

8a Commissione: Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica

Note informali sui disegni di legge n. 1136 Disposizioni per la tutela dei minori nella dimensione digitale, e nn. 1160, 1166 (Modifiche all'articolo 37 del decreto legislativo 8 novembre 2021, n. 208, in materia di impiego dei minori nell'ambito delle piattaforme digitali)

I DDL S. nn. 1136, 1160, 1166 si propongono di tutelare i diritti dei bambini sulle piattaforme digitali, in linea con il framework giuridico europeo espresso nel GDPR e nel DSA, ma anche con l'invito a estendere al digitale i diritti dell'infanzia contenuto nel General Comment 25 della UN CRC (pubblicato il 2 marzo 2021). Tuttavia, i testi dei tre disegni di legge presentano anche alcune differenze, in particolare:

- I DDL S. nn. 1160 e 1166 si concentrano sulle problematiche dell'impiego dei minori nell'ambito delle piattaforme digitali, e sui diritti di bambini e bambine alla privacy, alla tutela della propria immagine, all'identità personale e al rispetto delle opinioni del bambino. I disegni di legge, quindi, si concentrano sullo sharenting e sui baby influencer, di cui offrono una disanima approfondita. Tuttavia nel testo introduttivo di entrambi i disegni di legge si fa riferimento a altri rischi come la pedopornografia e il cyberbullismo, che esulano dai confini di questi provvedimenti;
- Il DDL S. 1136, invece, evidenzia la natura commerciale delle piattaforme e, in generale, degli ambienti digitali, che non sono progettati per e con i bambini e che traggono profitto dalla raccolta, profilazione e monetizzazione dei dati degli utenti. Oltre ai rischi di sharenting e baby influencer per la privacy e la tutela dei bambini, quindi, il DDL S. 1136 mette a fuoco i rischi della datificazione, sottolineando le responsabilità delle piattaforme e la necessità di meccanismi di *age verification*. Tuttavia, l'adozione di un linguaggio medicalizzato e allarmistico nell'introduzione solleva qualche perplessità. Inoltre, l'accento all'urgenza di regolamentare l'uso dei social media da parte dei più giovani sposta la responsabilità dalle piattaforme, e dalla mancata verifica dell'età insieme alla mancata adozione di *privacy* e *safety by design*, alla responsabilità individuale del bambino-dipendente. Sarebbe invece opportuno sottolineare come le piattaforme siano responsabili non solo della mancata verifica dell'età ma anche di incoraggiare l'uso eccessivo a causa dei *dark patterns*, mirati a catturare e mantenere l'attenzione prolungata degli utenti nel tempo.

In generale, riterrei opportuno contestualizzare in modo più chiaro i disegni di legge nn. 1136, 1160, 1166 nella cornice del passaggio del dibattito politico e accademico internazionale dai rischi all'inclusione e ai diritti digitali. In particolare, il General Comment 25¹ raccomanda di riconoscere anche negli ambienti digitali tutti i diritti dei bambini, non

¹ Livingstone, S., Third, A., & Lansdown, G. (2024). Children vs adults: negotiating UNCRC General comment No. 25 on children's rights in the digital environment. In M. Puppis, R. Mansell and H. Van den Bulck (Eds.), *Handbook of Media and Communication Governance* (pp. 414-428). Edward Elgar Publishing.

solo quello alla protezione. Analogamente, la nuova Better Internet For Kids+ Strategy della Commissione Europea² incoraggia non solo l'elaborazione di misure tese a garantire esperienze digitali sicure e a misura di bambino, attraverso standard di progettazione adeguata all'età; ma anche iniziative volte a contrastare la mancanza di competenze digitali e promuovere una maggiore autonomia e responsabilità digitale fra i più giovani.

Rispetto ai temi specifici oggetto dei disegni legge, mi preme sottolineare alcuni aspetti:

1. **Sharenting:** come ben evidenziato dai DDL S. nn. 1160 e 1166, lo sharenting (dalla crasi di share e parenting) è una pratica socioculturale che ben risponde, a livello individuale, alla costruzione dell'identità online del genitore — non a caso, i dati ci mostrano come lo sharenting sia praticato soprattutto nelle prime fasi di vita del bambino, quando il genitore deve costruirsi una nuova identità sui social media, e più intensamente da genitori più giovani, abituati a queste modalità di presentazione del sé online³. A livello sociale, inoltre, lo sharenting è parte integrante di forme di sovraesposizione del sé funzionali alla monetizzazione dei dati personali su cui si reggono le piattaforme. Oltre al rimarcare il diritto all'oblio da parte degli adolescenti che abbiano raggiunto i 14 anni, in conformità con il GDPR, è opportuno ricordare le responsabilità delle piattaforme, nonché l'opportunità di interventi di sensibilizzazione e awareness raising rivolte ai neo-genitori.
2. **Baby influencer:** in conformità con la normativa francese, i DDL propongono di introdurre provvedimenti specifici per la tutela dell'immagine dei minori, imponendo restrizioni alle aziende e ai brand che sfruttano commercialmente l'immagine di bambine e bambini. È altresì opportuno imporre ai genitori di versare i proventi dallo sfruttamento commerciale dell'immagine del minore su un conto corrente intestato allo stesso, nonché l'attenzione ai rischi in termini di benessere psicologico dei minori. In relazione a questo aspetto, le disposizioni contenute nei DDL S. nn. 1160 e 1166 sono più complete e puntuali.
3. **Pubblicità targettizzata e profilazione:** aggiungerei un riferimento esplicito al DSA e all'obbligo, per i fornitori di piattaforme online, non solo a richiedere il consenso dell'utente prima del trattamento dei dati personali per pubblicità mirata; ma, soprattutto, a non “presentare inserzioni pubblicitarie basate sulla profilazione utilizzando i dati personali del destinatario del servizio se sono consapevoli con ragionevole certezza che il destinatario del servizio è minore”. La pubblicità mirata destinata a bambini e bambine, infatti, li pone di fronte a forti rischi di manipolazione e influenza. Questo vale altresì per i *dark patterns*, ovvero la progettazione di interfacce e contenuti che portano subdolamente l'utente a compiere le scelte più vantaggiose per le piattaforme in termini di monetizzazione dei dati e del tempo di utilizzo. I dark patterns sono vietati dal DSA.
4. **Influencer marketing:** in ottemperanza al framework europeo, è opportuno includere un riferimento all'obbligo di trasparenza sulla natura sponsorizzata di contenuti in

² <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022DC0212>

³ Mascheroni, G., Cino, D., Amadori, G., & Zaffaroni, L. G. (2023). (Non-)Sharing as a Form of Maternal Care? The Ambiguous Meanings of Sharenting for Mothers of 0- To-8-Year-Old Children. *Italian Sociological Review*, 13(1), 111-130. <https://doi.org/10.13136/isr.v13i1.635>

apparenza *user generated*. In seguito alla diffusione di influencer artificiali, creati con IA generativa, è inoltre necessario, a mio avviso, richiedere alle piattaforme e ai brand di esplicitare la natura artificiale dell'influencer e dei contenuti, per evitare forme di manipolazione e pubblicità ingannevole di cui siano destinatari i minori.

5. **Meccanismi di age verification:** su questo aspetto, il mio invito è quello di incorporare in maniera più esplicita le indicazioni del DSA rispetto all'esigenza di minimizzare i dati raccolti dalle piattaforme anche per esigenze di verifica dell'età: "Conformemente al regolamento (UE) 2016/679, in particolare al principio della minimizzazione dei dati di cui al suo articolo 5, paragrafo 1, lettera c), tale divieto non dovrebbe indurre il fornitore della piattaforma online a mantenere, acquisire o trattare un numero di dati personali superiore a quello di cui dispone già per valutare se il destinatario del servizio è un minore".
6. **Trasparenza:** Inoltre, la trasparenza, prima ricordata rispetto alla pubblicità mirata e all'influencer marketing (di natura artificiale o meno), dovrebbe riguardare in generale il funzionamento degli algoritmi, e i termini e le condizioni di utilizzo di tutte le piattaforme o i servizi digitali accessibili ai minori: "I prestatori di servizi intermediari destinati principalmente ai minori, ad esempio attraverso la progettazione o la commercializzazione del servizio, o che sono utilizzati prevalentemente da minori, dovrebbero compiere sforzi particolari per rendere la spiegazione delle loro condizioni generali facilmente comprensibile ai minori".
7. **Datificazione:** il modello di business incentrato sulla monetizzazione dei dati personali, noto anche come capitalismo della sorveglianza, è dannoso: la classificazione dei minori in "tipi misurabili"⁴, ovvero profili di consumatori, implica necessariamente una stereotipizzazione e una "indifferenza formale"⁵ all'identità unica di ogni bambina e bambino. Oltre a rischi rappresentazionali e alla predeterminazione dei consumi culturali —con la riproposizione di contenuti simili a quelli già fruiti—, ne consegue anche il rischio di un'amplificazione delle diseguaglianze sociodigitali nell'accesso a risorse e opportunità sia online che offline. In tal modo i giovani utenti vengono privati della capacità di esercitare un controllo sulla propria identità e sulla propria agency⁶.
8. **Protezione dei minori online:** il diritto a essere protetti non deve mai andare a discapito degli altri diritti dell'infanzia riconosciuti nella UN CRC e estesi al digitale con il general Comment 25. Due decenni di ricerca empirica sulle opportunità e i rischi di internet per i minori⁷ ci hanno mostrato alcune evidenze: in primo luogo, che rischi e opportunità sono associati, tanto che diminuire l'esposizione ai rischi significa necessariamente ridurre le opportunità tangibili del digitale. Inoltre, rischio non significa danno: a fronte di una maggiore incidenza dei rischi che i giovani possono incontrare online —fra cui si segnalano contenuti d'odio e discriminatori, contenuti pornografici e contenuti dannosi per la salute come quelli che promuovono forme di autolesionismo o disturbi

⁴ Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York University Press.

⁵ Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, 30(1), 75-89.

⁶ Mascheroni, G. & Siibak, A. (2021). *Datafied Childhoods: Data Practices and Imaginaries in Children's Lives*. New York: Peter Lang

⁷ Si veda l'esperienza di EU Kids Online <http://www.eukidsonline.net/>

alimentari⁸—la maggior parte delle ragazze e dei ragazzi è in grado di sviluppare forme di resilienza e strategie di coping. Tuttavia, i dati mostrano che vulnerabilità online e offline vanno di pari passo: a essere maggiormente esposto alle conseguenze dannose dei rischi di internet sono i giovani già vulnerabili offline, a causa sia di fattori personali (difficoltà e malessere psicologico, tratti della personalità che li rendono inclini a comportamenti rischiosi, ecc.) e sociali (povertà economica, educativa e sociale, esclusione, l'aver subito forme di discriminazione, ecc.). L'efficacia delle iniziative volte a proteggere i bambini online e favorirne l'inclusione digitale dipende in misura cruciale dal contrasto delle diseguaglianze sociali e dall'inclusione sociale di tutte le bambine e i bambini.

Milano, 15 luglio 2024

Giovanna Mascheroni

Prof. Ordinaria di Sociologia dei Processi Culturali e Comunicativi

Università Cattolica del Sacro Cuore di Milano

Vice-Coordinatrice EU Kids Online

⁸ Mascheroni, G., & Cino, D. (2022). *Contesti e competenze digitali degli adolescenti italiani. Risultati dalla seconda wave della survey ySKILLS*. Zenodo. <https://doi.org/10.5281/zenodo.7677048>