attesa che la Corte di giustizia si pronunci sulle concessioni di piccole derivazioni (riflessioni in merito alle conclusioni dell'Avvocato generale Campos Sánchez-Bordona e alla loro possibile ricaduta sulle grandi derivazioni)</i>	1
Donatella del Vescovo <i>La frontiera interna della cittadinanza: limiti dell'Unione europea alla naturalizzazione basata sull'investimento</i>	21
Francesca Ferrari, Massimiliano Bina <i>Dalla bacheca al gatekeeper: piattaforme digitali e moderazione</i>	49
Francesca Martines <i>Effettività del controllo giurisdizionale e resistenza istituzionale: la dinamica ripetitiva nel contenzioso sul Sahara occidentale</i>	69
Matteo Ortino <i>Il Digital Services Act e la produzione di conoscenza: le specificità rispetto ai tradizionali regimi di trasparenza</i>	91
Agostina Latino <i>Violenza algoritmica di genere, tecnologie predittive e diritto internazionale</i>	123
Viviana Sachetti <i>La sostenibilità ambientale quale parametro di bilanciamento nella politica energetica dell'Unione europea</i>	175
Francesco Spera <i>Alla ricerca dell'autonomia strategica attraverso atti atipici e informali: il soft law nelle relazioni esterne dell'UE</i>	197
Giacomo Furlanetto <i>Il Digital Services Act alla prova del caso «Mia Moglie»: note sociologico-giuridiche</i>	219

Il *Digital Services Act* e la produzione di conoscenza: le specificità rispetto ai tradizionali regimi di trasparenza

Matteo Ortino*

SOMMARIO: 1. Introduzione. – 2. Il ruolo sociale epistemico delle piattaforme. – 3. Produzione di conoscenza e mera trasparenza. – 3.1. Produzione invece di mero trasferimento di conoscenza. – 3.2. L’oggetto della conoscenza e della trasparenza. – 3.3. La struttura relazione della trasparenza. – 3.4. Il bene giuridico tutelato. – 4. La produzione della conoscenza regolata ma non obbligatoria. – 5. Conoscenza nuova. – 6. Conclusioni.

1. Introduzione.

Il diritto dell’economia, in una pluralità crescente di ambiti, non si limita a prescrivere esiti sostanziali, vietare condotte o collegare sanzioni a determinati atti, ma disciplina anche le condizioni epistemiche, organizzative e procedurali entro cui i fatti rilevanti devono essere individuati, i rischi valutati, le decisioni formulate, le ragioni esplicitate e gli esiti sottoposti a controllo. In questa prospettiva, il diritto non governa soltanto l’azione finale, ma anche il processo istituzionale di produzione della conoscenza che deve rendere possibile un’azione giuridicamente adeguata.

Si può parlare in questo senso di diritto come processo cognitivo-istituzionale: esso regola le condizioni che consentono di orientare il comportamento dei soggetti regolati in un ambiente complesso e incerto. Il diritto prescrive al soggetto regolato quali informazioni sono rilevanti, come deve raccoglierle, secondo quali criteri deve valutarle, come deve tradurre tale valutazione in decisione, in quale forma deve motivarla e documentarla, e secondo quali modalità essa debba essere verificabile e rivedibile. La sequenza giuridica tipica di questi regimi vede la raccolta delle informazioni rilevanti, la loro selezione e qualificazione, su cui effettuare la valutazione, da cui consegue la decisione, con relativa motivazione e documentazione, e che sono soggette a controllo, revisione e adattamento.

È sotto questo profilo che si può dire che una parte del diritto dell’economia contemporaneo si sta trasformando da diritto della condotta in diritto del processo cognitivo della condotta. Ciò non comporta, naturalmente, l’abbandono della dimensione sostanziale: obblighi, divieti, sanzioni e rimedi continuano a svolgere un ruolo essenziale. Significa però che tali elementi sostanziali sono sempre più innestati su un’infrastruttura

* Professore associato di Diritto dell’economia, Università degli Studi di Verona.

procedurale e organizzativa che ha il compito di rendere possibile una conoscenza adeguata del problema da governare.

Possiamo accennare, tra i tanti, a tre esempi, per poi soffermarci sull'ultimo.

La disciplina dei servizi di investimento rappresenta un esempio particolarmente chiaro della logica in parola. In tale ambito, l'ordinamento non si limita a prescrivere che il prodotto o la raccomandazione siano adeguati al cliente, ma impone all'intermediario di organizzarsi in modo da conoscere il cliente, comprenderne il profilo, valutarne la situazione finanziaria, gli obiettivi di investimento, l'esperienza, la conoscenza dei mercati e la tolleranza al rischio¹. La procedura di *know your customer* non costituisce, pertanto, un mero adempimento informativo, bensì il dispositivo attraverso cui il diritto rende possibile una decisione professionalmente e legalmente corretta.

In questo caso, la conoscenza richiesta è prevalentemente individualizzata e relazionale: essa serve a orientare una prestazione verso un destinatario specifico. La regolazione, in altri termini, struttura le condizioni cognitive affinché l'intermediario possa fornire prodotti, raccomandazioni e servizi adeguati al profilo del singolo investitore. Il punto decisivo è che la correttezza della condotta non dipende soltanto dall'esito finale della raccomandazione, ma anche dal fatto che essa è il risultato di un processo di raccolta, valutazione e documentazione delle informazioni giuridicamente rilevanti.

Una logica analoga si rinviene nella disciplina bancaria prudenziale, sebbene con un oggetto differente. In questo ambito, il diritto organizza assetti di *governance*, funzioni di controllo, meccanismi di *risk management*, di *reporting* e linee di responsabilità al fine di garantire che l'ente sia strutturalmente capace di conoscere i rischi cui è esposto e di agire sulla base di tale conoscenza in modo prudente². L'oggetto della conoscenza richiesta è però diverso da quello che caratterizza i servizi di investimento: non si tratta primariamente di comprendere il profilo di un singolo cliente, ma di garantire la capacità dell'ente di conoscere e governare rischi prudenziali, patrimoniali, operativi, di liquidità, di tasso, di modello, e così via.

La disciplina bancaria, quindi, offre un modello di conoscenza per la *governance*: il diritto organizza l'impresa affinché essa sia capace di produrre, strutturare e utilizzare sapere rilevante per la propria sana e prudente gestione e, indirettamente, per la stabilità del sistema finanziario. Anche in questo caso il diritto non elimina l'incertezza; la rende istituzionalmente trattabile mediante meccanismi di controllo, documentazione e revisione.

¹ [Direttiva 2014/65/UE](#) del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE, del 12 giugno 2014.

² [Direttiva 2013/36/UE](#) del Parlamento europeo e del Consiglio del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento del 27 giugno 2013, ad es. art. 74.

Il terzo esempio è dato dalla disciplina dell'UE dei servizi digitali, rappresentata *in primis* dal *Digital Services Act*³. Oltre a richiedere che la piattaforma adotti decisioni corrette in singoli casi, il regolamento pretende che il prestatore produca una conoscenza organizzata tanto della singola decisione di moderazione quanto dell'architettura complessiva del servizio e dei rischi sistemici da essa generati. Le condizioni generali devono rendere intelligibili le politiche di moderazione, il ruolo dei sistemi algoritmici, la revisione umana e i sistemi di reclamo; le decisioni devono essere motivate; i reclami devono consentire il riesame; le piattaforme e i motori di ricerca di dimensioni molto grandi devono valutare i rischi sistemici, documentarli, attenuarli, sottoporsi ad *audit*, istituire una funzione di conformità e rendere parte di tale conoscenza accessibile a autorità, ricercatori e pubblico.

La particolarità del DSA risiede nel fatto che la conoscenza qui richiesta non è soltanto individuale o prudenziale, ma organizzativa, sociotecnica e sistemica⁴. La piattaforma deve conoscere non solo il singolo contenuto problematico, ma anche il modo in cui la propria architettura, i propri sistemi di raccomandazione, i propri strumenti pubblicitari, le proprie pratiche relative ai dati e le proprie condizioni generali contribuiscono a produrre effetti sui diritti fondamentali, sul dibattito civico, sui processi elettorali, sulla salute pubblica e sui minori⁵. Il DSA, dunque, non governa semplicemente contenuti o piattaforme, governa le condizioni cognitive della *governance* privata dell'ambiente digitale⁶.

Nel prosieguo del presente scritto, ci soffermeremo su alcuni aspetti della disciplina della produzione di conoscenza dettata dal DSA, per evidenziare antitutto le differenze strutturali e funzionali con i tradizionali regimi di trasparenza (par. 3), e in secondo luogo per chiarire come l'ordinamento da un lato regola la produzione di conoscenza volontaria da parte delle piattaforme (par. 4), e dall'altro lato limita gli obblighi di produzione di conoscenza che possono essere a queste imposti (par. 5). La premessa a tali analisi, da una prospettiva non giuridica, è una sintetica descrizione del ruolo sociale epistemico delle piattaforme (par. 2).

2. Il ruolo sociale epistemico delle piattaforme.

³ [Regolamento \(UE\) 2022/2065](#) del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

⁴ G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, in *Federalismi.it*, 2025, pp. 126-156, reperibile [online](#).

⁵ P. WOLTERS, F. ZUIDERVEEN BORGESIU, *The EU Digital Services Act: what does it mean for online advertising and adtech?*, in *International Journal of Law and Information Technology*, 2025, pp. 1-25.

⁶ F. CASOLARI, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza italiana*, 2024, pp. 462-465.

Nel tema del rapporto tra piattaforme digitali e produzione della conoscenza si devono distinguere due piani concettualmente connessi ma non sovrapponibili: quello della funzione sociale ed epistemica di fatto svolta dalle piattaforme, da quello della disciplina giuridica a cui sono sottoposte le stesse. Da un lato, vi è il ruolo delle grandi piattaforme nella società dell'informazione come infrastrutture della produzione, organizzazione e distribuzione della conoscenza⁷; dall'altro, vi sono gli obblighi che l'ordinamento giuridico (in particolare tramite il DSA) impone a tali soggetti concernenti la produzione di conoscenza sui propri sistemi, sui propri rischi e sui propri effetti sociali, e più ampiamente vi è la produzione della conoscenza regolata dalla disciplina giuridica⁸.

Il presente studio si concentrerà sulla dimensione giuridica, ma non prima di avere speso qualche parola introduttiva su quella sociale, in considerazione dell'interconnessione tra le due dimensioni.

Le piattaforme, per effetto della loro posizione sistemica, producono conoscenza in senso sociale, poiché organizzano la visibilità dei contenuti, influenzano i media, condizionano il pluralismo e modellano il dibattito pubblico⁹.

Le piattaforme più grandi devono essere comprese come spazi pubblici privati nei quali si formano, si selezionano e si amplificano contenuti, opinioni e cornici interpretative¹⁰. In dottrina si richiama la nozione di «*systemic opinion power*»¹¹, intesa come il potere di creare dipendenze e di influenzare altri attori della democrazia, e si sottolinea come tale potere si esercitato a più livelli: sul cittadino individuale, sulle redazioni e sull'intero ecosistema dei media. Il nucleo dell'argomento è che le piattaforme non si limitano a offrire un supporto tecnico neutrale alla circolazione di contenuti già prodotti altrove, ma incidono strutturalmente sulla visibilità, sulla prioritizzazione, sulla scoperta e sulla rilevanza pubblica dell'informazione. La loro architettura sociotecnica determina quali contenuti emergano, quali restino periferici, quali acquisiscano forza di agenda e quali divengano oggetto di attenzione diffusa¹². È in questo senso che le

⁷ A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 2023, pp.1-26, reperibile [online](#).

⁸ J. ORLANDO-SALLING, *The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation*, in *European Law Open*, 2024, pp. 849-864; J.P. QUINTAIS, S.F. SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, in *European Journal of Risk Regulation*, 2022, pp. 191-217

⁹ G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, cit.; A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, cit.

¹⁰ Sul ruolo para-statale dei «c.d. giganti di silicio», non solo rispetto all'esercizio dei diritti individuali, ma anche rispetto alla tutela della democrazia e dello Stato di diritto, v. F. CASOLARI, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, *Giurisprudenza italiana*, 2024, pp. 462-465.

¹¹ S.B. MICOVA, A. CALEF, *Elements for Effective Systemic Risk Assessment Under the DSA*, CERRE Report, 2023.

¹² G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, cit.

piattaforme partecipano alla produzione di conoscenza: non perché «creino» ogni singolo contenuto, ma perché modellano le condizioni entro cui quel contenuto può diventare conoscenza socialmente rilevante.

Tale ruolo si manifesta anzitutto nella strutturazione dei flussi informativi. Le piattaforme agiscono attraverso sistemi di *ranking*, raccomandazione, indicizzazione, presentazione dei contenuti e organizzazione dell'attenzione che incidono sulla probabilità che un certo messaggio venga incontrato, recepito, condiviso e trasformato in riferimento cognitivo per individui e gruppi. Si richiama, a questo proposito, la letteratura sulla personalizzazione, sulla diversità dell'esposizione informativa, sull'agenda *setting* rispetto agli altri media e sul graduale modellamento delle norme del dibattito pubblico¹³. Questi elementi mostrano che le piattaforme operano come ambienti epistemici: esse non si limitano a trasportare informazioni, ma intervengono nel processo di selezione di quanto è possibile vedere e comunicare, contribuendo a definire che cosa conta come tema pubblico, che cosa appare credibile, che cosa viene ripetuto e che cosa, invece, viene marginalizzato o non raggiunge mai una soglia significativa di attenzione.

Un secondo elemento essenziale riguarda il rapporto tra piattaforme e sistema dei media. In dottrina è stato già evidenziato che la relazione tra i c.d. fornitori di piattaforme *online* di dimensioni molto grandi e i c.d. fornitori di motori di ricerca *online* di dimensioni molto grandi¹⁴, da un lato, e *media companies*, dall'altro lato, non è riducibile alla sola concorrenza economica per la pubblicità o per il tempo di attenzione degli utenti¹⁵. Essa investe direttamente le modalità di produzione dell'informazione: le redazioni, i produttori di contenuto e gli attori dell'ecosistema informativo adattano progressivamente formati, tempi, titoli, strategie distributive e scelte editoriali alle logiche di visibilità imposte dalle piattaforme. Le forme di presentazione dei contenuti, i meccanismi di raccomandazione e le funzionalità di *engagement* generano infatti *path dependencies* che si consolidano in *routine* organizzative, standard tecnici e norme culturali condivise. In questo senso, le piattaforme influenzano non solo la distribuzione dell'informazione, ma anche la sua pre-produzione, cioè il modo in cui i contenuti vengono concepiti perché possano circolare efficacemente nel loro ambiente. Da questa prospettiva, il coinvolgimento nella produzione di conoscenza è ancora più evidente: le piattaforme incidono sulle condizioni materiali e organizzative della produzione informativa da parte di soggetti terzi.

Un terzo profilo concerne la dimensione della *platform society*. È stato già osservato che le piattaforme sono ormai inestricabilmente connesse alle strutture fondamentali della società e che ciò che accade entro i loro spazi pubblici non rimane confinato ai loro utenti

¹³ Rapporto CERRE 2023, cit.; H. C. H. HOFMANN, F. PFLÜCKE (edited by), *Governance of Automated Decision-Making and EU Law*, Oxford, 2024.

¹⁴ Artt. 33 e ss. DSA.

¹⁵ Rapporto CERRE 2023, cit.; P. WOLTERS, F. ZUIDERVEEN BORGESIU, *The EU Digital Services Act: what does it mean for online advertising and adtech?*, cit.

diretti¹⁶. Le conseguenze si estendono ai soggetti complementari, alle imprese che intrattengono relazioni dirette o indirette con i servizi, agli operatori dei media e perfino ai *non-users*, in quanto anch'essi subiscono gli effetti delle trasformazioni imposte all'ecosistema informativo, al pluralismo e al dibattito civico. Da ciò deriva che la produzione di conoscenza, in questo contesto, va intesa come fenomeno collettivo, sistemico e sociale. Le piattaforme non influenzano soltanto ciò che il singolo utente conosce, ma incidono sulle condizioni attraverso cui la società nel suo complesso seleziona temi, fonti, priorità, credibilità e forme di discussione pubblica.

Facendo leva sulla realtà che abbiamo appena tratteggiato, l'ordinamento giuridico impone alle piattaforme di produrre conoscenza in senso riflessivo e regolatorio, cioè di conoscere, analizzare, documentare e comunicare tanto il proprio funzionamento interno quanto i rischi sistemici derivanti dalle loro attività e dall'uso dei propri servizi. In questa prospettiva, il regolamento non crea il ruolo epistemico delle piattaforme, ma lo assume come presupposto e lo trasforma in una serie di obblighi di auto-osservazione, *accountability* e apertura alla verifica pubblica¹⁷. Si ha quindi la conversione di un potere privato di organizzazione dell'ambiente conoscitivo in un oggetto di conoscenza giuridicamente obbligata e istituzionalmente monitorabile.

A questo punto è bene approfondire ulteriormente le differenze più rilevanti tra il ruolo sociale di fatto assunto dalle piattaforme digitali e la loro regolazione da parte dell'ordinamento giuridico. Il fatto che le piattaforme partecipino di fatto alla produzione di conoscenza pubblica non significa, di per sé, che il diritto imponga loro di «produrre conoscenza» nello stesso senso. Il DSA non chiede alle piattaforme di produrre conoscenza pubblica in generale, né pretende di disciplinare integralmente il loro ruolo epistemico nella società. Come approfondiremo nei paragrafi successivi, il regolamento impone invece obblighi di produzione di conoscenza riflessiva: le piattaforme devono conoscere i propri sistemi, conoscere i rischi che essi generano, documentare tale conoscenza, stabilizzarla in procedure e documenti, e renderla disponibile alle autorità e, in parte, alla ricerca indipendente. Si tratta dunque di una conoscenza di secondo livello, orientata non alla produzione diretta del discorso pubblico, ma alla conoscibilità regolatoria dei meccanismi che lo strutturano. La disciplina della valutazione del rischio di cui all'art. 34 DSA, su cui si rinvia *infra*, è in tale prospettiva ben esemplificativa.

Un ulteriore elemento di distinzione riguarda la formalizzazione documentale della conoscenza. Il DSA oltre a pretendere che la piattaforma conosca i rischi derivanti dall'esercizio della sua attività, richiede che tale conoscenza venga fissato in documenti giustificativi, conservata nel tempo e resa disponibile, su richiesta, alla Commissione e al coordinatore dei servizi digitali competente (art. 34, par. 3). Ciò segnala che la

¹⁶ Rapporto CERRE 2023, cit.

¹⁷ J. ORLANDO-SALLING, *The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation*, cit.

conoscenza richiesta dal regolamento non è tacita, interna o puramente manageriale, ma una conoscenza istituzionalizzata, verificabile e suscettibile di scrutinio. Il diritto, in altri termini, converte il sapere che la piattaforma deve avere sui propri effetti in una forma di sapere giuridicamente rilevante. La piattaforma non è solo centro di produzione di flussi informativi; diventa anche soggetto obbligato a produrre evidenze, analisi, tracce documentali e giustificazioni.

Su questo sfondo, l'art. 35 DSA disciplinante l'attenuazione dei rischi mostra un altro aspetto decisivo della differenza. Se il ruolo sociale delle piattaforme riguarda la loro capacità di influenzare la formazione dell'opinione e la struttura del dibattito pubblico, l'obbligo giuridico del DSA consiste nel tradurre la conoscenza prodotta attraverso la valutazione del rischio in misure di attenuazione ragionevoli, proporzionate ed efficaci. In dottrina è già stato analizzato come tali misure possono riguardare l'adeguamento della progettazione del servizio, delle caratteristiche o del funzionamento, comprese le interfacce *online*; l'adeguamento delle condizioni generali e della loro applicazione; nonché l'adattamento delle procedure di moderazione dei contenuti¹⁸. Ciò dimostra che la conoscenza che il DSA impone di produrre è finalizzata alla trasformazione dell'architettura dei sistemi. Mentre il ruolo epistemico delle piattaforme nella società è un dato strutturale, la produzione di conoscenza imposta dal DSA è diretta a correggere o attenuare gli effetti prodotti da quel ruolo¹⁹.

L'art. 36 DSA, dedicato alle situazioni di crisi, consente di cogliere un'ulteriore sfumatura. Nei momenti di grave minaccia per la sicurezza o la salute pubblica, la Commissione può imporre alle piattaforme misure specifiche di adattamento dei propri sistemi. In tali situazioni, il nesso tra piattaforme e produzione di conoscenza pubblica diventa particolarmente visibile, perché la qualità della risposta sociale dipende in misura notevole dal modo in cui le informazioni vengono selezionate, raccomandate, amplificate o frenate. Tuttavia, anche in questo caso, l'obbligo del DSA non coincide con il ruolo sociale delle piattaforme: esso consiste nella necessità di produrre rapidamente una conoscenza operativa sulla crisi, sui rischi di amplificazione, sugli usi manipolativi e sulle possibili contromisure²⁰. Di nuovo, il regolamento prende atto del ruolo epistemico delle piattaforme e lo converte in un dovere di conoscenza formalizzata e di governo dei propri sistemi in funzione della tutela dell'interesse pubblico.

La distinzione diventa ancora più netta se si considera l'art. 40, par. 4, DSA, relativo ai ricercatori abilitati. Se la dimensione «sociale» riguarda la capacità delle piattaforme

¹⁸ C.R. TRAINA, O. POLLICINO, F. PAOLUCCI (a cura di), *Guida pratica al Digital Services Act. Responsabilità degli Internet Service Provider. Obblighi specifici delle piattaforme online. Diritto degli utenti e dei titolari di diritti*, Milano, 2024, p. 86 ss.

¹⁹ R. GRIFFIN, *Governing platforms through corporate risk management: the politics of systemic risk in the Digital Services Act*, in *European Law Open*, 2025, pp. 223-253.

²⁰ G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, cit.

di produrre, organizzare e orientare la conoscenza nella società, la dimensione giuridica, rappresentata dal DSA, riguarda anche la produzione di conoscenza esterna sulle piattaforme stesse. Il regolamento prevede l'accesso ai dati da parte dei ricercatori abilitati per indagare l'evoluzione e la gravità dei rischi sistemici *online*²¹. Quindi, il legislatore UE non si accontenta della sola auto-conoscenza della piattaforma, riconoscendo implicitamente che la produzione interna di sapere sui propri rischi può essere incompleta, opaca o strategicamente orientata, e perciò costruisce le condizioni per una contro-conoscenza indipendente. Rispetto al ruolo delle piattaforme nella società dell'informazione nel modellare l'ambiente epistemico pubblico, l'art. 40 introduce un correttivo fondamentale, rendendo possibile una conoscenza terza, scientifica e istituzionale, sulle piattaforme, sui loro sistemi e sui loro effetti.

A questo punto si può precisare ancora meglio la differenza di fondo. Il ruolo sociale-epistemico delle piattaforme è costitutivo: esso concerne il fatto che, nella *platform society*, tali soggetti sono divenuti condizioni strutturali della formazione dell'opinione, del pluralismo, dell'accesso alle fonti e della definizione delle priorità cognitive collettive. Gli obblighi del DSA, invece, sono riflessivi e regolativi: essi impongono alle piattaforme di osservare sé stesse, di analizzare il proprio impatto, di documentarlo e di renderlo conoscibile in forme istituzionalmente rilevanti. Nel primo caso, la piattaforma è una infrastruttura privata della conoscenza pubblica; nel secondo, essa diventa anche oggetto e soggetto di una produzione di conoscenza regolatoria sui propri sistemi. Nel primo caso essa plasma il sapere sociale; nel secondo deve produrre sapere sui modi in cui lo plasma.

Va inoltre sottolineato che il raggio del primo piano è molto più ampio del secondo. Si è evidenziato esplicitamente che le relazioni tra i fornitori di piattaforme *online* di dimensioni molto grandi e i fornitori di motori di ricerca *online* di dimensioni molto grandi - indicati spesso con l'acronimo inglese rispettivamente VLOP (*Very Large Online Provider*) e VLOSE (*Very Large Online Search Engine*), da un lato, e la società nel suo insieme, dall'altro lato, sono assai più vaste di quelle trattate, e che il focus si è concentrato soprattutto su innovazione nella *harm protection* e *communication rights* perché questi sono i profili chiaramente indicati dalle aree di rischio del DSA²². Questo significa che il ruolo delle piattaforme nella produzione di conoscenza eccede in larga misura il perimetro degli obblighi normativi. Le piattaforme influenzano la società dell'informazione in modi molteplici e spesso non pienamente catturati dalla disciplina dei rischi sistemici. Il DSA seleziona solo alcuni di questi profili, quelli ritenuti giuridicamente rilevanti in relazione ai contenuti illegali, ai diritti fondamentali, al dibattito civico, ai processi elettorali, alla sicurezza pubblica, alla salute pubblica, ai minori e al benessere fisico e mentale. Anche questo conferma che non si possono

²¹ *Ibidem*.

²² Rapporto CERRE 2023, cit.

identificare senz'altro i due piani: il DSA non disciplina tutto il ruolo epistemico delle piattaforme, ma solo quella parte di esso che assume la forma di rischio sistemico normativamente rilevante.

3. Produzione di conoscenza e mera trasparenza.

Il modello di trasparenza delineato dal DSA non coincide, se non in parte, con il paradigma tradizionale della *disclosure* imposto alle imprese per ridurre le asimmetrie informative nei confronti dei clienti, del mercato o delle autorità pubbliche. Benché anche il DSA impieghi il lessico della trasparenza, della pubblicazione di informazioni e della comunicazione al pubblico, la sua struttura normativa si distingue in modo significativo dai regimi classici di informazione obbligatoria. Nei prossimi sottoparagrafi saranno tratteggiate alcune delle differenze più rilevanti.

3.1. Produzione invece di mero trasferimento di conoscenza.

Nel paradigma tradizionale, la trasparenza assolve prevalentemente una funzione di correzione dell'asimmetria informativa. L'impresa è considerata titolare di informazioni rilevanti – ad esempio sulle caratteristiche del prodotto, sui costi, sui rischi contrattuali, sulla propria situazione finanziaria o su eventuali conflitti di interesse – e il diritto la obbliga a trasferire (almeno alcune di) tali informazioni al cliente, all'investitore al mercato o all'autorità, affinché questi siano posti nella condizione di scegliere consapevolmente, di vigilare sul comportamento dell'impresa o di reagire in modo appropriato. In questa logica, la *disclosure* ha essenzialmente natura traslativa: il suo oggetto è un'informazione preesistente, che il diritto impone di comunicare. Il modello resta dunque fondamentalmente lineare: al possesso dell'informazione segue la comunicazione, la ricezione, e l'eventuale reazione.

Nel DSA, invece, la trasparenza non si esaurisce in una logica di trasferimento di informazioni già date, ma si inserisce in una disciplina più complessa, nella quale il diritto organizza la produzione stessa della conoscenza giuridicamente rilevante. Il regolamento, infatti, non presuppone soltanto che il prestatore disponga già di informazioni da comunicare; gli impone, prima ancora, di strutturare processi interni di osservazione, qualificazione, motivazione, documentazione e revisione²³. Nel regolamento, gli obblighi di trasparenza verso l'esterno rappresentano soltanto il profilo più visibile di una disciplina che, a un livello più profondo, interviene sulla struttura interna del processo decisionale delle imprese digitali e, in particolare, sulle condizioni organizzative della produzione della conoscenza rilevante ai fini della moderazione, della gestione dei rischi

²³ C. CAUFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, 2021, pp. 758-774, reperibile [online](#).

e della conformità²⁴. Considerato da questa prospettiva, il DSA non si limita infatti a prescrivere che il prestatore renda conto delle proprie decisioni, ma impone che esso si doti di assetti procedurali, funzionali e tecnici idonei a consentirgli di sapere, in modo sufficientemente affidabile, che cosa accade sul servizio, quali fenomeni assumano rilevanza giuridica o sistemica, con quali criteri essi debbano essere qualificati e su quali basi sia legittimo intervenire. Si può dunque sostenere che il regolamento elabori una vera e propria disciplina del «processo produttivo della conoscenza» nell'impresa di piattaforma: una disciplina che non assume la forma di un dovere generale di sorveglianza, espressamente escluso dal divieto di obblighi generali di monitoraggio (art. 8 DSA), ma quella di un insieme di doveri mirati di organizzazione epistemica, volti a rendere possibile una conoscenza contestuale, procedimentalizzata, verificabile e proporzionata, anche attraverso indagini volontarie e misure adottate in buona fede dal prestatore (art. 7 DSA).

Anticipando quanto sarà approfondito più avanti, perciò, il DSA può essere letto come una normativa che istituisce una specifica forma di responsabilità epistemica dell'impresa digitale. Esso non impone una conoscenza totale e indiscriminata dell'ambiente informativo, né converte il prestatore in un sorvegliante universale; al contrario, preserva il divieto di obblighi generali di monitoraggio (art. 8 DSA). Tuttavia, proprio entro questo limite, richiede che l'impresa si organizzi in modo da poter venire a conoscenza in modo mirato²⁵, diligente e verificabile: sapere attraverso canali istituzionali o formalizzati di acquisizione delle informazioni (artt. 9, 10, 16 DSA); sapere mediante segnalazioni qualificate (i c.d. segnalatori attendibili) e criteri di valutazione dei possibili abusi (artt. 22 e 23 DSA); sapere da acquisire nell'elaborazione della decisione stessa (art. 17 DSA) o acquisito attraverso il sistema interno dei reclami (art. 20 DSA); sapere tramite la valutazione dei propri rischi sistemici (art. 34 DSA) e dalla necessità di adattarsi per gestire questi ultimi (art. 35 DSA); e sapere che deriva dal monitoraggio e controllo indipendente interno ed esterno (artt. 37, 40, 41 e 44 DSA)²⁶. La caratteristica del DSA che occorre evidenziare, da questa prospettiva, non è quindi soltanto la trasparenza, ma la traduzione in forme giuridiche delle condizioni organizzative della conoscenza all'interno dell'impresa di piattaforma.

²⁴ A. CREMONE, *Libertà di espressione e nuove tecnologie: a complicated relationship*, in *Rivista italiana di informatica e diritto*, 2025, pp. 441-473, reperibile [online](#), evidenzia come, nell'ambiente digitale, la libertà di espressione non si esaurisca più nella manifestazione individuale del pensiero, ma dipenda dalle infrastrutture private che selezionano, raccomandano, moderano e rendono visibili i contenuti. Il DSA interviene proprio su questo livello, non disciplinando direttamente la verità della conoscenza, ma le condizioni procedurali, algoritmiche e istituzionali della sua circolazione. Attraverso obblighi di trasparenza, *notice and takedown*, *trusted flaggers*, gestione dei rischi sistemici, rendicontazione e controllo pubblico, il regolamento cerca di trasformare il potere privato delle piattaforme sulla conoscenza in un potere regolato, motivato e contestabile.

²⁵ M. HUSOVEC, *Principles of the Digital Services Act*, Oxford, 2024.

²⁶ Per un'analisi di tali disposizioni v. tra i molti K. TORSTEN, *New Digital Services Act: a practitioner's guide*, Baden-Oxford, 2024.

Gli artt. 14 e 15 sono a questo proposito emblematici. Essi non possono essere ridotti al solo paradigma della trasparenza verso l'esterno, poiché operano, in modo più profondo, come disposizioni che conformano le condizioni organizzative della produzione della conoscenza all'interno dell'impresa digitale²⁷. L'art. 14 DSA prescrive che i prestatori di servizi intermediari includano nei termini e condizioni informazioni concernenti le restrizioni imposte rispetto alle informazioni fornite dai destinatari del servizio, specificando altresì le *policy*, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, ivi compresi i processi decisionali automatizzati, la revisione umana e le regole procedurali del sistema interno di gestione dei reclami. La stessa disposizione al par. 4 richiede inoltre che tali restrizioni siano applicate e fatte valere in modo diligente, obiettivo e proporzionato, tenendo conto dei diritti e degli interessi legittimi di tutte le parti coinvolte, inclusi i diritti fondamentali dei destinatari del servizio.

Ne consegue che la norma, pur assumendo formalmente la veste di un obbligo informativo, presuppone logicamente e insieme impone una previa attività di formalizzazione, classificazione e sistematizzazione delle categorie rilevanti per l'azione del prestatore. Per descrivere coerentemente le proprie restrizioni, i criteri di moderazione, il rapporto tra automazione e decisione umana e le modalità di riesame interno, la piattaforma deve infatti aver già costruito al proprio interno un insieme di termini e concetti utilizzati per descrivere, analizzare e gestire i processi decisionali, una tassonomia delle ipotesi rilevanti, una distribuzione funzionale delle competenze e una griglia di criteri valutativi suscettibili di applicazione uniforme. In tal senso, l'art. 14 non si limita a rendere conoscibile all'esterno una pratica già data, ma concorre a costituire normativamente i termini interni della moderazione, imponendo all'impresa di rendere il proprio operato intelligibile anzitutto a sé stessa.

Analoga, sebbene distinta, è la funzione dell'art. 15 DSA, il quale obbliga i prestatori di servizi intermediari a pubblicare periodicamente relazioni di trasparenza concernenti l'attività di moderazione dei contenuti, comprensive, tra l'altro, di dati sugli ordini ricevuti dalle autorità, sulle segnalazioni trattate, sulle decisioni adottate in applicazione dei termini e condizioni, sull'impiego di mezzi automatizzati e sulle risorse umane dedicate a tali attività. Anche in questo ambito, tuttavia, la trasparenza esterna costituisce soltanto il momento terminale di un presupposto organizzativo più profondo. Conformarsi all'art. 15 richiede necessariamente che il prestatore si doti di sistemi interni di raccolta, registrazione, aggregazione, comparazione e misurazione dei dati relativi all'*enforcement*, nonché di criteri stabili di classificazione dei casi e di tracciabilità delle decisioni, senza i quali la relazione non potrebbe essere né prodotta né verificata. Sotto

²⁷ Su questa considerazione v. F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, Oxford, 2024; L. BOLOGNINI, E. PELINO, M. SCIALDONE, *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano, 2023; C. CAUFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, cit.

questo profilo, se l'art. 14 impone una formalizzazione *ex ante* delle categorie e delle procedure mediante cui la piattaforma conosce e qualifica i fatti rilevanti, l'art. 15 impone una riflessività *ex post* sul funzionamento concreto di tali categorie e procedure, obbligando l'impresa a produrre conoscenza su sé stessa, sulle proprie pratiche di moderazione, sul ruolo effettivo dell'automazione e sulla distribuzione interna delle decisioni.

Perciò, entrambe le disposizioni, pur essendo indubbiamente norme di trasparenza, devono essere lette anche come norme che traducono in termini giuridici e istituzionali il processo produttivo della conoscenza dell'impresa di piattaforma: esse obbligano quest'ultima a organizzarsi in modo da poter sapere in forma strutturata, coerente, documentabile e riesaminabile, entro un assetto regolativo che, pur escludendo obblighi generali di monitoraggio²⁸, ammette e presuppone forme specifiche di investigazione volontaria e di organizzazione diligente della conoscenza ai sensi dell'art. 7 DSA²⁹.

Un secondo esempio è costituito dalla predisposizione di canali strutturati di acquisizione della conoscenza. Le procedure di segnalazione e azione (*notice-and-action*) previste per i prestatori di hosting non assolvono soltanto a una funzione reattiva rispetto alla presenza di contenuti illegali, ma istituiscono una forma giuridicamente tipizzata di raccolta delle informazioni rilevanti (art. 16 DSA)³⁰. L'obbligo di rendere disponibili meccanismi accessibili e funzionali per la segnalazione implica infatti che l'impresa non possa limitarsi a una ricezione non strutturata e dispersa delle informazioni, ma debba costruire un'infrastruttura organizzativa idonea a trasformare la segnalazione in un oggetto suscettibile di valutazione, classificazione e trattamento. Sotto questo profilo, il DSA non impone semplicemente di prendere atto di ciò che viene portato all'attenzione del prestatore, bensì di organizzare la ricezione dell'informazione secondo modalità che ne consentano la successiva elaborazione diligente.

A questa architettura di acquisizione della conoscenza concorrono altresì gli obblighi relativi agli ordini delle autorità nazionali di agire contro contenuti illegali e di fornire informazioni specifiche (artt. 9 e 10 DSA). La stessa disciplina dei *trusted flaggers* conferma tale impostazione, poiché introduce una gerarchia istituzionalizzata delle fonti informative: la piattaforma è tenuta non solo a ricevere segnalazioni, ma a distinguere tra fonti ordinarie e fonti qualificate, attribuendo a queste ultime una priorità basata su presunzioni normative di competenza, indipendenza e affidabilità (art. 22 DSA). Il processo conoscitivo richiesto dal DSA non è dunque indifferenziato, ma selettivo, e incorpora criteri di valutazione preventiva della qualità epistemica delle fonti.

²⁸ Art. 8 DSA.

²⁹ Sull'art. 7 DSA torneremo più avanti.

³⁰ F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit.; J.P. QUINTAIS, S.F. SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, cit.

A queste dimensioni si accompagna una terza, concernente la strutturazione interna del giudizio. Le disposizioni relative alle motivazioni delle decisioni di moderazione, pur essendo formulate in termini di obblighi di comunicazione verso il destinatario del provvedimento, presuppongono logicamente un processo interno di accertamento e qualificazione dei fatti (art. 17 DSA). Per poter indicare le ragioni della decisione, i fatti e le circostanze rilevanti, la base normativa o contrattuale dell'intervento e l'eventuale ruolo degli strumenti automatizzati, il prestatore deve aver previamente costruito un percorso decisionale nel quale i dati siano stati raccolti, selezionati, interpretati e collegati a una determinata qualificazione giuridica o regolativa. La motivazione non è, in questo senso, soltanto un obbligo di esternazione, ma la manifestazione finale di una più ampia esigenza di tracciabilità cognitiva della decisione. Il DSA esige, implicitamente ma in modo inequivoco, che la decisione sia il prodotto di un procedimento ricostruibile, nel quale sia possibile individuare l'oggetto della valutazione, gli elementi fattuali considerati, i criteri applicati, la relazione tra intervento umano e automazione e la giustificazione della conclusione raggiunta. Ne deriva una limitazione significativa della discrezionalità opaca e non formalizzata, poiché la conformità alla disciplina richiede che l'impresa sappia decidere, ma anche ricostruire retrospettivamente le condizioni di conoscenza della decisione.

Un ulteriore profilo decisivo concerne la revisione interna delle decisioni e, quindi, la capacità dell'organizzazione di conoscere i propri errori. L'obbligo di istituire sistemi interni di gestione dei reclami, da trattare in modo tempestivo, diligente, non discriminatorio e non arbitrario, introduce infatti un secondo livello epistemico, distinto da quello della decisione originaria (art. 20 DSA). Per operare una revisione non arbitraria, la piattaforma deve essere in grado di confrontare casi omogenei, individuare scostamenti applicativi, verificare la correttezza delle qualificazioni operate in prima battuta e sviluppare criteri di stabilizzazione interpretativa. Il reclamo non svolge quindi soltanto una funzione rimediale a beneficio dell'utente, ma costringe l'organizzazione a riflettere sui propri processi cognitivi, a classificare gli errori, a distinguere tra margini di incertezza fisiologica e disfunzioni sistemiche, nonché a introdurre meccanismi di apprendimento istituzionale. In questa prospettiva, il DSA impone che il prestatore non solo sappia che cosa ha deciso, ma sia anche strutturalmente capace di sapere se abbia deciso correttamente, secondo parametri di coerenza, diligenza e non arbitrarietà.

Tale logica si intensifica nelle disposizioni relative ai comportamenti abusivi. La possibilità, e in taluni casi il dovere, di sospendere utenti che diffondano frequentemente contenuti manifestamente illegali, ovvero soggetti che presentino con frequenza segnalazioni o reclami manifestamente infondati, implica che la piattaforma sviluppi criteri interni per riconoscere la recidiva, la manifesta infondatezza e la manifesta illegalità (art. 23 DSA). Questi concetti non operano automaticamente, ma richiedono la costruzione di metriche, soglie, categorie valutative e procedure di accertamento idonee

a distinguere l'errore occasionale dall'abuso sistematico, il dissenso ragionevole dalla strumentalizzazione del sistema di *enforcement*. Anche sotto questo aspetto il DSA impone un'organizzazione del sapere: non solo acquisire informazioni, ma filtrare l'informazione inaffidabile, classificare la cattiva fede, misurare la frequenza dei comportamenti e documentare le ragioni delle conseguenze applicate.

L'esigenza di una conoscenza strutturata emerge con particolare evidenza nella disciplina dei *marketplaces online*. Gli obblighi di tracciabilità dei *trader* e di *compliance by design* richiedono che la piattaforma renda visibili al consumatore determinate informazioni; ma oltre a ciò, essa è obbligata a costruire procedure interne per raccogliere, verificare e mantenere informazioni attendibili sull'identità del professionista e sulle caratteristiche dei beni o servizi offerti (artt. 30 e 31 DSA). Il modello del *know your business customer* esprime chiaramente questa trasformazione della piattaforma in un soggetto tenuto a produrre conoscenza *ex ante* sulla controparte economica che abilita all'accesso al mercato. L'interfaccia stessa deve essere progettata in modo da consentire la raccolta delle informazioni rilevanti e la loro integrazione nei processi di controllo, cosicché l'architettura tecnica del servizio diviene parte integrante dell'apparato cognitivo richiesto dal regolamento³¹. La conoscenza, in altre parole, non è soltanto un contenuto mentale o documentale, ma una proprietà dell'organizzazione e del design del sistema.

Questo impianto raggiunge il suo livello più sofisticato con riferimento alle piattaforme e ai motori di ricerca di dimensioni molto grandi, per i quali il DSA impone obblighi di identificazione, analisi e valutazione dei rischi sistemici derivanti non solo dai contenuti illeciti in senso stretto, ma anche dalla progettazione, dal funzionamento e dall'uso del servizio, compresi i sistemi algoritmici (art. 34 DSA). Qui la disciplina si sposta dal livello micro della singola decisione al livello macro della riflessività organizzativa: l'impresa oltre a sapere quali singoli contenuti o comportamenti richiedano un intervento, deve conoscere quali effetti sistemici derivino dalle proprie scelte architetture, dai propri modelli di *ranking*, raccomandazione e moderazione, dalle dinamiche di viralità o dalle vulnerabilità strutturali del servizio. Inoltre, la valutazione richiesta non può essere superficiale, poiché il regolamento esige che essa consideri in modo diligente la probabilità e la gravità dei rischi, nonché la loro incidenza su beni e interessi di rilievo pubblico, quali i diritti fondamentali, il dibattito civico, i processi elettorali, la sicurezza pubblica, la tutela dei minori e il benessere individuale (art. 34, parr. 1-2 DSA)³². Il DSA impone dunque una vera e propria capacità di autoconoscenza

³¹ G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, cit.

³² F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit.

sistemica: la piattaforma deve essere in grado di produrre sapere sul proprio impatto e sul nesso tra configurazione del servizio e produzione del rischio³³.

A ciò si collega l'obbligo di adottare misure di mitigazione ragionevoli, proporzionate ed efficaci (art. 35 DSA). La rilevanza di tale previsione, sul piano qui considerato, risiede nel fatto che la conoscenza richiesta dal regolamento non ha carattere meramente descrittivo, bensì operativo. L'impresa deve sapere in modo tale da poter modificare i propri processi, le proprie interfacce, i propri sistemi di raccomandazione, le proprie condizioni di utilizzo e le proprie pratiche di *enforcement*. La conformità non è quindi separabile dalla capacità di apprendere e di tradurre l'apprendimento in intervento organizzativo. È confermato così che il DSA non disciplina soltanto un dovere di valutazione, ma una forma di razionalità riflessiva incorporata nella *governance* della piattaforma.

Vi sono poi gli obblighi di *audit* indipendente e la previsione di una *compliance function* autonoma nelle imprese di dimensioni molto grandi. L'*audit* annuale richiede che i processi di valutazione dei rischi, le misure di mitigazione e più in generale la conformità agli obblighi del regolamento siano formulati in modo sufficientemente sistematico, documentato e verificabile da consentire il controllo da parte di soggetti indipendenti dotati di adeguata competenza tecnica e metodologica (art. 37 DSA). Ciò esclude che la conoscenza rilevante ai fini del DSA possa restare puramente tacita, occasionale o frammentata tra reparti privi di coordinamento. Parallelamente, l'istituzione di una funzione di *compliance* indipendente dalle funzioni operative traduce sul piano della *governance* l'idea che la produzione della conoscenza regolatoria debba avere una sede stabile, autonoma e capace di dialogare direttamente con il *management* (art. 41 DSA). Il sapere giuridicamente rilevante non può dipendere esclusivamente dalle esigenze del prodotto o dalle metriche commerciali dell'impresa, ma deve essere raccolto, valutato e trasmesso da un centro organizzativo distinto, incaricato di identificare i rischi, monitorare la conformità, supervisionare le verifiche e promuovere l'adozione delle misure necessarie.

Infine, anche le norme sull'accesso ai dati da parte dei ricercatori e sulla standardizzazione tecnica mostrano che, per il DSA, la conoscenza conforme deve essere non solo prodotta, ma anche tecnicamente estraibile, strutturata e interoperabile. L'obbligo di predisporre interfacce o modalità di accesso adeguate ai dati, in funzione della ricerca sui rischi sistemici e sulla valutazione delle misure di mitigazione, presuppone infatti una *governance* dei dati tale da consentire la circolazione controllata dell'informazione e la sua verificabilità dall'esterno (art. 40 DSA). A ciò si aggiunge il rinvio alla definizione di standard volontari relativi, tra l'altro, alle notifiche elettroniche,

³³ J. ORLANDO-SALLING, *The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation*, cit.

alle interfacce, alle API, agli *audit* e alla *choice architecture* (art. 44 DSA)³⁴. Da questo punto di vista, la disciplina europea non si limita a richiedere un'impresa «trasparente», ma pretende un'impresa «conoscibile», vale a dire dotata di sistemi interni nei quali l'informazione rilevante sia raccolta, organizzata e resa suscettibile di controllo.

3.2. L'oggetto della conoscenza e della trasparenza.

Un secondo elemento distintivo rispetto al tradizionale regime della trasparenza riguarda l'oggetto della stessa. Nella *disclosure* classica, l'obbligo informativo concerne per lo più elementi relativamente statici o stabilizzati: condizioni contrattuali, composizione del prodotto e del prezzo, dati societari, rischi del prodotto, caratteristiche dell'offerta. Nel DSA, invece, larga parte degli obblighi concerne elementi dinamici, processuali e riflessivi: le pratiche di moderazione, le decisioni assunte sui contenuti, il funzionamento dei sistemi di raccomandazione, i criteri di presentazione della pubblicità, la valutazione dei rischi sistemici, le misure di attenuazione adottate, gli esiti dell'*audit* e i processi di conformità³⁵.

Più nel dettaglio, il DSA non si limita a imporre la comunicazione esterna di informazioni già date, ma disciplina la produzione regolata di conoscenza su ciò che la piattaforma fa, su come lo fa e su quali effetti sistemici ne derivino: conoscenza delle proprie regole interne (art. 14 DSA), conoscenza dell'illegalità specifica e delle ragioni della decisione (artt. 16 e 17 DSA), conoscenza revisionabile e correggibile (artt. 20 e 21 DSA), conoscenza dell'ambiente cognitivo dell'utente (artt. 25 e 27 DSA; considerando 67 e 70), conoscenza dei rischi sistemici e delle relative misure di attenuazione (artt. 34 e 35 DSA; considerando 79, 80, 84, 85 e 86)³⁶, nonché conoscenza aggregata, empirica e comunicabile della prassi concreta di moderazione (art. 15 DSA)³⁷.

Esemplificativo è, anzitutto, l'art. 14 DSA, che – come abbiamo *supra* già rilevato – obbliga i prestatori di servizi intermediari a esporre nei termini e condizioni non solo le restrizioni imposte rispetto alle informazioni fornite dai destinatari del servizio, ma anche le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi i processi decisionali automatizzati, la revisione umana e le regole procedurali del sistema interno di gestione dei reclami. Ne deriva che una prima forma di

³⁴ Per *choice architecture* si intende l'insieme delle scelte di progettazione dell'interfaccia digitale attraverso cui il prestatore struttura le opzioni disponibili per l'utente, ne determina la visibilità, l'ordine, la comprensibilità e la facilità di esercizio, incidendo così sulla capacità del destinatario del servizio di assumere decisioni libere, informate e reversibili. Nel DSA, tale nozione rileva in particolare nell'art. 44, in quanto oggetto di possibili standard volontari relativi alle interfacce di scelta e alla presentazione delle informazioni sui sistemi di raccomandazione.

³⁵ M. HUSOVEC, *Principles of the Digital Services Act*, cit.

³⁶ G. CONTISSA, F. GALLI, *La governance della 'disinformazione aumentata' tra Digital Services Act e AI Act*, cit.

³⁷ L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, cit.

conoscenza giuridicamente organizzata ha per oggetto le regole e i criteri interni della decisione: le condizioni generali cessano di essere mero testo contrattuale e divengono il luogo in cui la piattaforma deve rendere conoscibile il proprio quadro cognitivo interno, cioè le categorie mediante cui qualifica i contenuti, distribuisce il rapporto tra automazione e intervento umano e struttura il riesame delle decisioni.

A un secondo livello, il DSA disciplina la produzione di conoscenza concernente la possibile illegalità di contenuti specifici. Gli artt. 16 e 17 DSA impongono infatti, da un lato, la predisposizione di meccanismi di *notice-and-action* idonei a far emergere informazioni sufficientemente precise e adeguatamente motivate circa la presunta illegalità di un contenuto e, dall'altro, l'adozione di una motivazione che renda esplicite le ragioni della decisione assunta dalla piattaforma. In tal modo, il regolamento non si limita a chiedere al prestatore di intervenire, ma lo obbliga a sapere perché interviene, a collegare la decisione a fatti e circostanze identificabili e a tradurre tale sapere in una forma argomentata, verificabile e contestabile. La conoscenza disciplinata dal DSA, tuttavia, non è neppure concepita come definitiva o immune da revisione: gli artt. 20 e 21 DSA, relativi rispettivamente al sistema interno di gestione dei reclami e alla risoluzione extragiudiziale delle controversie, mostrano che la decisione iniziale deve restare permeabile alla possibilità di riesame, in modo che la conoscenza rilevante per l'*enforcement* viene costruita come conoscenza revisionabile, aperta alla contestazione e alla correzione.

A ciò si aggiunge una ulteriore dimensione, che ha per oggetto non più soltanto il singolo contenuto o la singola decisione, ma il contesto cognitivo in cui il destinatario del servizio effettua le proprie scelte³⁸. Sotto questo profilo, l'art. 25 DSA vieta alle piattaforme *online* di progettare, organizzare o gestire le proprie interfacce in modo da ingannare o manipolare i destinatari del servizio o da compromettere in modo sostanziale o distorcere la loro capacità di prendere decisioni libere e informate, mentre l'art. 27 DSA impone alle piattaforme *online* di indicare, in termini chiari e accessibili, i principali parametri utilizzati nei sistemi di raccomandazione e le opzioni disponibili ai destinatari per modificare o influenzare tali parametri. La *ratio* è esplicitata nei considerando 67 e 70, che collegano rispettivamente il divieto di *dark patterns* alla tutela della capacità decisionale autonoma e informata degli utenti e la disciplina dei sistemi di raccomandazione alla necessità di rendere conoscibili i criteri che incidono sull'accesso alle informazioni³⁹. In questo segmento, dunque, il DSA disciplina la produzione e la comunicazione di conoscenza relativa all'architettura cognitiva del servizio, ossia al

³⁸ G. GRISI, S. TOMMASI (a cura di), *Contributi in Mercato digitale e tutela dei consumatori. Prove di futuro*, Torino, 2024.

³⁹ *Ibidem*.

modo in cui l'interfaccia e gli algoritmi orientano la percezione, l'attenzione e la scelta del destinatario⁴⁰.

La dimensione più avanzata di tale costruzione normativa emerge, infine, con riguardo alle VLOP e VLOSE, per le quali il regolamento impone una vera e propria conoscenza dei rischi sistemici generati dal servizio⁴¹. L'art. 34 DSA richiede infatti di individuare, analizzare e valutare diligentemente i rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'uso del servizio, compresi quelli connessi ai sistemi algoritmici, con riferimento almeno alla diffusione di contenuti illegali, agli effetti negativi sui diritti fondamentali, sugli effetti negativi effettivi o prevedibili sui processi civici e sul discorso pubblico, nonché su salute pubblica, minori e benessere fisico e mentale⁴². Il par. 2 del medesimo articolo precisa, inoltre, che tale valutazione deve tenere conto, tra l'altro, dei sistemi di raccomandazione, dei sistemi di moderazione dei contenuti, dei termini e condizioni, dei sistemi pubblicitari⁴³, delle pratiche relative ai dati e delle possibili manipolazioni del servizio, inclusa l'amplificazione rapida e ampia di contenuti illegali o incompatibili con i termini e condizioni. In questa sede il DSA costruisce una vera e propria epistemologia regolativa del rischio sistemico, imponendo ai prestatori di valutare probabilità e gravità dei rischi, di considerare il nesso tra progettazione del servizio e produzione degli effetti dannosi, di tenere conto dell'uso non autentico, della diffusione manipolativa delle informazioni e dell'amplificazione algoritmica, nonché di conservare la documentazione giustificativa delle valutazioni svolte⁴⁴. A tale obbligo di conoscenza si collega necessariamente l'art. 35 DSA, che richiede l'adozione di misure di attenuazione ragionevoli, proporzionate ed efficaci.

Entro questa architettura, l'art. 15 DSA offre forse la manifestazione più chiara del fatto che l'oggetto della trasparenza nel DSA coincide con l'oggetto della conoscenza interna che il prestatore deve essere in grado di produrre: la relazione annuale di trasparenza deve infatti riguardare le attività di moderazione dei contenuti. In questo ambito, la trasparenza ha per oggetto il funzionamento effettivo del sistema di *enforcement*, le sue decisioni, le sue metriche, le sue procedure e i suoi esiti. In questo senso, il DSA non si limita a imporre la comunicazione esterna di informazioni già date,

⁴⁰ P. WOLTERS, F. ZUIDERVEEN BORGESIU, *The EU Digital Services Act: what does it mean for online advertising and adtech?*, cit.; C. CAUFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, cit.

⁴¹ C. BUSCH, *Platform Responsibility in the European Union: From the E-Commerce Directive to the Digital Services Act*, in B. CHAKRAVORTI, J.P. TRACHTMAN (edited by), *Defeating Disinformation*, Cambridge, 2025, pp. 20-40; R. GRIFFIN, *Governing platforms through corporate risk management: the politics of systemic risk in the Digital Services Act*, cit.

⁴² A. TURILLAZZI, M. TADDEO, L. FLORIDI, F. CASOLARI, *The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications*, cit.

⁴³ P. WOLTERS, F. ZUIDERVEEN BORGESIU, *The EU Digital Services Act: what does it mean for online advertising and adtech?*, cit.

⁴⁴ A conferma, v. i considerando 79, 80, 84, 85 e 86 del DSA.

ma disciplina la produzione regolata di conoscenza in merito alle azioni e alle modalità operative della piattaforma e agli effetti sistemici che ne possono conseguire.

3.3. La struttura relazione della trasparenza.

Un terzo profilo di differenziazione concerne la struttura relazionale della trasparenza. Nella *disclosure* tradizionale, il rapporto informativo è per lo più costruito secondo una logica essenzialmente bilaterale, che vede contrapporsi il soggetto obbligato e il destinatario delle informazioni — l'impresa al cliente, all'investitore oppure all'autorità di vigilanza — e nella quale la funzione della trasparenza si esaurisce, in larga misura, nella messa a disposizione di informazioni rilevanti in favore di un centro decisionale specifico. Per quanto riguarda il cliente, per esempio, l'assunto è che, una volta correttamente informato, egli sarà posto in condizione di decidere meglio o di proteggersi più efficacemente

Nel DSA, al contrario, la conoscenza non è configurata come bene informativo destinato a un unico interlocutore, ma come oggetto di una circolazione plurale, istituzionalizzata e differenziata, che coinvolge una pluralità di attori dotati di funzioni diverse ma complementari⁴⁵. La correzione degli squilibri informativi e dei rischi non è affidata al solo utente informato, ma è incorporata in una architettura multilivello di verifica, controllo e intervento⁴⁶. Si tratta del prestatore che produce la conoscenza, la funzione di *compliance* che la organizza e la monitora, gli *auditors* indipendenti che la verificano, il coordinatore dei servizi digitali e la Commissione che la ricevono e la valutano, i ricercatori qualificati che ne scrutinano taluni presupposti empirici, nonché, in parte, il pubblico, cui una parte di essa viene resa accessibile. In questo quadro, la trasparenza si traduce nella costruzione di una vera e propria sfera pubblica e istituzionale della verificabilità.

Tale configurazione emerge con particolare evidenza nel regime applicabile alle VLOP e ai VLOSE. Gli artt. 34 e 35 DSA impongono infatti a tali prestatori di individuare, analizzare e valutare diligentemente i rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'uso del servizio, nonché di adottare misure di attenuazione ragionevoli, proporzionate ed efficaci; ma questa conoscenza, una volta prodotta, non resta confinata all'interno dell'organizzazione, perché viene ulteriormente formalizzata in documenti distinti — relazione di valutazione del rischio, documentazione delle misure di attenuazione, *audit report*, *audit implementation report*

⁴⁵ G. GRISI, S. TOMMASI (a cura di), *Contributi in Mercato digitale e tutela dei consumatori. Prove di futuro*, cit.

⁴⁶ Sul tema v. J. ORLANDO-SALLING, *The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation*, cit.; M. HUSOVEC, *Principles of the Digital Services Act*, cit.; C. CAUFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, cit.

— ed è inserita in un circuito normativamente organizzato di trasmissione, revisione e pubblicità⁴⁷.

L'art. 42 DSA assume una valenza paradigmatica. Esso impone ai fornitori di VLOPs e VLOSEs di trasmettere al *Digital Services Coordinator* del luogo di stabilimento, alla Commissione e al *Board* almeno tre settimane prima dell'*audit*, la relazione di valutazione dei rischi prevista dall'art. 34 e, senza indebito ritardo dopo il completamento dell'*audit*, l'*audit report* di cui all'art. 37, l'*audit implementation report* e, se del caso, le informazioni sulla consultazione svolta a supporto delle misure di mitigazione. La medesima disposizione richiede inoltre che tali documenti siano messi a disposizione del pubblico, al più tardi tre mesi dopo il ricevimento dell'*audit report*, con l'eventuale rimozione delle informazioni che possano rivelare segreti commerciali o compromettere la sicurezza dei destinatari del servizio. I considerando 79, 80 e 84-86 confermano questa lettura, poiché insistono sulla necessità che i prestatori valutino probabilità e gravità dei rischi sistemici, tengano conto della progettazione e del funzionamento del servizio, dell'uso manipolativo o non autentico, dell'amplificazione algoritmica e conservino la documentazione giustificativa delle valutazioni effettuate, mostrando così che il cuore della disciplina non risiede nella semplice comunicazione di informazioni, ma nella costruzione regolata di un sapere istituzionalmente verificabile e operativamente orientato.

L'art. 42 DSA mostra quindi che il regolamento non considera sufficiente che il prestatore sappia e, eventualmente, comunichi selettivamente ciò che conosce a un'autorità o a un singolo utente, ma pretende che la conoscenza rilevante (sui rischi, sulle misure adottate, ecc.) circoli entro una rete di soggetti istituzionalmente differenziati. Ne consegue che la trasparenza, nel DSA, non è una relazione informativa semplice, bensì una infrastruttura normativa di pubblicizzazione graduata del sapere regolatorio, nella quale la conoscenza prodotta dal prestatore è destinata a transitare dall'organizzazione interna alla verifica indipendente, dalla verifica indipendente al controllo pubblico e istituzionale, e da questo, almeno potenzialmente, a una più ampia sfera di discussione e *accountability*. È proprio in questa pluralizzazione dei destinatari, dei formati e delle sedi della conoscenza che si coglie uno dei tratti di più netta discontinuità del DSA rispetto al paradigma tradizionale della *disclosure*.

Quindi, il prestatore deve anzitutto produrre la conoscenza rilevante, in particolare mediante la valutazione dei rischi sistemici e la definizione delle corrispondenti misure di attenuazione ai sensi degli artt. 34 e 35 DSA. Tale conoscenza deve poi essere organizzata e monitorata internamente attraverso una *compliance function* indipendente dalle funzioni operative, cui l'art. 41 DSA attribuisce compiti di monitoraggio della

⁴⁷ F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit.; J.P. QUINTAIS, S.F. SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, cit.

conformità, assistenza rispetto alla valutazione dei rischi, supervisione dell'*audit* e interlocuzione con il *management*. Successivamente, essa deve essere sottoposta a revisione indipendente ai sensi dell'art. 37 DSA, il quale richiede un *audit* annuale sulla conformità agli obblighi del capo III, compresi quelli relativi alla valutazione e mitigazione dei rischi sistemici. Infine, essa deve essere trasmessa alle autorità competenti e, nei limiti stabiliti dall'art. 42 DSA, esposta anche alla conoscenza pubblica. In tal modo, il DSA costruisce una sequenza normativa nella quale la conoscenza non rileva soltanto in quanto posseduta dal prestatore, ma in quanto formalizzata, verificata, comunicata e resa contestabile in una pluralità di sedi istituzionali.

A questa architettura si collega, peraltro, anche l'art. 40 DSA, che disciplina l'accesso ai dati da parte dei coordinatori dei servizi digitali, della Commissione e dei ricercatori qualificati o accreditati, nella misura necessaria a monitorare e valutare il rispetto del regolamento e a contribuire alla rilevazione, identificazione e comprensione dei rischi sistemici nell'Unione. Ciò ribadisce che la struttura relazionale della trasparenza nel DSA non si esaurisce nella coppia prestatore-destinatario dell'informazione, ma si apre a un più ampio ecosistema di scrutinio differenziato, nel quale la conoscenza prodotta dall'impresa viene sottoposta a usi distinti: uso regolatorio da parte delle autorità, uso valutativo da parte degli *auditors*, uso organizzativo da parte della *compliance function*, uso scientifico da parte dei ricercatori e uso reputazionale e discorsivo da parte del pubblico. La trasparenza, pertanto, non è più soltanto una tecnica di riequilibrio informativo, ma una tecnica di istituzionalizzazione della verificabilità, diretta a rendere il potere di piattaforma conoscibile attraverso la sua esposizione a molteplici forme di controllo.

3.4. Il bene giuridico tutelato.

Un quarto elemento distintivo concerne la natura del bene giuridico tutelato mediante la trasparenza. Nel paradigma classico della *disclosure*, infatti, l'obbligo informativo è normalmente funzionale a migliorare la qualità della decisione economica individuale oppure a correggere il comportamento di una parte in un rapporto determinato; la trasparenza opera, cioè, come tecnica di riequilibrio di una specifica asimmetria informativa, tipicamente bilaterale. Nel DSA, invece, la trasparenza è strettamente connessa alla produzione di conoscenza su effetti collettivi, aggregati e sistemici, e si colloca perciò entro una logica che non ha più come referente principale la sola autodeterminazione del singolo destinatario del servizio, ma la comprensione e la governabilità dei meccanismi attraverso cui il servizio digitale può generare rischi diffusi per una varietà di beni di rilievo pubblicistico⁴⁸.

⁴⁸ R. GRIFFIN, *Governing platforms through corporate risk management: the politics of systemic risk in the Digital Services Act*, cit.; F. CASOLARI, *Il Digital Services Act e la costituzionalizzazione dello*

Tale impostazione emerge con particolare nettezza dal regime dei rischi sistemici applicabile alle VLOP e ai VLOSE, nel quale gli artt. 34 e 35 DSA impongono non già una mera comunicazione di criticità, bensì una vera attività di individuazione, analisi, valutazione e attenuazione dei rischi derivanti dalla progettazione, dal funzionamento e dall'uso del servizio⁴⁹.

Ai considerando 84 e 85 il regolamento conferma in modo particolarmente chiaro questa torsione sistemica della trasparenza. Il primo chiarisce che, nella valutazione dei rischi sistemici, i fornitori devono concentrarsi non solo sui contenuti illegali in senso stretto, ma anche sui fattori strutturali che ne rendono possibile la diffusione o l'amplificazione, quali i sistemi algoritmici, i sistemi di raccomandazione e pubblicitari, le pratiche di raccolta e utilizzo dei dati, i termini e le condizioni e la loro applicazione, nonché il modo in cui il servizio possa essere utilizzato per diffondere o amplificare informazioni fuorvianti o ingannevoli, compresa la disinformazione. Il considerando 85 aggiunge poi che i fornitori dovrebbero conservare i documenti giustificativi delle valutazioni dei rischi effettuate, inclusi i dati di base e quelli relativi alle prove dei sistemi algoritmici. Ne risulta che il bene giuridico in questione non consiste soltanto nella conoscibilità di una decisione o di una clausola contrattuale, ma nella possibilità di rendere conoscibili, verificabili e quindi governabili i meccanismi sistemici attraverso cui il servizio produce o amplifica rischi collettivi.

In tale prospettiva, la trasparenza nel DSA non è pensata principalmente per correggere una singola asimmetria informativa in un rapporto bilaterale, ma per sostenere una più ampia epistemologia regolativa del rischio sistemico. Essa serve a far emergere il nesso tra architettura del servizio e produzione degli effetti dannosi, e a consentire che tali effetti siano oggetto di valutazione interna da parte del prestatore, di *audit* indipendente, di controllo regolatorio e, in parte, di scrutinio pubblico. L'art. 35 DSA, nel richiedere l'adozione di misure di attenuazione ragionevoli, proporzionate ed efficaci sulla base della valutazione compiuta ai sensi dell'art. 34, mostra in modo inequivoco che la trasparenza è funzionale alla trasformazione della conoscenza prodotta in intervento organizzativo. Il bene giuridico protetto, pertanto, va oltre la qualità della scelta individuale del destinatario del servizio, e riguarda la governabilità dei rischi sistemici che derivano dall'esercizio del potere di piattaforma e dalla configurazione tecnica del servizio digitale.

Sotto questo profilo, il DSA segna un passaggio decisivo: la trasparenza rileva come strumento di emersione e trattamento di fenomeni che eccedono il rapporto interindividuale e investono il funzionamento complessivo dello spazio informativo

spazio digitale europeo, cit.; J. ORLANDO-SALLING, *The Digital Services Act in the European periphery: Critical perspectives on EU digital regulation*, cit.; M. HUSOVEC, *Principles of the Digital Services Act*, cit.; C. CAUFMANN, C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, cit.

⁴⁹ C. BUSCH, *Platform Responsibility in the European Union: From the E-Commerce Directive to the Digital Services Act*, cit.

digitale. Proprio per questo, l'obbligo di produrre e conservare conoscenza sui rischi, sui dati di base e sul testing dei sistemi algoritmici assume una valenza centrale: esso rende possibile non solo conoscere *ex post* gli effetti del servizio, ma anche costruire le condizioni per una loro valutazione anticipata, una loro verifica istituzionale e una loro mitigazione ragionata. In tal senso, la trasparenza del DSA è inseparabile da una logica di responsabilità sistemica del prestatore, nella quale il bene giuridico da salvaguardare non è la sola protezione del singolo contraente o utente, ma la tutela di beni collettivi quali l'integrità del discorso pubblico, i diritti fondamentali, la sicurezza, la salute e la protezione dei minori.

4. La produzione della conoscenza regolata ma non obbligatoria.

Ai sensi dell'art. 7 DSA, gli intermediari non possono essere considerati responsabili dei contenuti illegali dei clienti per il solo fatto che, in buona fede e con diligenza, adottano misure per rilevare, identificare, rimuovere o disabilitare contenuti di tale natura, oppure per rispettare obblighi di legge. Nell'ambito del presente studio, tale disposizione offre spunti che possono essere sviluppati su molteplici piani: quello teorico della conoscenza, quello sistematico della responsabilità e sul piano pratico⁵⁰.

Sul piano teorico, con l'art. 7 DSA il legislatore europeo oltre a non trattare la conoscenza del *provider* come un dato puramente fattuale, ma come un elemento giuridicamente costruito, distingue tra norme di produzione obbligatoria di conoscenza e norme di abilitazione/incentivazione della produzione di conoscenza. Il legislatore prosegue nel solco della giurisprudenza della Corte, relativamente alla particolare condizione di neutralità c.d. del buon samaritano ai fini di riconoscere l'applicabilità del *safe harbour* degli intermediari digitali in base alla direttiva sul commercio elettronico e ora in buona parte prevista agli artt. 4-6 DSA⁵¹. In tal modo la disciplina del DSA in questione non è indifferente alla produzione di conoscenza privata: la presuppone, la

⁵⁰ F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit.; L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, cit.

⁵¹ Cfr. Corte di giustizia, sentenza del 22 giugno 2021, [cause riunite C-682/18 e C-683/18](#), *Frank Peterson c. Google LLC, YouTube Inc, et al*, EU:C:2021:503, punto. 109 «il fatto, evocato da tale giudice, che il gestore di una piattaforma di condivisione di video, come YouTube, metta in atto misure tecniche volte a individuare, tra i video comunicati al pubblico tramite la sua piattaforma, contenuti che possano violare il diritto d'autore, non implica che, così facendo, detto gestore svolga un ruolo attivo che gli conferisca la conoscenza o il controllo del contenuto di tali video e ciò a pena di escludere dal regime di esonero dalla responsabilità previsto dall'articolo 14, paragrafo 1, della direttiva sul commercio elettronico i prestatori di servizi della società dell'informazione che adottano misure finalizzate proprio a contrastare siffatte violazioni.» Sul tema della responsabilità degli intermediari *online* nel passaggio dalla direttiva del commercio elettronico del 2000 ([direttiva 2000/31/CE](#) del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno) al DSA v., C. BUSCH, *Platform Responsibility in the European Union: From the E-Commerce Directive to the Digital Services Act*, cit.

incoraggia entro certi limiti e soprattutto la tiene separata, almeno in via di principio, dalla perdita automatica dell'esenzione di responsabilità.

In questa prospettiva, l'art. 7 DSA può essere letto come una norma che interviene sulla politica della conoscenza nel diritto delle piattaforme, non perché trasformi la conoscenza in un obbligo generale, ma perché la rende giuridicamente praticabile. Se il fornitore sapesse che ogni attività di ricerca, *screening* o moderazione volontaria lo espone automaticamente a un aggravamento della responsabilità, avrebbe un forte incentivo a non sapere o a sapere il meno possibile. L'art. 7 serve precisamente a neutralizzare questo incentivo perverso, evitando che la conoscenza volontariamente prodotta sia, di per sé, punita in termini di responsabilità.

Sul piano sistematico, il regolamento, quindi, costruisce un equilibrio molto preciso: da un lato, non vuole scoraggiare l'emersione di conoscenza privata; dall'altro, non vuole convertire tale emersione in una pretesa di controllo totale dell'ambiente informativo. La conoscenza ammessa e protetta è una conoscenza contestuale, finalizzata, diligente, non una sorveglianza totale e indifferenziata.

Questo equilibrio ha un rilievo teorico ulteriore: il DSA si colloca tra due modelli opposti. Da un lato, il modello dell'irresponsabilità fondata sull'ignoranza, in cui il *provider* è incentivato a restare «ignorante». Dall'altro, il modello della responsabilità da controllo totale, in cui il fornitore è di fatto spinto a monitorare tutto. L'art. 7 DSA adotta una scelta intermedia, riconoscendo che gli intermediari moderni possiedono capacità tecniche di osservazione e intervento, ma allo stesso tempo impedendo che il semplice uso di tali capacità faccia venir meno automaticamente l'applicabilità del regime di esenzione. In termini teorici, la disposizione serve a governare la transizione da un diritto dell'intermediazione «passiva» a un diritto dell'intermediazione «organizzata e riflessiva», senza abolire del tutto la logica del *safe harbour*⁵².

Sul piano pratico-organizzativo, l'art. 7 DSA incide anzitutto sull'architettura interna di *compliance* delle piattaforme. Esso rende giuridicamente meno rischioso per i *provider* creare *team* di *trust and safety*, procedure di *moderation review*, sistemi automatizzati di *detection*, strumenti di *hash matching*, controlli *ex ante* su certe categorie di rischio o *audit* interni sui flussi di contenuti. Tali misure non sono obbligatorie, ma la loro adozione volontaria, se svolta in buona fede e con diligenza, non fa perdere da sola la protezione del regime di responsabilità. Ciò riduce il costo legale dell'investimento in infrastrutture conoscitive interne.

In concreto, per una piattaforma questo significa che può adottare meccanismi di osservazione e rilevazione senza dover temere che ogni attività di *screening* sia interpretata, automaticamente, come prova del fatto che essa ha assunto un controllo generale tale da uscire dal perimetro del *safe harbour*. L'art. 7 DSA, quindi, favorisce la

⁵² J.P. QUINTAIS, S.F. SCHWEMER, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, cit.

costruzione di una infrastruttura della conoscenza privata: *database* di segnalazioni, sistemi di classificazione del rischio, protocolli di *escalation* interna, *decision trees* per i casi dubbi, registrazione delle ragioni della rimozione, cooperazione con *trusted flaggers* o autorità. Molti di questi strumenti trovano poi il loro completamento in altre disposizioni del DSA, come i meccanismi di *notice and action*, gli obblighi di motivazione delle decisioni di moderazione, e per le VLOPs/VLOSEs i doveri di *risk assessment*, *risk mitigation* e *data access*.

Ed è qui che emergono la differenza e i rapporti tra l'art. 7, da un lato, e le altre disposizioni del DSA che impongono ai prestatori obblighi in tema di conoscenza, dall'altro lato. Il primo di per sé non impone al *provider* di organizzare una macchina cognitiva sofisticata, ma rende quella macchina compatibile con il regime di esenzione. Le «vere» norme di produzione strutturata della conoscenza sono altre, in particolare quelle in cui il DSA chiede a determinati operatori di identificare, valutare, mitigare e documentare rischi sistemici, oppure di condividere dati con ricercatori abilitati. In relazione a queste, l'art. 7 DSA opera come una norma-ponte: collega il regime dei *safe harbours* risalente alla direttiva del commercio elettronico del 2000 al nuovo mondo della *governance* informata dal rischio digitale.

C'è però anche un profilo pratico più delicato. L'art. 7 DSA non sterilizza ogni effetto giuridico della conoscenza effettivamente acquisita in un caso concreto. Se attraverso le proprie indagini il *provider* arriva a una conoscenza o consapevolezza specifica di un contenuto illecito, quella conoscenza può comunque rilevare nel funzionamento complessivo del regime del DSA e del diritto applicabile. La norma prevede soltanto che le indagini volontarie non fanno perdere di per sé l'esenzione, ma non prevede che l'accertamento effettivo di fatti specifici sia sempre irrilevante. Questo è un punto teorico e pratico decisivo, giacché l'art. 7 DSA protegge la produzione della conoscenza come attività, ma non trasforma la conoscenza prodotta in un fatto giuridicamente neutro.

Perciò, sul piano applicativo, la vera questione diventa la qualità istituzionale della conoscenza prodotta. La mera conoscenza non è sufficiente, occorrendo altresì poter dimostrare come si è saputo, con quali procedure, con quali margini di affidabilità, con quali salvaguardie per gli errori e con quali garanzie per i diritti fondamentali degli utenti⁵³. Da questo punto di vista, l'art. 7 DSA apre un tema molto importante: la produzione di conoscenza nelle piattaforme non è solo un fatto tecnico, ma un processo strutturato in cui categorie, soglie, segnali, *escalation* e decisioni costruiscono ciò che giuridicamente conta come contenuto problematico o illecito.

⁵³ Ciò si ricava da una lettura sistematica comprensiva dell'art. 7 e degli obblighi di diligenza di cui al Capo III del DSA e da indicazioni contenute in vari considerando, tra cui il principale è il considerando 26.

Sul piano pratico, questo comporta almeno quattro effetti. Si incentiva i fornitori a investire in sistemi interni di *detection* e *review*; si spinge verso la documentazione delle decisioni, perché la conoscenza rilevante deve essere tracciabile e difendibile; si rafforza il ruolo di strutture ibride uomo-macchina, in cui l'automazione filtra e segnala, mentre la decisione finale su casi complessi richiede spesso verifica umana, e da ultimo, si rende centrale il problema degli errori di classificazione, perché maggiore capacità conoscitiva significa anche maggiore rischio di *over-removal*, *bias*, compressione della libertà di espressione o trattamenti diseguali tra categorie di utenti e di contenuti. Il DSA, nel suo insieme, affronta questo rischio attraverso obblighi di trasparenza, motivazione, *redress* e attenzione ai diritti fondamentali.

Da qui si capisce anche il rilievo teorico più generale dell'art. 7 DSA. Esso mostra che, nel diritto delle piattaforme, la conoscenza non è semplicemente un presupposto della responsabilità, ma diventa un oggetto di regolazione. Il legislatore non si limita a chiedersi se il fornitore sapesse o no, ma interviene sulle condizioni in cui quest'ultimo può cercare di sapere, sui costi giuridici di questa ricerca e sulle forme organizzative entro cui tale sapere viene prodotto. Questo è il passaggio dal paradigma classico della «conoscenza come fatto soggettivo» al paradigma della «conoscenza come *output* di una infrastruttura regolata».

5. Conoscenza nuova.

Nel sistema del DSA, il divieto posto dall'art. 10, par. 2, lett. b, secondo cui l'ordine dell'autorità può riguardare soltanto informazioni già raccolte per le finalità della prestazione del servizio e rientranti nel controllo del prestatore, assume un rilievo teorico che va ben oltre la mera disciplina procedurale degli ordini informativi. La norma, infatti, chiarisce che la regolazione europea non concepisce la conoscenza detenuta dagli intermediari come una risorsa pubblicamente esigibile in modo illimitato, ma distingue con nettezza tra il piano della *disclosure* di conoscenza esistente e quello della produzione coattiva di conoscenza nuova⁵⁴.

L'autorità può imporre al prestatore di rendere disponibili dati e informazioni già presenti nella sua infrastruttura tecnico-organizzativa, ma non può costringerlo a svolgere attività ulteriori di ricerca, correlazione, inferenza o ricostruzione, tali da tradursi nella produzione *ex novo* di sapere ulteriore. In questa prospettiva, il DSA non si limita a regolare l'accesso alla conoscenza privata delle piattaforme, ma governa anche il confine della pretesa pubblica di eterodirezione dell'attività cognitiva del prestatore. L'art. 10, dunque, è inquadrabile nel tema generale della regolazione della produzione di conoscenza, rappresentandone uno dei limiti fondamentali, nella misura in cui stabilisce

⁵⁴ F. WILMAN, S. L. KALÉDA, P.J. LOEWENTHAL, *The EU Digital Services Act*, cit.

che il costo cognitivo dell'accertamento non può essere trasferito senza limiti sull'intermediario mediante un semplice ordine di informazione.

La portata sistematica di tale scelta emerge con ancora maggiore chiarezza se la si pone in relazione con l'art. 7 DSA. Come appena visto *supra*, quest'ultimo dispone che i prestatori di servizi intermediari non perdono le esenzioni di responsabilità degli artt. 4, 5 e 6 DSA per il solo fatto di svolgere, in buona fede e con diligenza, indagini volontarie di propria iniziativa o altre misure dirette a individuare, identificare e rimuovere contenuti illeciti. Il regolamento, quindi, protegge la produzione volontaria di conoscenza, sottraendola all'automatismo per cui una maggiore capacità di sapere dovrebbe necessariamente tradursi in una maggiore esposizione alla responsabilità. L'art. 10, par. 2, lett. b), completa specularmente questa architettura: se l'art. 7 rimuove il disincentivo alla conoscenza spontaneamente prodotta, l'art. 10 impedisce che tale produzione si converta in un obbligo generalizzato di creare nuova conoscenza per conto dell'autorità. Tra le due disposizioni si instaura così una dialettica regolativa assai significativa: il DSA abilita la conoscenza volontaria, ma limita la conoscenza obbligatoria; favorisce l'emersione di capacità cognitive interne al prestatore, ma nega che esse possano essere mobilitate senza limiti come prolungamento dell'apparato investigativo pubblico.

Sul piano teorico, questa dialettica consente di confermare un tratto della logica normativa di fondo del DSA: la conoscenza non è trattata come un dato psicologico o meramente fattuale, bensì come un *output* istituzionalmente organizzato, che il diritto può incentivare, tollerare, proteggere o, al contrario, sottrarre alla coercizione. Il regolamento prende così le distanze da due modelli estremi. Da un lato, rifiuta il paradigma dell'ignoranza incentivata, in cui il prestatore sarebbe spinto a «non sapere» per non compromettere la propria posizione giuridica; è precisamente questo l'esito che l'art. 7 intende scongiurare. Dall'altro lato, rifiuta altresì il paradigma della piena disponibilità pubblica delle capacità cognitive private, in cui l'autorità potrebbe pretendere che il prestatore indaghi, elabori e produca nuove informazioni ogni volta che ciò risulti utile all'*enforcement*. Il risultato è un modello intermedio, nel quale la produzione di conoscenza è giuridicamente ammessa e, in certi segmenti del regolamento, persino strutturalmente valorizzata, ma non per questo diventa una funzione pubblica delegata in via generale agli intermediari. Tale equilibrio si raccorda, inoltre, con il principio per cui il DSA non consente l'imposizione di obblighi generali di monitoraggio o di ricerca attiva generalizzata di fatti o circostanze indicativi di attività illecite.

Sul piano pratico, la distinzione produce conseguenze molto concrete nella configurazione degli ordini e nell'organizzazione interna dei *provider*. Un'autorità può domandare, ad esempio, dati identificativi, elementi d'account o altre informazioni già detenute e controllate dal prestatore, purché l'ordine sia specifico, motivato e necessario a verificare la conformità di determinati destinatari del servizio al diritto applicabile. Non può invece imporre al *provider* di costruire nuovi *dataset*, svolgere analisi investigative

ulteriori, elaborare inferenze aggiuntive o attivare forme di monitoraggio non già incorporate nelle ordinarie finalità del servizio. L'effetto sistemico è duplice. Da una parte, il prestatore è incentivato a dotarsi di infrastrutture interne di *compliance* e di moderazione, perché la conoscenza prodotta volontariamente non è, di per sé, penalizzata sul terreno delle esenzioni di responsabilità. Dall'altra, esso conserva una tutela contro la trasformazione di tali infrastrutture in un apparato di investigazione obbligatoria permanente. In termini organizzativi, ciò implica che *team* di *trust and safety*, sistemi di segnalazione, protocolli di *escalation*, strumenti di classificazione e basi dati interne possono essere sviluppati come dispositivi di *governance* privata del rischio, ma non possono essere automaticamente imposti dall'autorità come macchine di produzione cognitiva ulteriore ogniqualevolta lo Stato ne abbia interesse.

La dialettica tra tali forme di conoscenza può essere rappresentata mediante la seguente tripartizione. Vi è, anzitutto, una conoscenza volontaria, che il prestatore produce di propria iniziativa e che il DSA protegge dal rischio di ritorcersi automaticamente contro di lui sul piano della responsabilità. Vi è poi una conoscenza incorporata, già raccolta per il funzionamento del servizio e perciò suscettibile di *disclosure* mediante ordini conformi all'art. 10. Vi è, infine, una conoscenza non coercibile, cioè quella che esigerebbe un surplus di attività cognitiva ulteriore e che il regolamento sottrae alla disponibilità autoritativa proprio per evitare che il potere informativo si trasformi in un obbligo surrettizio di investigazione o, in ultima analisi, in una forma indiretta di monitoraggio generalizzato. La coesistenza di queste tre figure mostra che il DSA non adotta, né una logica di pura neutralità tecnica, né una logica di integrale pubblicizzazione delle capacità conoscitive private: esso costruisce, piuttosto, un equilibrio nel quale la conoscenza delle piattaforme è riconosciuta come giuridicamente rilevante, ma resta selettivamente distribuibile, selettivamente proteggibile e selettivamente esigibile.

6. Conclusioni.

Si può dunque affermare che il DSA conserva solo in parte la logica tradizionale della *disclosure*. In realtà, esso la supera e la ingloba entro una architettura normativa più complessa, nella quale la trasparenza svolge una funzione non meramente informativa quanto piuttosto epistemica e organizzativa. Essa non mira soltanto a trasferire informazioni dall'impresa al destinatario, ma a costringere la piattaforma a produrre un sapere verificabile su sé stessa, sui propri processi decisionali, sui propri sistemi algoritmici e sui propri effetti sistemici. La trasparenza, in questo contesto, non è più semplicemente *disclosure* di dati o caratteristiche del servizio, ma diventa una tecnica di esteriorizzazione del sapere interno e di sottoposizione del potere privato a forme di conoscibilità e controllabilità istituzionale.

In termini conclusivi, mentre il regime tradizionale di *disclosure* è orientato prevalentemente alla riduzione dell'asimmetria informativa mediante il trasferimento di informazioni, il DSA, invece, è orientato alla *governance* del potere di piattaforma mediante la produzione, formalizzazione, documentazione, circolazione e verifica di conoscenza giuridicamente rilevante. Per questa ragione, la trasparenza del DSA non è semplicemente informativa, ma, più propriamente, strutturalmente epistemica.

ABSTRACT: Il contributo analizza il *Digital Services Act* come modello regolatorio che supera la tradizionale logica della trasparenza intesa come mera *disclosure* di informazioni. La tesi centrale è che il DSA disciplini non solo la comunicazione di dati verso utenti, autorità o pubblico, ma soprattutto le condizioni organizzative, procedurali e tecniche attraverso cui le piattaforme digitali devono produrre conoscenza giuridicamente rilevante sui propri sistemi, sulle proprie decisioni e sui rischi sistemici generati dai servizi offerti. In questa prospettiva, il diritto dell'economia contemporaneo viene letto come diritto del processo cognitivo della condotta: invece di limitarsi a prescrivere esiti o divieti, esso organizza le modalità attraverso cui i soggetti regolati raccolgono informazioni, le qualificano, decidono, motivano, documentano e si sottopongono a controllo. Dopo aver distinto il ruolo sociale-epistemico delle piattaforme dalla conoscenza regolatoria imposta dal DSA, l'articolo evidenzia le differenze tra il regime europeo dei servizi digitali e i tradizionali obblighi di trasparenza. Nel DSA, la conoscenza non è solo trasferita, ma prodotta; il suo oggetto non è statico, ma dinamico e sistemico; la sua circolazione non è bilaterale, ma multilivello e istituzionalizzata. Il bene giuridico protetto non coincide soltanto con l'autodeterminazione individuale, ma riguarda la governabilità dei rischi collettivi connessi al potere di piattaforma. Particolare attenzione è dedicata agli obblighi relativi alla moderazione dei contenuti, alla motivazione delle decisioni, ai sistemi di reclamo, alla valutazione e mitigazione dei rischi sistemici, agli *audit*, alla funzione di *compliance* e all'accesso ai dati da parte dei ricercatori. Il contributo esamina inoltre la distinzione tra conoscenza volontaria, conoscenza obbligatoria e conoscenza non coercibile. Da un lato, l'art. 7 DSA protegge le indagini volontarie svolte in buona fede, evitando che la produzione spontanea di conoscenza comporti automaticamente la perdita delle esenzioni di responsabilità. Dall'altro lato, l'art. 10, par. 2, lett. b), limita gli ordini informativi alle informazioni già raccolte e sotto il controllo del prestatore, impedendo che le autorità impongano la produzione coattiva di nuova conoscenza. Ne emerge un modello intermedio: il DSA incentiva e organizza la capacità cognitiva delle piattaforme, ma non la trasforma in un obbligo generale di monitoraggio o in una funzione investigativa pubblica delegata. La trasparenza del DSA si configura così come una tecnica epistemica di *governance* del potere digitale.

PAROLE CHIAVE: *Digital Services Act*; produzione di conoscenza; trasparenza; rischi sistemici; *governance* delle piattaforme.

The Digital Services Act and Knowledge Production: Specific Features Compared to Traditional Transparency Regimes

ABSTRACT: This article examines the Digital Services Act as a regulatory model that goes beyond the traditional understanding of transparency as the mere disclosure of information. Its central claim is that the DSA regulates not only the communication of data to users, authorities or the public, but also the organizational, procedural and technical conditions through which digital platforms are required to produce legally relevant knowledge about their systems, their decisions and the systemic risks generated by their services. From this perspective, contemporary economic regulation can be understood as a law of the cognitive process of conduct: it does not merely prescribe outcomes or prohibitions but structures the ways in which regulated actors collect information, qualify it, make decisions, provide reasons, document their activity and submit it to review. After distinguishing the social-epistemic role of platforms from the regulatory knowledge required by the DSA, the article identifies the main differences between the EU digital services regime and traditional transparency obligations. Under the DSA, knowledge is not only transferred but produced; its object is not static but dynamic and systemic; its circulation is not bilateral but multi-layered and institutionalized; and the protected legal interest is not limited to individual self-determination but extends to the governability of collective risks arising from platform power. Particular attention is devoted to obligations concerning content moderation, statements of reasons, internal complaint-handling systems, systemic risk assessment and mitigation, independent audits, compliance functions and data access for researchers. The article also explores the distinction between voluntary knowledge, mandatory knowledge and non-compellable knowledge. On the one hand, Article 7 DSA protects voluntary own-initiative investigations carried out in good faith, preventing the spontaneous production of knowledge from automatically leading to the loss of liability exemptions. On the other hand, Article 10(2)(b) confines information orders to data already collected and under the provider's control, thereby preventing public authorities from compelling the production of new knowledge. The DSA thus establishes an intermediate model: it encourages and organizes the cognitive capacity of platforms, without turning it into a general monitoring obligation or a delegated public investigative function. DSA transparency therefore emerges as an epistemic technique for governing digital power.

KEYWORDS: Digital Services Act; knowledge production; transparency; systemic risks; platform governance.