UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

Dark Pattern e Diritto Digitale: Manipolazione online e tutela del consumatore nell'economia dell'attenzione.

Alessio Camporeale
0366954

Anno accademico 2024/2025

Abstract

Questa tesina mira ad analizzare il fenomeno delle pratiche commerciali business-to-consumer (B2C) nell'ambiente digitale che negli ultimi anni hanno sollevato preoccupazioni in materia di equità, in particolare ci concentreremo sul fenomeno dei *dark pattern*, ovvero tecniche ingannevoli di progettazione delle interfacce digitali che condizionano ingannevolmente e occultamente le scelte degli utenti online, spesso riducendo la loro consapevolezza e limitando la libertà decisionale. In un contesto in cui piattaforme e servizi digitali impiegano sistematicamente questi schemi per amplificare l'engagement degli utenti *(personalizzazione manipolativa)* e le conversioni commerciali dei consumatori, i dark pattern negli ultimi anni sono stati sempre più centrali nel dibattito giuridico per la tutela dei diritti digitali e della protezione dei consumatori.
La ricerca si concentra sull'origine e sull'evoluzione delle principali tipologie di dark pattern e ne esamina gli effetti concreti sulla tutela dei consumatori e sui diritti fondamentali, come il diritto alla privacy e la libertà contrattuale. Particolare attenzione è dedicata al quadro normativo vigente in Italia ed Europa: dal Codice del Consumo e dal Regolamento Generale sulla Protezione dei Dati (GDPR), fino ai più recenti interventi europei con il Digital Services Act (DSA) e l'Artificial Intelligence Act (AI Act), che impongono nuovi vincoli di trasparenza e vietano esplicitamente l'uso di interfacce manipolative.

Attraverso l'analisi di due casi concreti, la seguente tesi evidenzia come l'utilizzo di dark pattern incida direttamente sull'individuo e sui suoi diritti, ostacolandone la capacità di compiere scelte consapevoli e di esercitare pienamente le proprie libertà digitali.

Si riflette infine sulle sfide future per il diritto digitale: il rafforzamento degli strumenti di enforcement, l'adozione di soluzioni tecnologiche per rilevare i dark pattern e la promozione di una cultura della trasparenza e del design etico, elementi imprescindibili per garantire un ambiente digitale più equo e rispettoso dei diritti degli utenti.

Sommario

CAPITOLO 1: FONDAMENTI E ORIGINE DEI DARK PATTERN

Nell'era attuale della trasformazione digitale, l'economia dei dati è diventata una fonte importante del benessere dei consumatori. Con l'avvento dello shopping online, infatti, i consumatori possono confrontare i prezzi più facilmente e sono in grado di prendere decisioni di acquisto più consapevoli in qualsiasi momento della giornata.
I dati più recenti di Eurostat mostrano come la percentuale di utenti Internet che hanno acquistato o ordinato beni/servizi per uso privato sia aumentata dal 54% al 81% nel decennio 2009-2019 [1]. Questa tendenza in crescita sta avvantaggiando le piattaforme online e i commercianti sia in termini di ricavi economici che per l'accumulo costante di dati che consente loro di apprendere le preferenze dei consumatori e di adattare di conseguenza la messa in vendita dei propri prodotti o servizi.
La crescente disponibilità di dati ha permesso ai commercianti online di mettere a punto una vasta gamma di pratiche persuasive basate sul tracciamento e la profilazione dei comportamenti dei consumatori. Oggi si raccolgono dati su siti visitati, prodotti cercati, frequenza di acquisti, ma anche su caratteristiche socio-demografiche.

Sebbene la personalizzazione e le tecniche persuasive non siano nuove e vengano applicate da tempo anche nei negozi fisici, la trasformazione digitale ne ha ampliato la portata come mai prima d'ora. Queste pratiche, pur non essendo sempre illegali o scorrette, comportano rischi: alcuni operatori le usano per creare sollecitazioni artificiose capaci di influenzare i consumatori verso decisioni d'acquisto contrarie ai loro interessi. Un rischio chiave in questo ambito è che tali pratiche operino in un'area grigia tra tentativi legittimi di persuasione e tecniche di manipolazione illecite, sfruttando la vulnerabilità dei consumatori.
Diventa quindi necessario interrogarsi sulla capacità del quadro normativo europeo di tutelare efficacemente i consumatori in questo scenario, dove il confine tra persuasione legittima e manipolazione illecita si fa sempre più sottile.
I ***dark pattern*** o *deceptive patterns*, sono tecniche di progettazione digitale di interfacce che spingono, ingannano, costringono o manipolano i consumatori a compiere scelte che spesso non sono nel loro interesse, indirizzandoli invece verso comportamenti che avvantaggiano l'operatore di servizio (ad esempio l'acquisto di un prodotto, la sottoscrizione di un abbonamento, la condivisione involontaria di dati personali o la permanenza prolungata su una piattaforma). Tra le pratiche più comuni rientrano anche fenomeni scorretti di *cross-selling* e *up-selling*, in cui l'utente viene indotto a selezionare opzioni aggiuntive o versioni superiori di un prodotto o servizio attraverso tecniche visive o informative fuorvianti.
Questi schemi sfruttano meccanismi cognitivi e psicologici ben documentati, come il *nudging* (dall'inglese "*nudge*" ossia "influenza leggera"), le euristiche decisionali e i bias comportamentali, ma lo fanno in modo non trasparente e spesso contrario agli interessi dell'utente. Contrariamente a un design etico, volto a semplificare l'esperienza digitale e a favorire decisioni informate, i dark pattern creano ostacoli, confondono l'interazione, distorcono la percezione delle opzioni disponibili

e nascondono informazioni rilevanti. Da almeno vent'anni, i progettisti di artefatti digitali integrano conoscenze per aumentare la capacità di questi strumenti di catturare le emozioni dei consumatori e ridurre il pensiero critico libero. Il design delle interfacce modella le *affordances*[1] che guidano il *persuasive computing*[2]. Tutte queste tecniche design-psicologiche mirano a gestire le emozioni dei consumatori inducendoli ad entrare in uno stato di *flow*, ovvero uno stato mentale di completo coinvolgimento e concentrazione in un'attività. [2]

In tali ambienti, la linea tra persuasione legittima e manipolazione ingannevole risulta spesso sottile, sollevando interrogativi etici e giuridici che investono il diritto digitale contemporaneo. Questi schemi violano infatti sia la privacy informativa, ovvero il controllo su chi può accedere alle informazioni personali e in che misura, sia la privacy decisionale, cioè il diritto dell'individuo a proteggere le proprie decisioni e azioni da accessi o interferenze indesiderate che minacciano la libertà contrattuale [3].

1.1 Definizione e origine del fenomeno

Il concetto di *dark pattern* nasce formalmente nel 2010, grazie al lavoro del designer britannico Harry Brignull, che per primo coniò il termine per descrivere l'uso di interfacce digitali concepite intenzionalmente per fuorviare l'utente. Sul sito *www.darkpatterns.org* (oggi divenuto *www.eceptive.design*), Brignull iniziò a raccogliere esempi concreti di queste pratiche, denunciandone la diffusione crescente nei siti web e nelle app più popolari. [4]

Tuttavia, le radici culturali e scientifiche del fenomeno sono più profonde. Già negli anni '70 e '80, la psicologia cognitiva e comportamentale aveva messo in luce la vulnerabilità della mente umana di fronte a certe tecniche persuasive, descrivendo i bias decisionali e l'influenza delle tecniche persuasive sul comportamento umano. Successivamente, con la diffusione del *behavioral economics*[3], autori come Richard Thaler e Cass Sunstein nel 2007 avevano proposto il concetto di *nudge,* inizialmente con una accezione più assoluta: interventi progettuali che, senza vietare opzioni, guidano le decisioni degli utenti. [5]

Nel contesto digitale più recente, tuttavia, questo approccio è stato spesso stravolto: molte aziende hanno iniziato ad adottare tecniche persuasive non per aiutare l'utente, ma per servirsi della sua vulnerabilità spingendolo verso comportamenti vantaggiosi per l'operatore economico. Con l'evoluzione del web 2.0, l'esplosione dell'e-commerce e l'ascesa delle piattaforme sociali, il design delle interfacce ha assunto un ruolo strategico per l'acquisizione e la fidelizzazione degli utenti. Le logiche di *conversion rate optimization* (ottimizzazione del tasso di conversione) e *growth hacking*

[1] In design, sono le possibilità d'uso che un'interfaccia suggerisce in modo implicito.
[2] Uso delle tecnologie per persuadere l'utente a compiere certe azioni.
[3] Disciplina che studia come i fattori psicologici e cognitivi influenzano le decisioni economiche delle persone.

(rapida crescita di un business trovando "scorciatoie") hanno portato a una proliferazione di pratiche di manipolazione comportamentale sempre più sofisticate.

Nel decennio successivo all'introduzione del termine, il concetto di dark pattern ha rapidamente guadagnato attenzione accademica e giuridica, divenendo oggetto di studi da parte di esperti di diritto digitale, psicologi comportamentali e autorità di regolazione. Oggi, con il moltiplicarsi dei servizi digitali e l'espansione dell'economia dell'attenzione, la lotta contro l'uso distorto delle tecniche persuasive rappresenta uno dei principali terreni di confronto per il diritto europeo e internazionale.

1.2 Varianti principali dei dark pattern

Negli ultimi anni, la ricerca accademica e i lavori della Commissione Europea hanno contribuito a sistematizzare il fenomeno dei dark pattern, elaborando tassonomie utili per l'analisi giuridica e per l'intervento normativo. Una delle classificazioni più autorevoli è quella proposta nello studio *Behavioural Study on Unfair Commercial Practices in the Digital Environment* (European Commission, 2022), che suddivide i dark pattern in sei macro-categorie basate sugli effetti che producono sul comportamento degli utenti. [6]

- **Nagging:** Comprende tutti i messaggi ripetitivi e insistenti che interrompono l'esperienza utente per spingerlo a compiere una determinata azione, come ad esempio accettare notifiche push, autorizzare la geolocalizzazione o sottoscrivere un abbonamento. La continua pressione psicologica limita la possibilità di compiere scelte serene e ponderate.

- **Obstruction:** Tecniche che introducono ostacoli artificiali, aumentando tempo e complessità per dissuadere l'utente dal completare un'azione, spesso legata alla protezione dei propri diritti (cancellazione di un account, revoca del consenso, disdetta di un abbonamento). È una delle forme più subdole di alterazione dell'autodeterminazione contrattuale.

- **Sneaking:** Includono la pratica di nascondere informazioni rilevanti (costi aggiuntivi, condizioni contrattuali), oppure aggiungere prodotti o servizi al carrello senza il pieno consenso. Questi meccanismi alterano la trasparenza della transazione, compromettendo il principio della decisione informata.

- **Interface interference:** Manipolazioni visive o strutturali che orientano l'utente verso scelte più vantaggiose per il fornitore: pulsanti con design ingannevole, opzioni pre-selezionate, scelte cromatiche che occultano determinate opzioni. Si tratta di vere e proprie "architetture della scelta" progettate per favorire scelte non pienamente libere.

- **Forced action:** Richiedere all'utente di compiere azioni non strettamente necessarie o non collegate all'uso del servizio, al fine di proseguire nella navigazione o accedere a contenuti:

ad esempio obbligarlo ad accettare trattamenti di dati non essenziali per l'erogazione del servizio.

- **Social proof & scarcity:** Tecniche che fanno leva su pressioni sociali o senso di urgenza artificiale: messaggi che indicano quante persone stanno guardando lo stesso prodotto, o che il numero di articoli disponibili sta rapidamente diminuendo. Tali meccanismi inducono decisioni affrettate, sfruttando i bias cognitivi legati al comportamento sociale e alla scarsità percepita.

1.3 Settori di maggiore diffusione e impatti sui consumatori

L'impiego dei dark pattern è oggi una prassi largamente diffusa in numerosi ambiti dell'economia digitale. Le evidenze raccolte da diversi studi dimostrano come queste pratiche siano ormai integrate nelle strategie di design e marketing di molte piattaforme online. Secondo i dati pubblicati da *Mathur et al. (2019)* [7], su un campione di circa 11.000 siti e-commerce, il 95% di questi impiega almeno una forma di dark pattern. Analogamente, lo studio della **Commissione Europea** precedentemente citato [6] rileva che il 97% dei principali siti di vendita online nell'UE incorpora pratiche di design manipolativo in almeno una fase del percorso utente.

1.3.1 Evoluzione del fenomeno e trend recenti

Le evidenze suggeriscono che il fenomeno sia cresciuto fino a divenire quasi ubiquo negli ultimi anni. I dati comparativi mostrano chiaramente questa tendenza: dal 2018 ad oggi la percentuale di servizi online che impiegano tali pratiche è aumentata nettamente: uno studio nel 2019 su oltre 11.000 siti di shopping online ha rilevato dark pattern in circa 11% di questi: sono state identificate ben 1.818 istanze di dark pattern, con pratiche come countdown di offerte a tempo, messaggi di scarsa disponibilità prodotto e opzioni preselezionate per servizi aggiuntivi. [8]
Tuttavia, l'evoluzione non è uniforme: in alcuni settori specifici ci sono stati segnali di miglioramento a seguito di interventi normativi, come i casi studio che verranno illustrati nel capitolo 3 della tesi.
Un recente sweep internazionale (ICPEN 2024) non ha riscontrato differenze significative tra aree geografiche: siti di aziende UE e extra-UE, così come versioni web e mobile, mostrano percentuali di adozione di dark pattern comparabili. Ciò suggerisce che la *"cultura del design manipolativo"* è diventata endemica a livello globale nell'economia digitale. [6]

1.3.2 Studi sperimentali sull'efficacia manipolativa dei dark pattern

Molte ricerche sperimentali condotte tramite A/B test, survey comportamentali ed anche eye-tracking, confermano che i dark pattern raggiungono gli effetti voluti influenzando le decisioni degli utenti, spesso senza che questi ne siano pienamente consapevoli. Uno studio condotto da Luguri e Strahilevitz pubblicato nel 2021 ha fornito una delle prime dimostrazioni quantificabili. In un esperimento, ai partecipanti veniva proposto l'acquisto di un finto servizio; il primo gruppo aveva opzioni neutre ("Accetta" o "No, grazie"), mentre al secondo gruppo venivano presentate schermate manipolative (es. "Accetta e continua (consigliato)" contro un vago "Altre opzioni", seguito da messaggi di *confirmshaming*, ossia una tecnica manipolativa per spingere l'utente ad accettare qualcosa facendolo sentire in colpa se sceglie di rifiutare (in questo caso "Non voglio proteggere i miei dati" da cliccare per rifiutare). Il risultato è che solo l'**11%** del primo gruppo aderiva all'offerta, contro il **25%** del secondo gruppo esposto a due schermate ingannevoli. [9]
L'aggiunta di ulteriori popup aggressivi faceva salire le adesioni fino al **37–40%**. In pratica, poche manipolazioni hanno più che raddoppiato il numero di utenti che si sono iscritti a un servizio indesiderato. Lo studio ha inoltre osservato che gli utenti "manipolati" del secondo gruppo non si sentivano significativamente più infastiditi di quelli del primo gruppo, ovvero molti non si rendevano conto di aver subito un raggiro. Dall'etnografia digitale emerge che la consapevolezza più alta è tra esperti di UX, policy maker, accademici e attivisti consumeristi. Gli utenti comuni, senza formazione sul tema, faticano a riconoscere i dark pattern e li considerano comunque una parte "normale" dell'esperienza online e si sentono costretti ad accettarli pur di accedere ai servizi.

1.3.3 Danni sul consumatore

Vengono riconosciuti tre tipi di danno associati all'uso dei dark pattern nelle interfacce digitali:

- **Danno all'autonomia del consumatore**: riduce la capacità del consumatore di valutare consapevolmente le scelte proposte;
- **Danni Personali:** perdite finanziarie (dovute a costi nascosti, preselezioni ingannevoli, …), lesione della privacy (causata da impostazioni predefinite invasive o procedure complicate per negare il consenso al trattamento dei dati), danno psicologico e perdita di tempo (senso di frustrazione, inganno e fatica cognitiva);
- **Danni Strutturali:** distorsione della concorrenza (ostacolo del confronto tra offerte e alterazione del mercato); perdita di fiducia (i consumatori, sentendosi manipolati, riducono il loro coinvolgimento nelle attività online).

In merito al secondo punto, 8,5 milioni di consumatori britannici hanno riferito di aver speso soldi in acquisti non voluti o poi rimpianti a causa di interfacce ingannevoli sulla piattaforma SHEIN, per un totale stimato di 2,1 miliardi di sterline spesi in 12 mesi di cui avrebbero fatto a meno. [10] In media ogni persona ha subito un danno di £276 in un anno per acquisti indesiderati indotti dal design della piattaforma. Il sondaggio ha identificato i meccanismi più comuni dietro questi pentimenti: il 27% ha acquistato il prodotto sbagliato a causa di informazioni fuorvianti, il 25% ha comprato qualcosa perché inizialmente sembrava più economico (poi comparsi costi nascosti), il 22% si è

sentito pressato dall'urgenza artificiale ("disponibilità limitata") e il 21% è stato spinto da timer con conto alla rovescia a concludere un acquisto affrettato.
Per quel che concerne invece il terzo punto, è stato evidenziato che un eccesso di dark pattern possa minare la fiducia: una ricerca sulle prenotazioni alberghiere ha trovato che un alto numero di stratagemmi ingannevoli riduce la fiducia del consumatore nel sito e la propensione a prenotare, talvolta spingendolo a rinviare l'acquisto. Ciò suggerisce che esiste un equilibrio delicato: i dark pattern aumentano le conversioni nell'immediato, ma a livelli estremi possono intaccare la reputazione e la *user experience* al punto da allontanare parte degli utenti. [11]

CAPITOLO 2: LEGISLAZIONE, REGOLAMENTAZIONE E TUTELE CONTRO I DARK PATTERN

Negli ultimi anni, la crescente diffusione di interfacce manipolative e pratiche di design ingannevole hanno spinto i garanti e le autorità di controllo a rafforzare il quadro normativo volto a proteggere i consumatori nell'ambiente digitale. Sebbene il termine *dark pattern* non sia ancora formalmente presente in molte norme, le condotte grafiche manipolatorie sono oggi espressamente riconosciute come pratiche scorrette o illegittime in diversi ambiti giuridici. In Italia, la disciplina rilevante si articola tra le previsioni del Codice del Consumo e gli obblighi imposti dal GDPR in tema di consenso e trasparenza. A livello europeo, il Digital Services Act ha segnato un'importante innovazione, vietando espressamente l'uso di interfacce ingannevoli. Accanto a questi strumenti, si affermano progressivamente principi di design etico e di tutela contro le forme più insidiose di personalizzazione manipolativa. In questo contesto dinamico, il capitolo si propone di analizzare il quadro regolatorio esistente, il ruolo delle autorità competenti e le attuali possibilità di tutela per gli utenti del digitale.

2.1 Quadro normativo europeo: GDPR, DSA, UCPD e AI Act

Negli ultimi anni, l'Unione Europea ha avviato un processo di aggiornamento del proprio quadro giuridico per adeguarlo alle sfide poste dall'economia digitale e in particolare dal crescente ricorso a tecniche manipolative nelle interfacce dei servizi online. Sebbene il concetto di *dark pattern* sia stato originariamente coniato in ambito accademico e tecnico, oggi trova riconoscimento esplicito o implicito in diverse fonti normative europee, che mirano a garantire la trasparenza e l'equità dei servizi digitali, la tutela dei diritti dei consumatori e la protezione dei dati personali.

2.1.1 Regolamento (UE) 2016/679 – GDPR

Il Regolamento Generale sulla Protezione dei Dati **(GDPR)** è il principale strumento normativo europeo in materia di tutela dei dati personali. Approvato nel 2016 ed entrato pienamente in vigore il 25 maggio 2018, il GDPR si applica in tutti gli Stati membri dell'Unione Europea e ha carattere direttamente vincolante: non richiede leggi nazionali di recepimento, ma si impone direttamente a imprese, enti pubblici e soggetti che trattano dati di cittadini europei.

Il GDPR è stato elaborato e approvato dal Parlamento Europeo e dal Consiglio dell'Unione Europea. La sua applicazione e interpretazione sono coordinate a livello europeo dal Comitato Europeo per la Protezione dei Dati **(EDPB)**, che riunisce le autorità garanti privacy di tutti gli Stati membri, oltre al Garante Europeo per la Protezione dei Dati.
Il GDPR non contiene disposizioni specifiche sui dark pattern né norme che regolino direttamente la correttezza della progettazione delle interfacce. Il regolamento si concentra infatti esclusivamente sulla protezione dei dati personali e sulla tutela della privacy degli interessati in relazione ai trattamenti effettuati. Tuttavia, è fondamentale che le interfacce non inducano in errore gli utenti né presentino elementi fuorvianti, poiché ciò violerebbe i principi di trasparenza e correttezza sanciti dal regolamento in materia di protezione dei dati e privacy. Come dimostra un recente studio infatti [12], il tasso di accettazione delle opzioni privacy sale dallo 0,16% all'83,55% nel caso in cui le stesse siano già preselezionate dal fornitore del servizio.
Il principio di trasparenza, è uno dei principi cardine del diritto europeo in materia di protezione dei dati personali. L'**Art. 5** del GDPR prevede infatti che i dati siano *«trattati in modo lecito, corretto e trasparente nei confronti dell'interessato»*. Le informazioni relative al trattamento dei dati personali, secondo il **Considerando [4] n.58,** devono essere fornite agli interessati in modo chiaro, facilmente accessibile e di facile comprensione, e si impone inoltre l'uso di un linguaggio semplice e chiaro. Segue l'**Art. 12** che prevede che *«il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile».* L'interessato deve quindi essere informato dell'esistenza del trattamento e delle sua finalità (**Considerando n.60**).
Gli utenti devono essere messi in condizione di sapere quali dati vengono raccolti, per quali finalità, per quanto tempo saranno conservati, con chi potranno essere condivisi e quali diritti possono esercitare. È vietato l'uso di linguaggi oscuri, informative eccessivamente complesse o interfacce ingannevoli che possano compromettere la consapevolezza e la libertà delle scelte dell'utente.
Segue nel **Considerando n.78**, il quale riporta che *«in fase di sviluppo, progettazione, selezione e utilizzo di applicazione, servizi e prodotti basati sul trattamento di dati personali, i produttori dei prodotti/servizi dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati dei consumatori allorchè sviluppino e progettino tali prodotti/servizi e, tenuto debito conto dello stato dell'arte, a far si che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezioni di dati».*

[4] Il "Considerando" nel GDPR è una parte introduttiva che precede il testo normativo vero e proprio.

Gli aspetti appena elencati sono stati oggetto di chiarimenti specifici da parte del Gruppo dell'Art. 29 (**WP29**)[5], che aggiunse che le informazioni devono essere facilmente accessibili e all'interessato non dovrebbe essere richiesto uno sforzo eccessivo per ricercarle, ovvero l'accesso alla sezione privacy dovrebbe essere immediatamente attuabile e non prevedere lo scorrimento di una grande quantità di testi o di pagine. Oltre il posizionamento, anche la combinazione dei colori che rendono meno evidente un testo o un collegamento sono considerati come facilmente accessibili ai sensi del Regolamento Europeo. [13]
È importante inoltre menzionare **l'Art. 25** e i due importanti principi in ambito privacy: *privacy by design* e *privacy by default*. Questi principi sono stati introdotti proprio nell'Art. 25, il quale prevede che il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate già nella fase di progettazione (e non solo nella fase finale) di un prodotto/servizio che comporti trattamento di dati personali per garantire il rispetto dei principi del GDPR e proteggere i diritti degli interessati. La protezione dei dati sin dalla progettazione per tutelare i diritti degli interessati prende proprio il nome di **privacy by design** e si basa su 7 principi elaborati da Ann Cavoukian: 1) prevenire e non correggere; 2) privacy come impostazione di default; 3) incorporazione della privacy nel progetto; 4) garanzia di massima funzionalità; 5) garanzia di sicurezza durante il ciclo del prodotto/servizio; 6) visibilità e trasparenza del trattamento; 7) centralità dell'utente. [14]
Per **privacy by default** si intende invece che la protezione di un trattamento di dati personali è garantita da impostazioni predefinite ("di default") affinché gli utenti ricevano un elevato livello di protezione dei propri dati anche se non si attivano autonomamente. [15] Questi princìpi mirano quindi a salvaguardare la privacy e i dati personali delle persone nella misura effettivamente necessaria. I dark pattern sono invece un modo per eludere questi princìpi spingendo i consumatori ad ignorare la loro privacy e a fornire più dati personali del necessario.
Un ultimo aspetto da tenere in considerazione è il consenso finale dell'utente per l'elaborazione dei dati personali dell'**Art.4**, ovvero *«una manifestazione di volontà libera, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso mediante dichiarazione inequivocabile».* Il successivo **Art. 7** prevede che la richiesta di tale consenso deve essere presentata in modo chiaramente distinguibile, comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. In generale, aggiunge l'EDPB, qualsiasi elemento di pressione o influenza inappropriata sul soggetto cui appartengono i dati, se idoneo ad impedire al soggetto stesso un libero esercizio della propria volontà rende il consenso non validamente fornito.

Il GDPR, ricorda poi l'EDPB, non prescrive un modo o una forma particolari per fornire le informazioni necessarie a soddisfare il requisito di un consenso libero ed informato: tali informazioni possono infatti essere comunicate in diverse forme. Tuttavia, il regolamento stabilisce principi volti a garantire elevati standard di chiarezza e accessibilità. L'impiego di dark pattern viola questi principi, poiché riduce la trasparenza e compromette la capacità dell'utente di esercitare un controllo effettivo sui propri dati personali: il consenso ottenuto non può più considerarsi realmente libero. L'uso di

[5] Gruppo di lavoro comune delle autorità nazionali di protezione dati ad oggi sostituito dal Comitato Europeo per la protezione dei dati (EDPB).

dark pattern per “guidare” gli utenti verso opzioni meno rispettose della privacy è quindi lesivo dei princìpi del GDPR anche sotto questo ulteriore aspetto.

2.1.2 Direttiva 2005/29/CE – Pratiche commerciale sleali (UCPD)

La UCPD costituisce uno degli strumenti normativi fondamentali dell’Unione Europea per la tutela dei consumatori. Entrata in vigore nel 2007 e recepita in Italia attraverso il Codice del Consumo (D.Lgs. 2006/2005), il suo obiettivo è vietare tutte quelle pratiche sleali che, nel contesto di un rapporto commerciale, distorcono in modo significativo il comportamento economico del consumatore medio, proteggendolo da messaggi ingannevoli, omissioni di informazioni rilevanti e tecniche aggressive. Per quanto non venga espressamente usato il termine “dark pattern”, la direttiva vieta espressamente in ogni forma e per mezzo di ogni canale (tradizionale e digitale) le pratiche commerciali sleali, in tutte le fasi del rapporto commerciale B2C (pubblicità, marketing, vendita). L’**Art. 5** introduce un divieto generale di pratiche sleali, vietando ogni comportamento contrario alla diligenza professionale che alteri le scelte economiche del consumatore. Gli **Art. 6 e 7**, poi, vietano rispettivamente le pratiche ingannevoli basate su azioni (ad esempio l’uso di informazioni false o ingannevoli sulla disponibilità di un prodotto, o sulla presenza di sconti fittizi) e le omissioni ingannevoli (come la mancata comunicazione di costi aggiuntivi, o la difficoltà nel reperire opzioni alternative). L’**Art. 8** vieta le pratiche aggressive che limitano la libertà decisionale dell’utente tramite coercizione o indebito condizionamento.
Per quanto tutti questi riferimenti possano ricondursi anche nel mondo digitale e all’utilizzo dei dark pattern, c’è da tenere a mente che in Europa il contesto dei dark pattern nasce in modo frammentato: l’UCPD è la prima norma che vieta le pratiche commerciali sleali, ma vieta solo alcuni tipi di comportamenti, ovvero quelli elencati nell’**Allegato I** (“lista nera”), ed essendo una direttiva nata nel 2005, non tratta in modo specifico i dark pattern digitali (perché la sua nascita è antecedente all’impiego di queste tecniche). [16] Però qui nasce un problema, in seguito alla successiva emanazione del Digital Service Act “DSA” nel 2022 (*che tratteremo nel paragrafo 2.1.4*) si sono riscontrate delle difficoltà applicative dell’UCPD. L’Art 25 del DSA (che vieta espressamente l’adozione di dark pattern da parte dei fornitori di piattaforme online**)**, infatti, non si applica se la pratica è già regolata da UCPD o GDPR. [17] Se un comportamento rientra già tra le pratiche vietate dalla UCPD (per esempio perché ingannevole) o è contrario ai principi GDPR (per esempio ottenimento scorretto del consenso), allora prevalgono queste norme essendo il DSA subordinato alle suddette previsioni, circoscrivendo così l’ambito effettivo di intervento dell’Art. 25. Questo crea conseguentemente un’incertezza giuridica: quale norma si applica tra GDPR, UCPD e DSA? Inoltre, poiché la UCPD ha un ambito di applicazione molto ampio, il rischio è che in sede applicativa si continui a far prevalere questo approccio caso per caso: ciò potrebbe vanificare l’intento del DSA e limitarne l’efficacia e la portata sui dark pattern. [18] Le difficoltà applicative della UCPD hanno progressivamente messo in luce la necessità di un aggiornamento del quadro normativo europeo. L’assenza di un riferimento esplicito alle nuove forme di manipolazione delle interfacce online e la natura ancora troppo generale delle disposizioni vigenti limitavano l’efficacia della tutela offerta ai

consumatori. In questo contesto si è avvertita l'esigenza di un intervento normativo volto a modernizzare e integrare la disciplina esistente, esigenza che verrà approfondita nel paragrafo successivo.

2.1.3 Direttiva Omnibus UE 2019/2161

La Direttiva (UE) 2019/2161, comunemente nota come **Direttiva Omnibus**, nasce con l'obiettivo di rafforzare la protezione dei consumatori e adeguare il quadro normativo alle sfide poste dall'ambiente digitale. La direttiva ha modificato vari strumenti esistenti, tra cui la stessa UCPD, intervenendo su aspetti quali:

- **Veridicità delle recensioni: dall'Art. 3,** l'utente deve essere informato se la recensione è stata sollecitata, originata da una sponsorizzazione o proveniente da un acquisto verificato. È inoltre vietato eliminare recensioni negative o inserire recensioni false.
- **Disciplina degli sconti: l'Art. 2** della direttiva recita che *ogni annuncio di riduzione di un prezzo deve indicare il prezzo precedente applicato dal professionista per un determinato periodo di tempo prima dell'applicazione di tale riduzione,* ossia lo sconto dovrà essere sempre in relazione al prezzo più basso avuto negli ultimi 30 giorni. Sono inoltre vietati gli aumenti di prezzo fittizi e sconti perpetui. [19]

Riportiamo anche altri aggiornamenti tra cui la trasparenza nelle pratiche di marketing online e la personalizzazione dei prezzi. Sebbene non abbia modificato direttamente l'Allegato I della UCPD, la Direttiva Omnibus ha contribuito a colmare alcune delle principali lacune esistenti, introducendo obblighi più stringenti per le imprese che operano nel contesto digitale. Proprio per valutare l'efficacia di questo quadro normativo aggiornato, la Commissione ha avviato nel 2020 un ampio *fitness check*[6]sul diritto dei consumatori. [20] Questo ha evidenziato che, nonostante i miglioramenti introdotti dalla Omnibus, la normativa risultava ancora insufficiente per contrastare in modo chiaro ed efficace i dark pattern: l'elenco delle pratiche vietate rimaneva troppo generico e privo di riferimenti specifici alle nuove forme di manipolazione digitale. Parallelamente, il **Digital Services Act (DSA)**, adottato nel 2022 che vedremo di seguito, ha introdotto per la prima volta un divieto esplicito dei dark pattern.

2.1.4 Regolamento (UE) 2022/2065 - Digital Services Act (DSA)

Il **DSA** (*Digital Services Act*) è una normativa dell'Unione Europea entrata in vigore nel 2022 che disciplina la responsabilità delle piattaforme online e dei servizi digitali. Il suo obiettivo principale è garantire un ambiente digitale più sicuro e trasparente, imponendo obblighi specifici per contrastare

[6] Strumento utilizzato dalla Commissione Europea per valutare se la norma vigente è ancora idonea a raggiungere i suoi obiettivi. Si tratta di una sorta di "verifica di forma" con cui la Commissione esamina l'efficacia, l'efficienza, la coerenza e la rilevanza di una normativa o di un pacchetto normativo.

contenuti illegali, proteggere i diritti fondamentali degli utenti e regolamentare l'uso degli algoritmi e della pubblicità online. Il DSA si applica a una vasta gamma di servizi digitali, dai piccoli siti ai grandi operatori come social network e marketplace. Fa parte di un pacchetto legislativo autonomo che agiscono sulla *governance*[7]

Il DSA affronta in modo esplicito l'uso dei dark pattern, riconoscendo come queste pratiche ingannevoli compromettano la capacità degli utenti di esercitare scelte autonome e consapevoli online. Nel **Considerando 67**, il regolamento evidenzia che i fornitori di servizi devono garantire che i loro sistemi di interfaccia non distorcano intenzionalmente o manipolino i comportamenti degli utenti, né li spingano verso decisioni non desiderate o meno rispettose dei loro diritti. *«Ai fornitori di piattaforme online dovrebbe pertanto essere vietato ingannare o esortare i destinatari del servizio e distorcere o limitare l'autonomia, il processo decisionale o la scelta dei destinatari del servizio attraverso la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa. Dovrebbe inoltre vietare di reiterare la richiesta a un destinatario del servizio di effettuare una scelta qualora tale scelta sia già stata effettuata, rendendo la procedura di cancellazione di un servizio notevolmente più complessa di quella di aderirvi, o rendendo talune scelte più difficili o dispendiose in termini di tempo rispetto ad altre, rendendo irragionevolmente difficile interrompere gli acquisti o uscire da una determinata piattaforma online».* Tali tecniche sono considerate incompatibili con i principi di trasparenza e libertà decisionale che il DSA promuove. Questo orientamento si traduce in un preciso obbligo normativo previsto dall'**Art. 25** del DSA, che **vieta espressamente l'adozione di dark pattern da parte dei fornitori di piattaforme online**. Inoltre, il DSA chiarisce che tale divieto opera in parallelo e in coordinamento con altre normative esistenti come il **GDPR** laddove una pratica scorretta configuri anche una violazione di queste norme, il quadro sanzionatorio e regolatorio specifico continuerà ad applicarsi. Le violazioni possono comportare sanzioni fino al **6% del fatturato globale annuo** per le Very Large Online Platforms (VLOPs), come dimostrano i primi casi già oggetto di procedimenti da parte delle autorità di vigilanza. [21]

Accanto agli strumenti già trattati, altre normative recenti stanno contribuendo in modo significativo a rafforzare la disciplina europea contro i dark pattern. La **Direttiva sui diritti dei consumatori (CRD, Direttiva 2011/83/UE)**, modificata nel **2023**, ha introdotto, con **l'Art.16** (Paragrafo 16, lettera e), il divieto per i professionisti di *«utilizzare tecniche di progettazione o interfacce che spingano i consumatori a prendere decisioni che non avrebbero altrimenti preso»*, con specifico riferimento ai contratti di servizi finanziari a distanza. [22] Si tratta di un primo riconoscimento formale, a livello settoriale, dell'impatto delle interfacce manipolative sui diritti dei consumatori.

Parallelamente, il **Digital Markets Act** (DMA, Regolamento UE 2022/1925), adottato nel **2022** ed entrato in applicazione il 2 maggio 2023, affronta la questione dei dark pattern nelle piattaforme digitali più influenti. L'**Art. 13** prevede infatti che *«i gatekeeper*[8] *non devono eludere o tentare di*

[7] Per governance si intende l'insieme delle regole e dei meccanismi che disciplinano il funzionamento e le responsabilità dei servizi digitali.

[8] Grande piattaforma digitale che, per dimensioni e influenza sul mercato, controlla l'accesso di imprese e utenti a servizi digitali essenziali.

eludere gli obblighi che derivano dal presente regolamento», e la Commissione europea ha chiarito nei documenti interpretativi che tale clausola comprende anche il divieto di ricorrere a interfacce manipolative o fuorvianti per ottenere consensi o modificare comportamenti degli utenti in modo sleale. Questo aspetto è particolarmente rilevante, poiché mira a impedire che i gatekeeper sfruttino il loro potere di mercato attraverso tecniche manipolative che rafforzano il lock-in o distorcono la concorrenza. [23]

Ancora più innovativo è l'approccio adottato nell'**Artificial Intelligence Act (AI Act)**, approvato nel **2024**. L'**Art. 5** (paragrafo 1, lettere a) e b)) vieta l'uso di *«sistemi di intelligenza artificiale che impiegano tecniche subliminali non percepibili dalla persona o che sfruttano vulnerabilità legate all'età, alla disabilità o alla situazione sociale o economica di un gruppo specifico»*, quando tali tecniche sono *«intese a distorcere materialmente il comportamento di una persona in modo da causarle o a terzi danni fisici o psicologici»*. [24] Questo intervento apre un nuovo fronte di regolazione, volto a contrastare l'uso delle tecnologie AI per sviluppare dark pattern avanzati, capaci di influenzare le scelte degli utenti in maniera sempre più pervasiva.

Tuttavia, la molteplicità di fonti normative e l'attuale frammentazione tra strumenti settoriali sollevano ancora questioni di coerenza e certezza del diritto. Per questo, la Commissione europea, in seguito al fitness check, ha avviato la preparazione di un nuovo intervento organico: il **Digital Fairness Act**, atteso per la metà del **2026**, il cui obiettivo sarà proprio quello di introdurre un divieto trasversale, uniforme e pienamente armonizzato dei dark pattern in tutto l'ecosistema digitale europeo. [25] L'evoluzione normativa in atto evidenzia una crescente consapevolezza, a livello europeo, della necessità di disporre di strumenti giuridici chiari e integrati per tutelare i diritti fondamentali dei cittadini contro le moderne tecniche manipolative delle interfacce digitali.

2.2 Quadro normativo italiano: GDPR e Codice del Consumo

Nel sistema giuridico italiano, la disciplina in materia di dark pattern si costruisce su un intreccio tra fonti nazionali ed europee. I **regolamenti europei** (come il GDPR e il DSA) hanno efficacia diretta in Italia: non richiedono recepimento e prevalgono sulle norme nazionali in caso di conflitto. Le **direttive europee** (come la UCPD e la Direttiva Omnibus), invece, vengono recepite dallo Stato italiano tramite decreti legislativi, che ne integrano i contenuti all'interno dell'ordinamento, ad esempio attraverso il Codice del Consumo che vedremo seguentemente. Questo sistema garantisce una coesistenza tra i due livelli: le norme italiane devono essere coerenti con quelle europee, e si applicano in modo complementare salvo che un regolamento europeo non imponga regole direttamente applicabili e prevalenti. In assenza di una normativa italiana specifica dedicata ai dark pattern, oggi il contrasto a queste pratiche si basa su questo quadro integrato tra fonti europee e nazionali, e sull'azione delle autorità indipendenti.

2.2.1 D.Lgs. 206/2005 - Codice del Consumo

Il **Codice del Consumo** (D.Lgs. 6 settembre 2005, n. 206) è il principale strumento normativo italiano volto a garantire la tutela dei consumatori nei rapporti con i professionisti. Introdotto per coordinare e sistematizzare le disposizioni nazionali in materia, esso rappresenta anche il recepimento della Direttiva 2005/29/CE (UCPD) nell'ordinamento italiano. In tale quadro, il rapporto tra il Codice del Consumo italiano e il diritto europeo è fondato sul principio di *armonizzazione minima*: la normativa europea (come, ad esempio, una direttiva) stabilisce solo dei requisiti minimi che gli Stati membri devono garantire. La normativa nazionale deve quindi rispettare gli standard stabiliti dall'UE ma può prevedere un livello di tutela più elevato.
Il Codice si applica a ogni fase del rapporto commerciale B2C. L'**Art. 20** (comma 2), stabilisce che *«È considerata sleale ogni pratica commerciale contraria alla diligenza professionale e idonea a falsare in misura apprezzabile il comportamento economico del consumatore medio»*.
L'**Art. 21** disciplina le pratiche ingannevoli *per azione*, vietando *«le pratiche commerciali che contengono informazioni non rispondenti al vero o che, sebbene di fatto corrette, sono idonee a trarre in inganno il consumatore medio»*, mentre l'**Art. 22** disciplina invece le pratiche ingannevoli per omissione**,** vietando *«l'omissione di informazioni rilevanti»* che impediscano al consumatore di prendere una decisione consapevole.
Si riporta anche l'**Art. 24** che vieta *«le pratiche commerciali aggressive»* che, attraverso coercizione o indebita pressione, possano compromettere la libertà di scelta del consumatore. [26]
Il Codice del Consumo recepisce integralmente l'elenco delle pratiche commerciali sleali vietate dall'Allegato I dell'UCPD, come abbiamo visto precedentemente, in una propria appendice normativa chiamata anch'essa Allegato I. Qui vi sono elencate una serie di pratiche considerate sleali in ogni caso, senza necessità di ulteriore valutazione. Sebbene non vi sia un riferimento espresso ai dark pattern, molte tecniche manipolative digitali risultano inquadrabili nelle condotte vietate dal Codice.

2.2.2 D.Lgs. 26/2023 - recepimento Direttiva Omnibus

Il D.Lgs. 26/2023, entrato in vigore nel 2023, ha recepito in Italia la Direttiva (UE) 2019/2161- Direttiva Omnibus precedentemente trattata, con l'obiettivo di aggiornare e rafforzare la disciplina nazionale in materia di tutela dei consumatori, in particolare per far fronte alle sfide poste dal contesto digitale. Il decreto ha modificato in modo significativo il **Codice del Consumo**, introducendo nuove norme in tema di trasparenza e pratiche sleali online. Gli articoli riportati qui di seguito sono i principali che possono essere collegati, anche in modo interpretativo, al contrasto ai dark pattern.
L'**Art.1** ha aggiornato l'**Art. 17** del Codice di Consumo (visto appena precedentemente), introducendo l'obbligo per i professionisti di fornire informazioni chiare sulle recensioni online. Il comma 4 dello stesso articolo ha modificato l'**Art. 21** del codice di consumo introducendo il divieto assoluto di pratiche commerciali ingannevoli che inducono o possono indurre il consumatore medio a prendere decisioni commerciali che non avrebbero preso altrimenti. L'**Art. 2** ha modificato l'**Art.**

17-bis, disponendo, come abbiamo visto, che *«ogni annuncio di riduzione di prezzo debba indicare il prezzo praticato nei trenta giorni precedenti»*. Chiunque violi tale disposizione sarà soggetto alla sanzione amministrativa pecuniaria da Euro 516,45 a Euro 3.098,74.
Inoltre, l'**Art. 3** ha aggiunto nel Codice di Consumo il nuovo **Art. 22-bis**, che vieta pratiche relative alla personalizzazione dei prezzi senza adeguata informazione: *«Nel caso di offerte personalizzate di prezzi sulla base di processi automatizzati di profilazione, il consumatore deve essere chiaramente informato»*.
Sebbene il decreto non abbia modificato l'Allegato I del Codice di Consumo, le disposizioni recepite dal D.Lgs. 26/2023 contribuiscono comunque a rafforzare il contrasto a molte pratiche tipiche di design manipolativo, in particolare quelle legate a sconti ingannevoli, recensioni non trasparenti e personalizzazione occulta dei prezzi.

2.2.3 D.Lgs. 196/2003 + D.Lgs. 101/2018

In Italia, il contrasto ai dark pattern legati alla raccolta del consenso e al trattamento dei dati personali trova fondamento nel Codice Privacy (D.Lgs. 196/2003), modificato successivamente dal D.Lgs. 101/2018 per adeguarsi al GDPR europeo. Pur recependo pienamente i principi europei, il Codice introduce norme che rafforzano la disciplina interna, in particolare l'**Art. 130**, che vieta l'uso di *«tecniche ingannevoli o manipolative»* per ottenere il consenso della privacy. Vieta inoltre l'invio di comunicazioni promozionali e pubblicitarie *"senza il preventivo consenso espresso del contraente o dell'utente"* e sancisce che tale consenso deve essere raccolto nel rispetto dei principi di *«libertà, specificità e informazione completa»*.
Questo articolo si applica anche in relazione a interfacce grafiche ingannevoli o modelli di design che rendano difficile per l'utente comprendere che sta prestando il proprio consenso al trattamento dei dati per finalità di marketing. Ad esempio, in presenza di pulsanti "accetta*"* particolarmente evidenti o percorsi tortuosi per negare il consenso. In questo caso si può configurare una violazione dell'Art. 130.

2.3 Sistemi di ispezione in Italia e strumenti nelle mani dei consumatori

In Italia, un ruolo essenziale nel contrasto ai dark pattern è svolto non solo dalla normativa, ma anche dall'attività delle cosiddette **autorità indipendenti**: organismi pubblici dotati di autonomia e poteri di vigilanza, regolazione e sanzione, istituiti per garantire il rispetto di diritti fondamentali in specifici settori. Queste autorità già consentono di contrastare molte pratiche riconducibili ai dark pattern, pur non essendo, ad oggi, dotata di una disciplina organica specifica.
Tra questi, le autorità oggi più coinvolte sul tema sono: il **Garante per la protezione dei dati personali, l'Autorità Garante della Concorrenza e del Mercato (AGCM)** e, con ruolo potenziale crescente, l'**Autorità per le Garanzie nelle Comunicazioni (AGCOM**).

L'**AGCM** (Autorità Garante della Concorrenza e del Mercato) opera con particolare efficacia sul versante dei rapporti B2C, estendendo l'applicazione del Codice del Consumo per sanzionare pratiche che rientrano a pieno titolo tra i dark pattern. Sono stati colpiti comportamenti come ostacoli alla disdetta, opzioni preselezionate, percorsi d'acquisto costruiti per indurre il consumatore a scelte non volute o non consapevoli. Attraverso tali interventi, l'AGCM sta contribuendo a definire una prassi nazionale che, in assenza di un divieto espresso, fornisce comunque una protezione concreta contro le manipolazioni digitali.
L'**AGCOM** (Autorità per le Garanzie nelle Comunicazioni), invece, è un'autorità indipendente competente per i settori delle telecomunicazioni e dei media audiovisivi, non ha ancora adottato provvedimenti formali in materia di dark pattern, ma svolge attività di vigilanza in tema di trasparenza contrattuale e correttezza dell'informazione nei servizi digitali.
Infine, il **Garante per la protezione dei dati personali** è l'autorità indipendente preposta al controllo dell'applicazione della normativa italiana ed europea in materia di privacy e protezione dei dati personali, con poteri di ispezione, regolamentazione e sanzione. In tale funzione, il Garante contrasta attivamente l'uso di interfacce manipolative, in particolare nei meccanismi di acquisizione del consenso, che violino i principi previsti dal GDPR e dal Codice Privacy. Un ambito particolarmente esaminato è quello dei *cookie banner*, dove il Garante, ai fini di esigere parità di visibilità tra opzioni di accettazione e rifiuto e contrastando percorsi grafici ingannevoli, applica le **Linee guida 03/2022 dell'EDPB**, uno strumento operativo (che vedremo qui di seguito) per autorità di controllo, enti, imprese e consumatori, volto a chiarire quali pratiche di design manipolativo nei servizi digitali risultino incompatibili con i principi di trasparenza e correttezza.

2.3.1 Strumenti per i consumatori: Linee guida 03/2022 dell'EDPB

Il 24 febbraio 2023, l'**EDPB** ha pubblicato le linee guida su come riconoscere ed evitare questi sistemi. Il documento offre raccomandazioni pratiche a gestori dei social media, a designer e utenti su come comportarsi di fronte a queste interfacce che si pongono in violazione del Regolamento europeo in materia di protezione dati.
Le linee guida dell'EDPB individuano sei tipologie riguardo alle quali si può parlare di modelli di progettazione ingannevoli: [27]

- **Overloading:** quando gli utenti si trovano di fronte a una enorme numero di richieste, informazioni, opzioni o possibilità finalizzate a spingerli a condividere più dati possibili e consentire involontariamente il trattamento dei dati personali contro le aspettative dell'interessato;
- **Skipping:** quando le interfacce sono realizzate in modo tale che gli utenti dimentichino o non riflettano su aspetti legati alla protezione dei propri dati;
- **Stirring:** quando le scelte degli utenti sono influenzate facendo appello alle loro emozioni o usando sollecitazioni visive;

- **Hindering:** quando gli utenti sono ostacolati o bloccati nel processo di informazione sull'uso dei propri dati o nella gestione dei propri dati;
- **Flickle:** quando gli utenti acconsentono al trattamento dei propri dati senza capire quali siano le finalità a causa di un'interfaccia incoerente o poco chiara;
- **Leftinthedark:** quando l'interfaccia è progettata in modo da nascondere le informazioni e gli strumenti di controllo della privacy agli utenti.

CAPITOLO 3: CASI STUDIO RILEVANTI NEL SETTORE DELL'ECOMMERCE

Il settore e-commerce costituisce oggi uno degli ambiti in cui l'utilizzo dei dark pattern raggiunge le forme più articolate e pervasive. Secondo uno studio della Commissione Europea (2022), oltre il 40% dei principali siti di e-commerce analizzati in Europa applica tecniche di design manipolativo idonee a condizionare le scelte dei consumatori. L'interfaccia utente, elemento chiave dell'esperienza d'acquisto online, viene spesso progettata per sfruttare bias cognitivi e meccanismi comportamentali, con l'obiettivo di massimizzare i tassi di conversione e incrementare i ricavi.

Tra le tecniche più diffuse rientrano: il preselezionamento automatico di servizi accessori (polizze assicurative, opzioni premium), messaggi di scarsità artificiosa (*"ultima camera disponibile"*), pressioni temporali (*"offerta valida solo per oggi"*), l'uso di falsi countdown o di notifiche sociali ingannevoli (*"altri 20 utenti stanno guardando questo prodotto"*), oltre a percorsi di checkout disegnati per rendere più difficile rifiutare servizi opzionali o per ostacolare la revoca del consenso.

Secondo un report del 2023 [28], il 38% dei siti analizzati in Europa ha ricevuto richieste formali di adeguamento da parte delle autorità nazionali; in particolare 42 siti impiegavano falsi countdown, **54** spingevano i consumatori verso scelte di abbonamento/consegna più onerose tramite design grafico o linguaggio, e **70** occultavano o rendevano meno visibili informazioni rilevanti. In **23** di questi casi, l'occultamento delle informazioni era finalizzato a far attivare inconsapevolmente abbonamenti. Inoltre, l'indagine ha esaminato anche le app mobili di **102 siti**, riscontrando che **27** di queste impiegavano almeno una delle tre categorie di dark pattern individuate. In Italia, negli ultimi anni, l'AGCM ha sanzionato piattaforme e-commerce per un ammontare complessivo superiore ai 15 milioni di euro in relazione a pratiche scorrette legate all'uso di interfacce manipolative. Non sorprende, quindi, che il commercio elettronico sia oggi uno dei principali obiettivi delle autorità di vigilanza e che il tema sia al centro delle future politiche europee in materia, a partire dal progetto di **Digital Fairness Act**, che mira a rafforzare la tutela dei consumatori nel contesto digitale.

3.1 Il caso studio in Italia: Volagratis

Un caso di particolare rilievo nel panorama italiano in tema di dark pattern applicati al settore **e-commerce** è rappresentato dal procedimento che ha coinvolto nel 2019 la piattaforma **Volagratis**[9] (gruppo Bravofly Rumbo Group), sottoposta a sanzione da parte dell'Autorità Garante della Concorrenza e del Mercato (AGCM) con il provvedimento **PS11006**. [29] Il procedimento si è concentrato sull'esame delle pratiche adottate dal sito di prenotazione di voli e pacchetti viaggio, con riferimento al modo in cui venivano presentati i prezzi e costruito il processo di acquisto online.
L'istruttoria dell'**AGCM** ha fatto emergere l'uso sistematico di tecniche riconducibili ai dark pattern in diverse fasi dell'interazione utente. In particolare, i prezzi pubblicizzati durante la **prima fase di ricerca** non includevano una serie di **costi obbligatori** che, di fatto, sarebbero stati applicati al consumatore. Nelle fasi successive del processo di check-out, numerosi servizi e supplementi, tra cui assicurazioni facoltative, scelta del posto a pagamento, priorità di imbarco, bagaglio extra, che venivano aggiunti automaticamente oppure proposti in maniera che spingesse il consumatore ad accettarli inconsapevolmente. [30]
Tali opzioni risultavano **preselezionate di default** *"pre-flag"* una pratica che, secondo l'Autorità, comprometteva la capacità decisionale del consumatore e lo portava ad accettare servizi non espressamente desiderati. A questa struttura di interfaccia si aggiungeva un percorso d'acquisto volutamente frammentato e opaco, che riduceva la trasparenza e ostacolava il confronto tra le opzioni o la comprensione immediata del costo finale dell'acquisto.
Dal punto di vista giuridico, l'AGCM ha rilevato che tali pratiche configuravano una violazione dei principi di diligenza professionale e di correttezza richiesti agli operatori di mercato, e che l'insieme delle condotte aveva un impatto significativo sulla libertà di scelta economica dell'utente. In termini normativi, il comportamento di Volagratis è stato ritenuto in contrasto con le disposizioni del **Codice del Consumo** (D.Lgs. 206/2005), e in particolare:

- **Art. 20**, che vieta le pratiche commerciali contrarie alla diligenza professionale;
- **Art. 21**, in relazione alle omissioni ingannevoli circa i costi effettivi dell'acquisto;
- **Art. 22**, in merito alla presentazione ingannevole del prezzo;
- **Art. 24**, relativo alle pratiche aggressive che condizionano indebitamente la decisione del consumatore.

L'**Autorità** ha sottolineato che la costruzione dell'interfaccia grafica e il design del percorso di acquisto avevano chiaramente la funzione di guidare inconsapevolmente il consumatore verso scelte più onerose e meno consapevoli. Non si trattava quindi di una mera carenza informativa, ma di un vero e proprio utilizzo strategico del design per alterare il comportamento economico dell'utente.
Come esito del procedimento, l'AGCM ha irrogato una sanzione amministrativa di **Euro 1,1 milioni** nei confronti di Volagratis. Più importante ancora dell'importo della sanzione è stato il valore "giurisprudenziale" del caso: è considerato, infatti, uno dei primi riconoscimenti formali in Italia dell'esistenza e della rilevanza giuridica dei dark pattern applicati nei meccanismi commerciali digitali.

[9] Piattaforma online per prenotare voli, alloggi ed hotel.

Il caso Volagratis è stato successivamente più volte richiamato in dottrina e nelle relazioni annuali dell'AGCM, e ha anticipato molte delle tematiche che sarebbero poi state rafforzate nella successiva Direttiva Omnibus e nelle Linee guida EDPB 03/2022 precedentemente visti, contribuendo all'attuale interpretazione estensiva del Codice del Consumo rispetto alle interfacce manipolative nel commercio elettronico.

3.2 Il caso studio europeo: Booking.com

Un caso particolarmente rilevante e paradigmatico nel contrasto europeo ai dark pattern è quello che ha coinvolto la piattaforma di prenotazione online Booking.com, leader globale nel settore travel e-commerce. Il procedimento ha preso avvio nel 2019 a seguito di un'azione concertata tra la Commissione Europea, il network Consumer Protection Cooperation (**CPC**) e numerose autorità nazionali, tra cui l'AGCM italiana. L'indagine ha posto al centro dell'attenzione una serie di pratiche di design manipolativo finalizzate a condizionare la libertà decisionale del consumatore. [31]
Le condotte contestate includevano l'uso sistematico di **messaggi di scarsità artificiosa** ("ultima camera disponibile", "prenotata 10 volte oggi"), di **pressioni temporali** ("offerta valida solo per oggi"), e di **notifiche sociali ingannevoli** ("15 persone stanno guardando questa struttura ora"). Inoltre, il sistema di prenotazione presentava in modo poco trasparente le informazioni relative ai prezzi, omettendo spese accessorie (ad esempio tasse di soggiorno, spese di pulizia) che diventavano visibili solo nelle ultime fasi del check-out. [32]
L'indagine ha mostrato come tali tecniche fossero progettate per suscitare urgenza, ansia da scarsità e pressione emotiva, inducendo l'utente a concludere l'acquisto rapidamente e senza un confronto critico delle alternative. La Commissione ha valutato che queste pratiche violassero i principi sanciti dalla Direttiva 2005/29/CE **(UCPD)** in materia di pratiche commerciali sleali, configurandosi come pratiche ingannevoli e aggressive che falsavano le scelte dei consumatori. In particolare risultano violati i seguenti articoli dell'UCPD:

- **Art. 6**: *Pratiche commerciali ingannevoli per azione*: uso di messaggi falsi o ingannevoli sulla scarsità dei prodotti, urgenza dell'acquisto e popolarità delle offerte;
- **Art. 7:** *Pratiche commerciali ingannevoli per omissione*: occultamento o presentazione poco chiara di costi accessori obbligatori, quali spese di pulizia e tasse locali;
- **Art. 8**: *Pratiche commerciali aggressive*: tecniche di pressione psicologica e design manipolativo tali da limitare la libertà decisionale del consumatore;
- **Allegato I:** richiamo alle pratiche vietate, quali la falsa dichiarazione di offerte a tempo limitato o vantaggi esclusivi non reali.

L'azione congiunta della Commissione e delle autorità nazionali ha portato Booking.com ad accettare un piano di adeguamento sostanziale entro giugno 2020, impegnandosi a garantire piena trasparenza sui prezzi e sulle condizioni di prenotazione, a rimuovere i falsi messaggi di scarsità e urgenza, e a correggere il design delle interfacce per eliminare le componenti manipolative. L'AGCM ha inoltre

avviato in parallelo un proprio procedimento autonomo, conclusosi con l'irrogazione di una sanzione amministrativa **di Euro 1,35 milioni** a Booking.com B.V. per le stesse condotte, arrivando con le sanzioni degli altri ad Euro 3,9 milioni. [33]
Questo caso ha segnato un precedente di grande rilievo per il diritto europeo in materia di dark pattern. In primo luogo, ha dimostrato l'efficacia del modello CPC nella lotta ai comportamenti sleali transfrontalieri. In secondo luogo, ha influenzato direttamente l'evoluzione normativa successiva: la Direttiva Omnibus (2019/2161/UE) ha introdotto obblighi più stringenti in tema di trasparenza dei prezzi e di marketing online, e le Linee guida EDPB 03/2022 hanno recepito molte delle problematiche emerse nel caso Booking.
Dal punto di vista del mercato, l'impatto è stato rilevante: Booking.com è tra le piattaforme più utilizzate in Europa per la prenotazione di viaggi, con oltre 40 milioni di utenti attivi mensili. La rimozione di queste pratiche manipolative ha migliorato in modo significativo la trasparenza e l'equità per milioni di consumatori, contribuendo a creare standard più elevati per l'intero comparto travel online.

CAPITOLO 4: CONCLUSIONI

L'analisi condotta sul fenomeno dei dark pattern e sul relativo quadro normativo europeo e italiano ha permesso di evidenziare come tali pratiche costituiscano oggi una delle forme più sofisticate e pervasive di alterazione della libertà decisionale dei consumatori nel contesto digitale.
Negli ultimi anni, l'evoluzione normativa dimostra come a livello europeo vi sia oggi una crescente consapevolezza della necessità di rafforzare la tutela del consumatore contro queste tecniche.
I casi esaminati in questa tesina dimostrano chiaramente che i dark pattern producono effetti materiali rilevanti sui consumatori. Queste pratiche non solo falsano il processo decisionale ed espongono l'utente a costi inattesi o non voluti, ma possono generare frustrazione, senso di inganno e, nel lungo periodo, erosione della fiducia nei confronti delle piattaforme digitali. Gli effetti risultano ancora più accentuati per categorie vulnerabili, come gli anziani, i minori o gli utenti con scarsa alfabetizzazione digitale.
Guardando al futuro, il contrasto ai dark pattern richiederà un approccio sempre più dinamico e integrato. Sarà fondamentale aggiornare costantemente il quadro normativo per intercettare nuove tecniche che evolvono in parallelo alle innovazioni tecnologiche, come l'intelligenza artificiale e i modelli predittivi. Parallelamente, sarà necessario rafforzare il coordinamento tra autorità nazionali ed europee, per assicurare un'azione di enforcement armonizzata e tempestiva. Ma il diritto da solo non basterà: un ruolo essenziale dovrà essere svolto anche dall'educazione digitale, affinché i consumatori sviluppino maggiore consapevolezza critica verso i meccanismi manipolativi insiti in molte interfacce online. Solo attraverso un'azione congiunta di diritto, enforcement e cultura digitale sarà possibile costruire un ecosistema digitale che rispetti davvero i principi fondamentali di trasparenza, correttezza e libertà di scelta sanciti dal diritto europeo e nazionale.

Bibliografia

[1] Eurostat, «Internet purchases by individuals (2002–2019),» 2024. [Online]. Available: https://ec.europa.eu/eurostat/databrowser/view/ISOC_EC_IBUY/default/table?lang=en.

[2] D. D. BJ Fogg, «ResearchGate,» 2007. [Online]. Available: http://captology.info/wp-content/uploads/2014/10/Fogg-HCI2007.pdf.

[3] Lanzing, «"Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies,» 2019. [Online]. Available: https://www.researchgate.net/publication/325606545_Strongly_Recommended_Revisiting_Decisional_Privacy_to_Judge_Hypernudging_in_Self-Tracking_Technologies.

[4] H. Brignull, «Deceptive Patterns,» 2010. [Online]. Available: https://www.deceptive.design/.

[5] C. S. Richard Thaler, «Nudge: Improving Decisions About Health, Wealth, and Happiness.,» 2008. [Online]. Available: https://www.researchgate.net/publication/257178709_Nudge_Improving_Decisions_About_Health_Wealth_and_Happiness_RH_Thaler_CR_Sunstein_Yale_University_Press_New_Haven_2008_293_pp.

[6] F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, «Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation,» 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en.

[7] A. Mathur, G. Acar, E. Lucherini, «Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,» 2019. [Online]. Available: https://arxiv.org/abs/1907.07032.

[8] University Of Chicago, «University Of Chicago,» 2019. [Online]. Available: https://computerscience.uchicago.edu/news/dark-patterns/#:~:text=...%20computerscience.uchicago.edu%20%20A%20first,1%20out%20of%2010.

[9] C. -. I. Ivanova, «How websites use "dark patterns" to manipulate you,» 2021. [Online]. Available: https://www.cbsnews.com/news/manipulative-advertising-technology-dark-patterns/#.

[10] Verbraucherverband, The European Consumer Organisation Bureau Européen des Unions de Consommateurs Europäischer, «CLICK TO BUY (MORE): How fast fashion giant SHEIN uses dark patterns to push overconsumption,» 2025. [Online]. Available: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-051_How_fast_fashion_giant_SHEIN_uses_dark_patterns.pdf#:~:text=BEUC's%20UK%20member%20Citizens%20Advice114,£276%20during%20the%20last%2012.

[11] H. Baldick, S.C. Jang, «Tricked into booking? The hidden influence of dark patterns on boutique hotel bookings,» 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0278431925002270#:~:text=Tricked%20into%20booking%3F%20The%20hidden,to%20postpone%20booking%20among.

[12] C. Utz, M. Degeling, S. Fahl, «(Un)informed Consent: Studying GDPR Consent Notices in the Field,» 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3319535.3354212.

[13] EDPB, «Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them,» 2018-2022. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

[14] «iapp.org,» [Online]. Available: https://iapp.org/resources/article/oipc-privacy-by-design-resources/.

[15] EUR-Lex, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

[16] EUR-Lex, «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,» Gazzetta ufficiale dell'Unione europea, 2005.

[17] European Parliament, «Regulating dark patterns in the EU: Towards digital fairness,» 2025. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf.

[18] E. Gatelli, «Dark pattern e personalizzazione manipolativa: fit check del panorama legislativo europeo,» 2025. [Online]. Available: https://www.medialaws.eu/rivista/dark-pattern-e-personalizzazione-manipolativa-fit-check-del-panorama-legislativo-europeo/#_ftnref6.

[19] EUR-Lex, «Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e u,» in *Gazzetta Ufficiale dell'Unione europa*, 2019.

[20] European Commission, «Fitness check on Consumer Law of Digital Fairness,» 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52024SC0245.

[21] EUR-Lex, «Text Document information Procedure Document summary Up-to-date link Permanent link Download notice Save to My items Create an email alert Create an RSS alert 27/10/2022 Legal act Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 o,» in *Gazzetta ufficiale dell'Unione europea*, 2022.

[22] EUR-Lex, «Direttiva (UE) 2023/2673 del Parlamento europeo e del Consiglio, del 22 novembre 2023, che modifica la direttiva 2011/83/UE per quanto riguarda i contratti di servizi finanziari conclusi a distanza e abroga la direttiva 2002/65/CE,» in *Gazzetta ufficiale dell'Unione europea*, 2023.

[23] EUR-Lex, «Regolamento (UE) 2022/1925 del Parlamento europeo 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),» in *Gazzetta ufficiale dell'Unione europea*, 2022.

[24] EUR-Lex, «European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),» 2024.

[25] D. F. Act, EDPI, 2024. [Online]. Available: https://digitalfairnessact.com/historic-timeline?utm_source=chatgpt.com.

[26] Normattiva, «DECRETO LEGISLATIVO 6 settembre 2005 , n. 206 Codice del consumo,» 2005.

[27] E. D. P. B. (EDPB), «Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them,» 2023. [Online]. Available: https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

[28] European Commission, «Consumer protection: manipulative online practices found on 148 out of 399 online shops screened,» 2023.

[29] Autorità Garante della Concorrenza e del Mercato (AGCM), «Provvedimento PS11006 — Pratica commerciale scorretta posta in essere da Bravofly Rumbo Group S.A. (Volagratis), Bollettino n. 16/2019, 11 aprile 2019,» 2019.

[30] G.Milizia, «“Vola gratis!”, ma il consumatore deve pagare un caro prezzo: pratica commerciale scorretta,» 2019. [Online]. Available: https://www.dirittoegiustizia.it/#/documentDetail/9199222.

[31] Commissione Europa, «Consumer Protection: Booking.com commits to improve presentation of online offers following dialogue with the European Commission and national consumer authorities, Bruxelles, 20 dicembre 2019,» 2019.

[32] Commissione Europea – CPC Network (Consumer Protection Cooperation), «Booking.com improves the transparency of its online offers following dialogue with the European Commission and EU consumer authorities,» 2019.

[33] AGCM, «Provvedimento PS11755 del 2021,» 2021.