
Dai *Dark Patterns* agli *Hyper-Engaging Dark Patterns*: per un'applicazione moderna del divieto ex art. 25 DSA*

Alessio Scaffidi, Vincenzo Forte

Sommario

1. Introduzione – 2. Articolo 25 DSA, una norma già obsoleta? – 3. Gli *Hyper-Engaging Dark Patterns*: maggiori rischi, tutele minori (e inique) – 4. Conclusione

1. Introduzione

Il 1° novembre 2022 il Regolamento (UE) 2022/2065, meglio conosciuto come Digital Services Act (DSA) è entrato in vigore all'esito di un lungo *iter* negoziale¹. Come facilmente deducibile dalla stessa nomenclatura, il DSA disciplina la fornitura di servizi di intermediazione *online* all'interno dell'Unione europea ponendosi, contestualmente, l'obiettivo di contrastare la diffusione sulle piattaforme digitali di disinformazione e di contenuti

* Questo lavoro è stato condotto nell'ambito del PRIN 2022 "Towards Stricter Rules on Transparency and Liability for Online Platforms in the European Digital Single Market", codice 20223KNYEX, responsabile nazionale Prof. Giuseppe Morgese, finanziato dall'Unione europea - PNRR Next Generation EU - Investimento M4.C2.1.1 - CUP I53D23002870006. Introduzione e conclusioni sono frutto di riflessioni comuni dei due autori; il § 2 è opera del dott. Forte, mentre il § 3 è opera del dott. Scaffidi. Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

¹ 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 - DSA). Sebbene il DSA sia stato presentato dalla Commissione nel dicembre 2020, solo nell'aprile 2022 è stato raggiunto un accordo politico tra le istituzioni europee, seguito poi dall'approvazione formale del testo il 19 ottobre 2022. Il regolamento è quindi entrato in vigore nel novembre 2022. Ai sensi delle disposizioni transitorie, entro il 17 febbraio 2023, le piattaforme e i motori di ricerca online erano tenuti a pubblicare il numero di utenti attivi medi mensili da essi registrati. Successivamente, a partire dalla fine dell'agosto 2023, le norme del regolamento hanno trovato applicazione nei confronti delle piattaforme e dei motori di ricerca designati come VLOPs e VLOSEs (*amplius* nota 8). Infine, il 17 febbraio 2024, il regolamento è divenuto vincolante per tutte le piattaforme di intermediazione *online*, indipendentemente dalla loro dimensione o classificazione.

illegali².

Proprio al fine di perseguire tale *mission*, il DSA introduce un paradigma normativo innovativo³ che si sostanzia, principalmente, in una stretta collaborazione tra privati, operatori economici digitali e autorità pubbliche⁴, ma anche nell'imposizione di obblighi e, eventualmente di sanzioni⁵; il tutto – come anticipato – allo scopo di bilanciare le esigenze di tutela dei diritti fondamentali degli utenti con quelle di un funzionamento equo e sostenibile del mercato digitale.

L'ambito applicativo del DSA si estende a tutti gli intermediari *online*

² Come affermato dalla Commissione europea in diversi documenti preparativi, il Regolamento sui servizi digitali mira a creare uno spazio digitale più sicuro in cui siano tutelati i diritti fondamentali degli utenti, nonché a creare condizioni di parità per le imprese; sul punto, *ex multis*, cfr. Commissione Europea, *Impact Assessment – Digital Services Act*, Direzione-generale per la Strategia digitale, 15 dicembre 2020. Tale finalità, poi, ha trovato esplicita affermazione all'interno dello stesso DSA e, in particolare, nel considerando 9, il quale afferma: «Il presente regolamento armonizza pienamente le norme applicabili ai servizi intermediari nel mercato interno con l'obiettivo di garantire un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali sanciti dalla Carta siano efficacemente tutelati e l'innovazione sia agevolata, contrastando la diffusione di contenuti illegali online e i rischi per la società che la diffusione della disinformazione o di altri contenuti può generare». Per una più ampia lettura del DSA all'interno del contesto normativo europeo si veda, invece, F. Casolari, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza italiana*, 2, 2024, 462-465.

³ Sebbene il DSA trovi la propria base giuridica nell'art. 114 TFUE, esso presenta una caratteristica distintiva di particolare rilievo rispetto alla tradizionale disciplina concernente il mercato unico, ovvero la consapevolezza che le norme europee in materia di concorrenza, pur frequentemente impiegate nel contesto dello sviluppo tecnologico, non siano pienamente adeguate a contrastare la tendenza alla concentrazione nei mercati digitali; di conseguenza, il recente strumento normativo non si orienta verso una loro regolazione di tipo *ex-ante* cosa che, invece, accade nel caso del regolamento (UE) 2022/1925 del Parlamento e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali – DMA), ciò in quanto il DMA persegue una finalità distinta, mirando a regolamentare il funzionamento dei mercati digitali attraverso l'introduzione di una serie di obblighi specifici a carico delle imprese che svolgono un ruolo centrale nell'accesso al mercato. Sul punto cfr. G. Contaldi, *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, 2021, 292 ss.

⁴ Al riguardo, si segnalano in particolare i *Digital Services Coordinators* i quali aiutano la Commissione a monitorare e a far rispettare gli obblighi previsti dalle disposizioni sui servizi digitali. Nello specifico, essi sono responsabili della supervisione, dell'applicazione e del monitoraggio del DSA. Ciascuno Stato membro deve designare un coordinatore dei servizi digitali (DSC), responsabile di tutte le questioni relative all'applicazione e all'esecuzione della legge sui servizi digitali; cfr. art. 53 DSA. Per quel che concerne l'Italia, il Coordinatore è stato individuato nell'Autorità per le Garanzie nelle comunicazioni (AGCOM); sul punto, si veda S. Lavagnini, *DSA e coordinatori nazionali: il ruolo di Agcom in Italia*, in *agendadigitale.eu*, 11 novembre 2024; Osservatorio Data Protection, *DSA: AgCom appointed as Digital Services Coordinator with power to impose fines*, in *osservatorio-dataprotection.it*, 20 settembre 2023.

⁵ È opportuno sottolineare come il DSA applichi un regime di responsabilità alle piattaforme solo nel caso di mancata rimozione dei contenuti illegali dopo la pubblicazione *online*. Sul punto cfr. G. Cangiano, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in G. Cangiano - G. Contaldi - P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, 3 ss.

che operano nel mercato unico europeo⁶, indipendentemente dalla localizzazione della loro sede⁷. A ben vedere, però, il regolamento in questione introduce un sistema di obblighi differenziati, con le prescrizioni più rigorose che, nello specifico, trovano applicazione solo nei confronti delle cc.dd. *Very Large Online Platforms* (VLOPs) e dei *Very Large Online Search Engines* (VLOSEs)⁸. Il DSA, infatti, adotta un approccio regolatorio multilivello⁹, caratterizzato da un sistema di vincoli progressivi: a tutti i prestatori di servizi *online* sono imposti obblighi generali ai quali si aggiungono, poi, disposizioni sempre più stringenti, calibrate proporzionalmente in relazione alla tipologia dei servizi offerti¹⁰ e alla

⁶ Ai sensi dell'art. 2 DSA, il regolamento in esame si applica ai servizi intermediari offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari; esso, invece, non si applica ai servizi che non sono servizi intermediari né alle prescrizioni imposte in relazione a tali servizi, indipendentemente dal fatto che i servizi siano prestati facendo ricorso a servizi intermediari.

⁷ In dottrina si è sviluppata l'idea che la scelta di estendere l'ambito di applicazione territoriale del DSA sia giustificata dalla necessità di prevenire agevoli pratiche di elusione della stessa normativa. Non stupisce, quindi, che ai sensi dell'art. 13 DSA i prestatori di servizi intermediari che non sono stabiliti nell'Unione, ma che offrono servizi all'interno dell'UE, sono obbligati a designare per iscritto una persona fisica o giuridica che funga da loro rappresentante legale in uno degli Stati membri in cui offrono i propri servizi, incaricando quest'ultima di fungere da punto di riferimento, in loro aggiunta o sostituzione, seguendo sostanzialmente quanto già previsto dal GDPR.

⁸ Il DSA differenzia le piattaforme *online* in base alla dimensione e indica, al suo art. 33, come *Very Large Online Platforms* e *Very Large Online Search Engines* le piattaforme *online* e i motori di ricerca *online* che abbiano un numero mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni (ovvero il 10% della popolazione europea).

⁹ Come evidenziato dal Considerando (41), la distinzione tra le diverse categorie di prestatori di servizi *online* è ritenuta indispensabile per perseguire in maniera efficace gli obiettivi di interesse pubblico individuati dal regolamento.

¹⁰ Il DSA, all'art. 3 (al quale si rimanda), effettua una tripartizione dei servizi intermediari sottoposti alla sua disciplina: 1) servizio di "semplice trasporto" (detto anche di *mere conduit*), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio o nel fornire accesso a una rete di comunicazione; 2) servizio di "memorizzazione temporanea" (c.d. *caching*), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficiente il successivo inoltramento delle informazioni ad altri destinatari su loro richiesta; 3) servizio di "memorizzazione di informazioni" (c.d. *hosting*), consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta dello stesso. Sulla base di questa differenziazione il DSA individua poi: le "piattaforme online" quale servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del regolamento; i "motore di ricerca online", ovvero un servizio intermedio che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto.

dimensione delle piattaforme operanti sul *web*.

In tale rinnovato contesto, tra le previsioni di maggiore rilievo presenti nel Digital Services Act deve segnalarsi sicuramente l'art. 25, norma che vieta l'utilizzo di quelle interfacce ingannevoli o manipolative comunemente denominate *dark patterns*. Siffatto divieto, invero, inserito a seguito dei negoziati di trilogo¹¹, si affianca a quanto già sancito in materia dalla Direttiva sulle pratiche commerciali sleali (UCPD) e dal Regolamento Generale sulla Protezione dei Dati (GDPR)¹², andando così a completare la tutela degli internauti dai rischi connessi all'uso di *dark patterns* e, più in generale al rischio di scelte inconsapevoli¹³.

Tuttavia, all'intento meritorio sottostante all'art. 25 DSA fa attualmente da *pendant* una prassi applicativa¹⁴ portatrice di significative criticità. In

¹¹ L'inclusione nel DSA del divieto di utilizzo dei *dark patterns* è infatti frutto dell'adozione di un emendamento del Parlamento europeo presentato in prima lettura, cfr. Posizione del Parlamento europeo definita in prima lettura il 5 luglio 2022 in vista dell'adozione del regolamento (UE) 2022/... del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, EP-PE_TC1-COD(2020)0361.

¹² Rispettivamente direttiva 2005/29/CE del Parlamento europeo e del Consiglio dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (direttiva sulle pratiche commerciali sleali - UCPD) e regolamento (UE) 2016/679 (GDPR) del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR). Sul punto cfr. A. Afferni, *Dark pattern: cosa sono e il loro rapporto con il GDPR*, in *cybersecurity360.it*, 21 maggio 2020; BEUC, *Dark patterns and the EU consumer law acquis. Recommendations for better enforcement and reform*, 7 febbraio 2022. L'art. 25, par. 2, afferma che il divieto previsto dal par. 1 non si applica alle pratiche contemplate alla direttiva 2005/29/CE (UCPD)

¹³ A ben vedere, infatti, l'art. 25 DSA, in quanto garanzia trasversale, completa il mosaico di tutele previsto dal regolamento. L'articolo in questione, invero, si affianca agli obblighi di trasparenza (artt. 14-17 DSA) e alla disciplina sulla pubblicità (art. 26 DSA), nonché alle valutazioni di rischio sistemico (artt. 34-35 DSA), assumendo la funzione di norma di chiusura a salvaguardia dell'autonomia decisionale degli utenti. Calato in siffatto contesto, appare allora evidente come il divieto di *dark patterns* non rappresenti una disposizione isolata, bensì si configuri quale parte integrante della logica multilivello del DSA. Sul punto, *ex multis*, cfr. EPRS – European Parliamentary Research Service, *Regulating dark patterns in the EU: Towards digital fairness*, gennaio 2025.

¹⁴ Un caso emblematico in materia di applicazione del DSA e, più nello specifico, di divieto di *dark patterns* è rappresentato dalla vicenda *Temu*, il quale prende le mosse da un reclamo presentato dalle organizzazioni dei consumatori della rete *Bureau Européen des Unions de Consommateurs* (BEUC) ai loro competenti *Digital Services Coordinators*. Nello specifico, il BEUC nella sua doglianza esprimeva forti preoccupazioni nei confronti di *Temu*, ritenendo che tale *marketplace* non garantisse un ambiente *online* sicuro, prevedibile e affidabile. In particolare, venivano segnalate numerose pratiche grafiche manipolative adottate dalla piattaforma, con conseguente diffusione di informazioni ambigue e fuorvianti sui prodotti e sui relativi prezzi, nonché la presenza di elementi di *social shopping* e di forme di *rewards*. In ragione del suddetto reclamo, il 28 giugno 2024 la Commissione europea richiedeva a *Temu* di fornire informazioni sulle misure adottate per adempiere agli obblighi previsti dal DSA, in particolare riguardo: alla efficace predisposizione di un "meccanismo di segnalazione e azione"; alla protezione dei minori durante la navigazione sul proprio sito; alla trasparenza dei "sistemi di raccomandazione"; alla "tracciabilità degli

particolare, persiste tutt'oggi una grave incertezza sulla stessa definizione di *dark patterns* la quale, a sua volta, determina ulteriori dubbi circa il campo di applicazione oggettivo del relativo divieto e la conseguente esatta individuazione dei soggetti destinatari della norma.

Alla luce di un così complesso stato dell'arte, quindi, il presente contributo si propone di analizzare le principali questioni ermeneutiche scaturenti dal divieto di utilizzo di *dark patterns* presente nel DSA, offrendo alcune riflessioni critiche sul tema e delineando, poi, possibili soluzioni volte al superamento delle ambiguità ancora esistenti all'interno dell'ecosistema digitale.

2. Articolo 25 DSA, una norma già obsoleta?

Nonostante nel quadro giuridico europeo attuale i *dark patterns* siano espressamente vietati da diverse fonti normative¹⁵, in un suo recente studio la Commissione europea ha rilevato che il 97% dei siti web e delle app più popolari tra i consumatori dell'UE ne fa ancora uso¹⁶; un dato questo che permette di comprendere appieno la rilevanza di tale fenomeno, così come l'evidente difficoltà nel contrastarlo.

Al riguardo, il primo problema che emerge è di natura definitoria. Invero, con il termine *dark patterns*¹⁷ si è soliti indicare quelle tecniche di progettazione della c.d. *user interface*¹⁸ volte a manipolare le scelte degli utenti in modo ingannevole o non trasparente¹⁹. In particolare, si fa qui

operatori", ma soprattutto – per quanto qui interessa – alla predisposizione di interfacce *online* non ingannevoli o manipolative, quindi rispettose del divieto di *dark patterns*. Dopo una seconda richiesta formale, inviata l'11 ottobre 2024, valutate negativamente le informazioni così ottenute, il 31 ottobre 2024 la Commissione avviava un procedimento formale per valutare l'eventuale violazione da parte di *Temu* degli artt. 27, 34, 35, 38 e 40 DSA.

¹⁵ Come anticipato, un sostanziale divieto di *dark patterns* è presente nell'UPCD e nel GDPR, ma anche nella direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori, nella direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), nel DMA e nell'AI Act (su quest'ultimo *amplius infra*); cfr. European Parliament, *Regulating dark patterns in the EU: Towards digital fairness*, gennaio 2025.

¹⁶ Cfr. European Commission, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization – Final Report*, Bruxelles, 2022.

¹⁷ Nello specifico, il termine *dark pattern* è stato coniato, nel 2010, da Harry Brignull, founder of the Deceptive Patterns Initiative & Head of Innovation at Smart Pension. Interessante al riguardo è l'intervento fatto dallo stesso Brignull al Parlamento europeo, disponibile *online*.

¹⁸ L'interfaccia utente «è l'insieme di quegli elementi con i quali il cittadino interagisce per ottenere servizi digitali. Non si compone esclusivamente di elementi grafici o visuali, ma comprende tutto ciò con cui l'utente entra in relazione durante l'utilizzo di un servizio digitale», cfr. Agenzia per l'Italia Digitale, *Linee guida di design per i servizi digitali della PA*.

¹⁹ In tal senso cfr.: C. Sinderson, *Designing Against Dark Patterns, in The German Marshall Fund of the United States*, in gmfus.org, 12 luglio 2021; J. Luguri - L.J. Strahilevitz, *Shining a light*

riferimento a quegli strumenti informatici utilizzati dalle piattaforme *online* per indurre i propri utenti a compiere azioni che potrebbero non essere nel loro interesse; ciò avviene principalmente sfruttando le vulnerabilità psicologiche dei fruitori dei servizi *online*, limitando la loro capacità di prendere decisioni informate e, di conseguenza, causando agli utenti un pregiudizio²⁰ o rendendo loro più difficile il compimento di azioni sfavorevoli per il fornitore del servizio. Si tratta, quindi, di tecniche grafiche e di *web-design* che, sulla base di studi di scienza cognitiva e di abitudini del comportamento umano, mirano a sfruttare i cc.dd. *bias* cognitivi degli utenti per l'esclusivo profitto dell'azienda che offre il servizio.

Muovendo da tale definizione, le linee guida dello European Data Protection Board (EDPB)²¹ hanno individuato sei tipologie di “modelli di progettazione ingannevoli”, ovvero di *dark patterns*, quali: 1) l'*overloading*, cioè quando gli utenti si trovano di fronte ad un ingente numero di richieste, informazioni, opzioni e/o possibilità finalizzate a spingerli a condividere più dati personali possibili ed a consentirne involontariamente il loro trattamento; 2) lo *skipping*, ovvero quando le interfacce sono realizzate in modo tale che gli utenti dimentichino o non riflettano su aspetti legati alla protezione dei propri dati; 3) lo *stirring*, ovvero quando le scelte degli utenti sono influenzate facendo appello alle loro emozioni o usando sollecitazioni visive; 4) l'*hindering*, cioè quando gli utenti sono ostacolati o bloccati nel processo di informazione sull'uso dei propri dati o nella gestione di questi ultimi; 5) il *flickle*, ovvero quando gli utenti acconsentono al trattamento dei propri dati senza capire quali siano le finalità a causa di un'interfaccia incoerente o poco chiara; 6) il *leftinthedark*, cioè quando l'interfaccia è progettata in modo da nascondere agli utenti le informazioni e gli strumenti di controllo della *privacy*²².

Dal canto suo anche il DSA ha fatto propria tale impostazione, adottando una definizione di *dark patterns* – ed un conseguente divieto di loro utilizzo – incentrata principalmente sulla natura “grafica” di questi ultimi. Invero, sotto la rubrica “Progettazione e organizzazione dell'interfaccia online”, l'art. 25 DSA vieta ai fornitori di servizi in rete di «progettare, organizzare o gestire le loro interfacce online in modo da ingannare o manipolare i destinatari del loro servizio o in modo da falsare o compromettere in altro modo la capacità dei destinatari del servizio di prendere decisioni libere

on dark patterns, in *Journal of Legal Analysis*, 13, 2021, 43 ss.

²⁰ Il pregiudizio dell'utente si manifesta quando il suo giudizio o il suo processo decisionale si discosta in modo sistematico, e non causale, da un criterio di riferimento. Il criterio più comunemente adottato dagli studiosi è la c.d. teoria della scelta razionale. Quest'ultima, nell'ambito della sociologia, si occupa di analizzare e definire i principi che guidano un individuo, o che dovrebbero guidarlo, nello scegliere tra diverse opzioni quella più vantaggiosa per sé, sul punto cfr. J. S. Coleman, *Fondamenti di teoria sociale*, in *Collezione di testi e di studi*, Bologna, 2005 e G. Ballarino, *Teoria dell'azione sociale e sistematica sociologica*, in *Quaderni di Sociologia*, 38, 2005, 173 ss.

²¹ L'European Data Protection Board è un organismo indipendente dell'Unione europea, il cui scopo è garantire un'applicazione del Regolamento Generale sulla Protezione dei Dati Personali e promuovere la cooperazione tra le autorità di protezione dei dati dell'UE.

²² European Data Protection Board, *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*, 14 febbraio 2023.

e informate»²³. A ben vedere, però, questo approccio restrittivo trova sostanzialmente la propria *ratio* nel testo del più generico considerando 67 DSA, unico punto del regolamento (UE) 2022/2065 dove si faccia espresso riferimento ai *dark patterns* e quindi, di conseguenza, indispensabile per integrare la *littera legis* dell'art. 25 DSA. Ebbene, il citato considerando, dopo aver definito i *dark patterns* quali «pratiche che distorcono o compromettono in misura rilevante, intenzionalmente o di fatto²⁴, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate», vieta l'ingannare, il distorcere e il limitare l'autonomia, il processo decisionale e la scelta dei destinatari di un servizio digitale attraverso «la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa».

Non stupisce, dunque, che sovrapponendo il considerando 67 con quanto disposto dall'art. 25 DSA sia possibile individuare un elenco di *dark patterns* vietati di natura grafica o di *web-design*, ossia: attribuire maggiore rilevanza visiva ad una specifica opzione quando si chiede al destinatario di prendere una decisione²⁵; chiedere ripetutamente che l'utente effettui una scelta laddove questa sia già stata fatta, specialmente presentando “*pop-up*” che interferiscano con l'esperienza dell'utente²⁶; rendere la procedura di disdetta di un servizio più difficile della sottoscrizione dello stesso²⁷; rendere determinate scelte più difficili o dispendiose in termini di tempo rispetto ad altre²⁸; rendere irragionevolmente difficile l'interruzione degli acquisti o la disdetta da una determinata piattaforma *online*²⁹; predisporre impostazioni predefinite molto difficili da modificare³⁰.

Tuttavia, un divieto di *dark patterns* completamente appiattito sulla natura grafica di questi ultimi cela il rischio di una rapida obsolescenza della norma, incapace così di intercettare i nuovi strumenti informatici manipolativi già presenti in larga misura sui *marketplaces*; tendenza questa confermata anche dalla prassi, con la Commissione europea che preferisce contestare alle VLOP la violazione dell'art. 34 DSA piuttosto che dell'art.

²³ Da una analisi complessiva dell'art. 25 DSA è possibile affermare che esso persegue un triplice obiettivo: a) vietare l'utilizzo di *dark patterns*; b) proteggere l'autonomia dell'utente nel compiere scelte libere e autonome; c) agire come disposizione sussidiaria e complementare rispetto all'UCPD e al GDPR.

²⁴ Al riguardo in dottrina si è soliti distinguere “l'intenzionalità della strategia” di una piattaforma dal suo “impatto prevedibile”: nel primo caso l'utilizzo dei *dark patterns* per ingannare, manipolare o compromettere l'esperienza dell'utente avviene intenzionalmente da parte della piattaforma; nel secondo caso, invece, il fornitore di servizi digitali è consapevole solo di un potenziale impatto negativo sugli utenti in ragione dell'interfaccia utente impiegato. Sul punto, *amplius*, C. Santos - N. Bielova - S. Ahuja - C. Utz - C. M. Gray - G. Mertens, *Which Online Platforms and Dark Patterns Should be Regulated under Article 25 of the DSA?*, Digital Legal Talks 2024, 28 november 2024.

²⁵ Cfr. art. 25, par. 3, DSA.

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ Cfr. considerando 67 DSA.

²⁹ *Ibid.*

³⁰ *Ibid.*

25 DSA³¹. Eppure, tale scelta appare quantomeno discutibile visto che il dato normativo dell'art. 25 DSA – ed in particolare l'uso del verbo “compromettere” – è di per sé sufficiente a riconoscere alla norma in questione quella elasticità necessaria ad adattarsi ai continui mutamenti tipici delle innovazioni tecnologiche, uscendo dal limitato campo delle vesti grafiche. Del pari, non va poi dimenticato come sia lo stesso considerando 67 a riconoscere la non esaustività dell'elenco in esso contenuto³², aprendo così *de facto* a soluzioni ermeneutiche più inclusive.

3. Gli *Hyper-Engaging Dark Patterns*: maggiori rischi, tutele minori (e inique)

Come anticipato, a discapito della copiosa normativa europea esistente in materia, i *dark patterns* rappresentano tutt'oggi «a continuing, prominent and increasingly problematic characteristic of online life»³³. Questa scarsa capacità dissuasiva della legislazione europea è da ricondurre, secondo parte della dottrina, primariamente a carenze di tipo applicativo³⁴; se ciò non è certamente da escludere, appare tuttavia più corretto imputare primariamente l'attuale fallimento del divieto in questione alla “qualità” del quadro normativo. Quest'ultimo, invero, come è stato attentamente osservato, si è principalmente concentrato sulle caratteristiche “statiche”³⁵ dei *dark patterns* quando oggi, invece, le forme di manipolazioni online sono sempre più “dinamiche”, cioè derivanti dal trattamento dei dati degli utenti per personalizzarne le interfacce e, di conseguenza, condizionarne i comportamenti³⁶.

Muovendo proprio da siffatti presupposti, in ragione soprattutto del

³¹ Si fa qui riferimento, da ultimo, al già menzionato caso *Temu* dove la Commissione non ha contestato alla VLDP cinese – pur potendolo fare - l'art. 25 DSA.

³² Cfr. considerando 67, par 1.

³³ Cfr. T. Akhurst - L. Zurdo - R. Rapparini - C.M. Markhof, *How should the European Union regulate dark patterns?*, in *SciencesPO Chair Digital, Governance and Sovereignty*, Parigi, 2023, 4.

³⁴ Cfr. F. Esposito - T. M. C. Ferreira, *Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns*, in *European Journal of Risk Regulation*, 2024, 1 ss., secondo i quali sarebbe necessaria la creazione di un complesso sistema istituzionale incentrato sul Coordinatore dei servizi digitali – con poteri di indagine autonomi integrati dall'intervento delle parti interessate ai sensi dell'art. 40 DSA – e poteri sanzionatori diretti, anche alla luce della recente bozza di regolamento delegato, cfr. Commission Delegated Regulation (EU) .../... supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data pursuant to Article 40 of Regulation (EU) 2022/2065.

³⁵ Per caratteristiche “statiche” si intendendo, solitamente, gli aspetti dell'interfaccia facilmente osservabili e non personalizzati per gli utenti.

³⁶ K. Yeung, *Hyper-nudge: Big Data as a Mode of Regulation by Design*, in *Information, Communication & Society*, 20(1), 2016, 118 ss. In modo simile, alcuni sostengono che l'UE abbia bisogno di una regolamentazione aggiuntiva più adatta all'era digitale cfr. BEUC, *Dark patterns and the EU consumer law acquis. Recommendations for better enforcement and reform*, cit., 11 ss.

quadro tecnologico attuale, risulta quanto mai indispensabile ampliare il concetto di *dark patterns* (ed il conseguente divieto), ai cc.dd. *Hyper Engaging Dark Patterns* (HEDP)³⁷. Orbene, questa particolare fattispecie di strumenti informatici rappresenta una categoria avanzata di pratiche manipolative, capace di sfruttare al massimo l'interazione con l'utente. Ciò avviene, ad esempio, attraverso i cc.dd. algoritmi adattivi³⁸, i quali analizzano i dati degli utenti e formulano previsioni sul loro comportamento futuro, adeguando così i contenuti mostrati e il *design* delle piattaforme in base alle interazioni precedenti. Tuttavia, se le interfacce personalizzate erano già conosciute dai *dark patterns* "di prima generazione", sono la eterogeneità e la frequenza degli stimoli volti a catturare l'attenzione dell'utilizzatore a caratterizzare ontologicamente gli HEDP. Rientrano, infatti, in tale categoria i *pop-up*³⁹, le notifiche *push*⁴⁰, i *like*, le *emoji*, la *gamification*⁴¹, il c.d. *scroll* infinito⁴², l'*autoplay*⁴³, il numero di visualizzazioni dei propri contenuti, le storie che scompaiono dopo un breve periodo di tempo, i programmi di *rewards*⁴⁴; una varietà fenomenologica questa pensata appositamente per prolungare il tempo di utilizzo dei *social networks* e dei *marketplaces*, incentivando azioni inizialmente non volute (come acquisti non pianificati⁴⁵), ma soprattutto –

³⁷ Definiti anche: *darkest patterns*, *deceptive patterns* o *deception by design*.

³⁸ Gli algoritmi adattivi sono algoritmi progettati per modificare il loro comportamento in base ai dati ricevuti o alle condizioni del contesto in cui operano. A differenza degli algoritmi tradizionali, che seguono una sequenza di istruzioni fisse, gli algoritmi adattivi sono dinamici: si adattano e aggiornano le proprie regole o parametri in tempo reale in risposta a nuove informazioni, *feedback* degli utenti o mutamenti dell'ambiente. L'obiettivo di questi ultimi è creare nell'utente un senso di ricompensa per aumentare il c.d. rinforzo comportamentale e influenzare le sue scelte future. Questo ha reso necessario inserire anche nel regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828, noto come AI Act, un riferimento ai *dark patterns*; cfr. combinato disposto considerando 28, considerando 29 e art. 5, par. 1, lett. a) AI Act.

³⁹ In informatica, con il termine *pop-up*, si intendono elementi dell'interfaccia grafica che appaiono automaticamente durante l'uso dei dispositivi al fine di attirare l'attenzione dell'utente.

⁴⁰ Con il termine *notifica push* si intende il breve messaggio che appare come *pop-up* sui *device* digitali o nel centro notifiche dei dispositivi *mobile*.

⁴¹ Per *gamification* si intende l'utilizzo di attività ludiche per favorire il coinvolgimento emotivo dell'utente. Questa pratica è stata già sanzionata negli USA cfr. N. Gallo, *Robinhood and the Gamification of Investing*, in *finmasters.com*, 21 febbraio 2022.

⁴² Con il termine *inifinite scrolling* si intende lo scorrimento ossessivo dei contenuti *online*; tale attività prende il nome dallo scorrere delle dita sui *touch screen* dei *device* effettuato per permettere un continuo caricamento dei contenuti (c.d. *refresh*) delle pagine *web*.

⁴³ Per *autoplay* si intende l'impostazione che permette la riproduzione automatica di un video al momento dell'accesso su una pagina *web*.

⁴⁴ Con programma di *reward* si intende, in generale, una strategia di *marketing* pensata per incoraggiare i clienti a continuare ad acquistare beni e/o servizi dall'azienda promotrice grazie a premi accumulati durante/con l'utilizzo della piattaforma.

⁴⁵ Sul punto si veda M. Leiser - C. Santos, *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface*, in *European Journal of Law and Technology*, 15, 2024.

cosa più preoccupante – coinvolgendo emotivamente e psicologicamente l'utente fino a generare vere e proprie forme di dipendenza dal servizio e/o dalla piattaforma.

Gli HEDP rappresentano, quindi, un'evoluzione più pericolosa dei "classici" *dark patterns* precedentemente descritti i quali, come facilmente deducibile, per i loro potenziali effetti negativi impongono nuove sfide⁴⁶, soprattutto nel campo normativo. Invero, come anticipato, l'attuale interpretazione restrittiva dell'art. 25 DSA esclude gli HEDP dal suo campo di applicazione, rischiando così di lasciare l'utilizzatore del servizio *online* privo di tutele. Per provare ad ovviare a tale pericolo, la prassi applica in queste circostanze gli artt. 34 e 35 DSA⁴⁷ che impongono ai fornitori di servizi di valutare e mitigare «i rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi»⁴⁸. Nello specifico, si tratta di una scelta applicativa avviene facendo leva sul considerando 83 DSA, il quale afferma che tra i rischi sistemici che devono essere valutati dai fornitori di servizi *online* rientrano anche «i rischi relativi alla progettazione di interfacce online che possono stimolare le dipendenze comportamentali dei destinatari del servizio».

Orbene, tre almeno le criticità derivanti da tale opzione ermeneutica. In primo luogo, alla luce del dato normativo del considerando 83, sembra essere forzata una sua interpretazione che contenga al proprio interno tutte le forme di HEDP in precedenza descritte; se, invero, non emergono particolari problemi nel ricondurre nell'alveo della norma in questione l'utilizzo di algoritmi adattativi, meno consequenziale appare invece l'accostamento del considerando 83 ai programmi di *rewards*, i quali certamente non attengono alla progettazione delle interfacce. In secondo luogo, poi, diverso è il tenore letterale degli artt. 25 e 34 DSA; se, infatti, si facessero confluire nel primo articolo menzionato anche gli HEDP si sarebbe alla presenza di un loro totale divieto, mentre oggi, applicando in tali casi gli artt. 34 e 35 DSA si invitano i fornitori di servizi online esclusivamente ad «individuare, analizzare, valutare»⁴⁹ i rischi esistenti e, di conseguenza, «adottare misure di attenuazione»⁵⁰. Infine, la criticità più grave attiene certamente al campo applicativo soggettivo di tale scelta. Dalla lettura combinata del considerando 83 e degli artt. 34 e 35 DSA emerge, difatti, come il legislatore europeo abbia chiaramente deciso di limitare l'approfondita valutazione del rischio alle sole VLOPs, lasciando

⁴⁶ Al riguardo si veda C. M. Gray - C. Santos - N. Bielova - T. Mildner, *An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action*, CHI'24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, 2024

⁴⁷ Sul punto, cfr. *Atti del convegno "Regole europee di trasparenza e responsabilità per le piattaforme online: sfide e prospettive" – Convegno conclusivo PRIN 2022 "Towards Stricter Rules on Transparency and Liability for Online Platforms in the European Digital Single Market"*, intervento Prof. S. Pugliese, *Protezione degli utenti, interessi delle imprese ed empowerment del settore pubblico nella disciplina europea dei servizi digitali*.

⁴⁸ Art. 34, par. 1, DSA.

⁴⁹ *Ibid.*

⁵⁰ Art. 35, par. 1, DSA.

invece sostanzialmente un ampio margine di manovra alle piattaforme più piccole con conseguenti minori tutele per i loro utenti. Al contrario, ciò non accadrebbe qualora si estendesse l'interpretazione dell'art. 25 DSA anche agli HEDP poiché tale divieto si applica uniformemente a tutti i fornitori di servizi *online*. D'altronde, siffatta disparità di trattamento appare *ex se* irragionevole visto che: un'interpretazione "estensiva" del divieto posto dall'art. 25 DSA – come anticipato – sarebbe conforme alla *littera legis* di tale articolo; l'applicazione della norma in questione non comporterebbe maggiori costi per le non-VLOPs; i rischi per gli utenti conseguenti all'uso di HEDP non vedono la propria gravità mutare in ragione della grandezza della piattaforma che li utilizza.

4. Conclusioni

Operando nella zona grigia tra le tecniche legittime di *design Platform* e i metodi illegittimi per influenzare il comportamento degli utenti, la presenza dei *dark patterns* nell'architettura delle piattaforme *online* è divenuta nel tempo sempre più presente e l'intento manipolativo manifestato dai fornitori di servizi digitali si è elevato dal livello del processo decisionale individuale al livello superiore, quello di natura collettiva. In ragione di tali caratteristiche, allora, è ben comprensibile che parte della dottrina si sia spinta a considerare i *dark patterns* quali «a serious and pervasive threat to core liberal democratic principles»⁵¹.

Conscio dei pericoli insiti ontologicamente nell'uso di tali strumenti informatici, il legislatore europeo ha deciso quindi di tutelare giuridicamente i fruitori dei servizi *online* contro i *dark patterns*, inserendo all'interno del Regolamento (UE) 2022/2065 – più specificamente all'interno del suo art. 25 – un esplicito divieto. Nonostante ciò, come rapidamente illustrato, al riguardo sussistono ancora numerose perplessità.

In primo luogo, l'interpretazione attualmente consolidata sul divieto sancito dall'art. 25 DSA, appare irragionevolmente circoscritta all'impiego dei *dark patterns* nel solo ambito del *design* delle interfacce delle piattaforme *online*. Questa applicazione restrittiva dell'articolo in questione solleva preoccupazioni di natura tanto teorica quanto pratica. Da un lato, infatti, si sta creando un ingiustificato *gap* tra dato normativo dell'art. 25 DSA e prassi della Commissione europea, con la conseguente mancata corrispondenza tra obiettivo dichiarato del regolamento (ovvero contrastare in modo efficace le pratiche ingannevoli) e sua concreta applicazione; dall'altro, si rischia di lasciare così un ampio margine di azione alle tecniche manipolative più sofisticate, le quali sfruttano non tanto il *design* visivo, quanto il funzionamento psicologico e comportamentale degli utenti; conseguenze queste che potrebbe essere facilmente evitate dato che il testo del primo paragrafo dell'art 25 DSA risulta di per sé adatto ad estendere il divieto in esso contenuto anche agli HEDP.

D'altronde, la scelta – perpetrata dalla Commissione – di inserire gli *Hyper-*

⁵¹ Cfr. T. Akhurst - L. Zurdo - R. Rapparini - C.M. Markhof, *How should the European Union regulate dark patterns?*, in *SciencesPO Chair Digital, Governance and Sovereignty*, Parigi, 2023, 4.

Engaging Dark Patterns nel più ampio contesto della valutazione del rischio (secondo il combinato disposto del considerando 83 e degli artt. 34 e 35 DSA) porta con sé quella che potrebbe essere considerata la principale criticità del sistema, ovvero la disparità di trattamento tra VLOPs e piattaforme di minori dimensioni. Queste ultime, infatti, sebbene soggette al Digital Services Act, non sono obbligate a effettuare una vera e propria valutazione del rischio, né a implementare misure di mitigazione come nel caso delle VLOPs.

Ampliare l'interpretazione dell'art. 25 DSA – *rectius* riconoscerne la sua vera portata – significherebbe, allora, imporre a tutte le piattaforme un divieto effettivo di ogni forma di *dark patterns*, eliminando così quel divario applicativo che indebolisce la capacità regolativa del DSA e pone in discussione la sua stessa efficacia come strumento di tutela dell'ecosistema digitale.

Del pari, una ulteriore soluzione potrebbe consistere nell'imporre anche alle piattaforme *online* di “piccole dimensioni” l'obbligo di redigere una valutazione del rischio. Tale misura contribuirebbe certamente a limitare gli spazi per lo sviluppo e l'adozione di strumenti informatici che sfruttano al massimo l'interazione dell'utente per arrecargli un danno (primi fra tutti i meccanismi di *rewards* e la *gamification*) ma, allo stesso tempo, andrebbe ad inficiare l'intero impianto del DSA, volto a lasciare alla *rule of reason* e al *private enforcement* il “sottobosco” digitale, concentrando invece il proprio controllo sugli operatori i cui comportamenti possono essere veramente dannosi in ragione dell'impatto sistemico che rischiano di sortire.

Abstract

L'art. 25 del Digital Services Act (DSA) vieta l'utilizzo e la diffusione sulle piattaforme online dei cc.dd. dark patterns, ossia di quegli strumenti informatici progettati per influenzare il comportamento degli utenti durante la loro esperienza nel web. L'interpretazione prevalente in dottrina riguardo tale divieto – come confermato anche dalla prassi della Commissione UE – appare, tuttavia, irragionevolmente restrittiva, limitandone la vigenza esclusivamente alla categoria dei dark patterns di natura grafica. Invero, siffatta operazione ermeneutica porta con sé il rischio di creare un vuoto di tutela in relazione alle nuove generazioni di dark patterns e, più nello specifico, rispetto agli *Hyper-Engaging Dark Patterns* (HEDP), progettati non solo per massimizzare l'interazione con gli utenti ma, soprattutto, per spingere questi ultimi a compiere azioni da loro non intenzionalmente volute (come, ad esempio, effettuare acquisti non programmati). Alla luce di tale stato dell'arte, il presente lavoro propone un superamento dell'odierno approccio maggioritario il quale, tra le altre cose, crea una forte differenziazione di tutele tra utenti delle *Very Large Online Platforms* (VLOPs) e utenti delle non-VLOPs.

Art. 25 of the Digital Services Act (DSA) proscribes the use and dissemination of so-called dark patterns on online platforms. The term “dark patterns” refers to computer tools designed to influence users’ behaviour during their web experience. The prevailing interpretation in scholarship concerning this prohibition, also confirmed by the practice of the EU Commission, appears, however, to be unreasonably restrictive, limiting its validity exclusively to the category of dark patterns of a graphic nature. This approach carries the risk of creating a protection gap concerning new generations of dark patterns, particularly Hyper-Engaging Dark Patterns (HEDP), which are designed not only to maximise interaction with users but also to compel them to perform unintended actions (e.g. making unplanned purchases). In the light of this scenario, this paper proposes moving away from the prevailing majority approach, which, among other issues, creates a marked differentiation in protections between users of Very Large Online Platforms (VLOPs) and those of non-VLOPs.

Keywords

divieto – dark patterns – Digital Service Act – HEDP – VLOPs