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 +

Ruolo del diritto digitale nella protezione dei consumatori online: analisi dei Dark Pattern e della manipolazione del marketing

Ludovica De Santis

0351044

Anno accademico 2023/2024

Indice:


JEAN
MONNET
CHAIR
Erasmus+
FUTURE
SIGHT
TOR VERGATA

Abstract

Questa tesina si focalizza sull'analisi delle strategie per lo sviluppo dei siti internet che utilizzano non solo tecniche di *marketing* ma anche elementi di psicologia comportamentale. In particolare si focalizza sul sempre più diffuso utilizzo dei *dark pattern*: una strategia che, unendo concetti di *neuro-marketing*, scienza cognitiva e abitudini comportamentali a pratiche commerciali, induce l'utente a compiere determinate azioni non sempre legali ovvero a rendere più difficile il compimento di altre soprattutto se sfavorevoli per il fornitore del servizio.

Vengono descritte ed analizzate le strategie di programmazione ingannevoli utilizzate nello sviluppo della *user experience* (*UX design*) ed i diversi tipi di *dark pattern* spesso usati anche contemporaneamente per amplificarne l'efficacia e per camuffarne la reale intenzione.

Particolare attenzione viene posta alle recentissime leggi promulgate dal Parlamento europeo e finalizzate a contrastare l'utilizzo delle pratiche scorrette nell'ambito della transizione al digitale. Con il *Digital Service Act* (DSA) sono state infatti stabilite una serie mirata di norme obbligatorie uniformi ed efficaci volte a implementare un ambiente digitale sicuro e affidabile che tuteli in modo concreto i diritti dei consumatori e allo stesso tempo promuova l'innovazione e la competitività.

Al fine di dare un riscontro tangibile e fornire una chiave per decodificare i *dark pattern* presenti in varie forme nei più diffusi siti di commercio ed informazione digitale, vengono altresì presentati casi reali attuali di utilizzo dei *dark pattern* corredati dalle relative sanzioni imposte dagli enti preposti alla tutela dei consumatori e analizzato il caso *Verisure* sanzionata dall'AGCM con una maximulta di 4.250.000 Euro per quattro condotte in violazione del Codice del consumo.

In sintesi, le tecniche di programmazione ingannevoli ed occulte si stanno sviluppando parallelamente alla diffusione globale dei siti di commercio e informazione *online* e con esse le contromisure adottate dalle Istituzioni per limitarne e sanzionarne l'applicazione e la diffusione.

Capitolo 1: *Dark Pattern*: Analisi e Impatto sul comportamento dei consumatori

1.1) Introduzione ai Dark Pattern

Il termine *Dark Pattern* è stato introdotto per la prima volta nel 2010 da Harry Brignull[1] consulente in *User Experience* (UX), un approccio di *design* per siti web che mette l'utente al centro del processo di sviluppo di servizi e prodotti. Lo specialista ha coniato questo termine per spiegare i modi in cui un software può manipolare gli utenti e indurli a scelte sbagliate nella rete internet.

Nel corso degli anni successivi, in seguito all'evoluzione del mondo digitale, si sono sviluppate una serie di ricerche accademiche sull'argomento[2,3,4,5].

I *Dark Pattern* sono il termine inglese per indicare i "modelli di progettazione ingannevoli". Con tale definizione si indicano quelle interfacce e quei percorsi di navigazione progettati per influenzare l'utente affinché intraprenda azioni inconsapevoli o non desiderate - e potenzialmente dannose dal punto della *privacy* del singolo - ma favorevoli all'interesse della piattaforma o del gestore del servizio[6]. Sono di fatto delle pratiche che giocano con il cervello umano, sfruttandone i limiti e gli errori automatici per una manipolazione a fini commerciali. Sono dunque molto diffusi su *social media*, motori di ricerca, siti di *e-commerce*, applicazioni e videogiochi. Possono essere non solo un fastidio ma possono anche ingannare gli

---

[1] H. Brignull, "*Dark Patterns: inside the interfaces designed to trick you*", 2013 https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you; "*Dark Patterns*", https://darkpatterns.org

[2] A. Mathur et al., "*Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*", Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Article 81, 2019, https://dl.acm.org/doi/10.1145/3359183

[3] A. Mathur et al., "*What Makes a Dark Pattern… Dark?*", Proceeding of the Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan, https://dl.acm.org/doi/10.1145/3411764.3445610

[4] T. Kollmer and A. Eckhardt, "*Dark Pattern – Conceptualization and Future Research*", https://doi.org/10.1007/s12599-022-00783-7

[5] D. Kelly and V. L. Rubin, "*Identifying Dark Patterns in User Account Disabling Interfaces: Content Analysis Results*", Social Media + Society January-March 2024: 1–24, DOI:10.1177/20563051231224269

[6] GPDP, "*Modelli di progettazione ingannevoli (Dark Pattern)*", Bus Inf Syst Eng 65(2):201–208 (2023) https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern

utenti, spingendoli verso acquisti impulsivi oppure verso la cessione dei propri dati personali. Si tratta quindi di trucchi di manipolazione psicologica, che sfruttano le debolezze ed i comportamenti umani, e che si fondano su studi di scienza comportamentale e cognitiva.

Il 24 febbraio 2023, il Comitato europeo per la protezione dati (*European Data Protection Board* - EDPB) ha pubblicato le linee guida su come riconoscere ed evitare questi sistemi[7]. 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 macrocategorie riguardo alle quali si può parlare di "modelli di progettazione ingannevoli" che, a seconda delle circostanze, possono essere realizzati attraverso la modulazione del contenuto o dell'interfaccia. La suddivisione è stata fatta sulla base degli effetti provocati verso gli utenti:

1. sovraccarico *(overloading)*: l'utente viene sottoposto ad una grande quantità di informazioni, richieste o opzioni che lo inducono a fornire più dati del necessario oppure a consentire involontariamente al trattamento dei propri dati personali;
2. saltare *(skipping)*: si induce l'utente a saltare alcuni passaggi relativi alla protezione dei dati;
3. agitazione *(stirring)*: influisce sulle scelte degli utenti facendo leva sulle emozioni o attraverso l'impatto visivo delle interfacce;
4. ostruzione *(hidering)*: ostacolare o bloccare gli utenti in vari modi, come ad esempio rendendo delle azioni difficili o impossibili da realizzare;
5. volubilità *(fickle)*: il design dell'interfaccia è incoerente e rende difficile all'utente navigare tra gli strumenti di controllo della protezione dei dati e comprendere lo scopo del trattamento.
6. abbandonati nel buio *(left in the dark)*: l'interfaccia è progettata in modo da nascondere le informazioni e gli strumenti di controllo della *privacy* agli utenti. Risulta *dark* anche l'utilizzo di parole o informazioni ambigue, come ad esempio l'uso del condizionale o di una formulazione vaga, che lascia l'utente incerto

[7] EDPB, "*Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*" 2023, 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

sull'utilizzo dei dati e finalità di raccolta dei dati, oppure l'utilizzo di un linguaggio specifico o tecnico difficilmente comprensibile da un utente medio.

All'interno di ciascuna categoria, rientrano diverse tipologie di *dark pattern* riconducibili, riportate in modo schematico nella Tabella qui sotto.

Categoria	Descrizione	Dark patterns riconducibili
Sovraccarico	Gli utenti ricevono ingenti quantità di richieste, informazioni, opzioni o possibilità. Scopo: spingere gli utenti a condividere più dati o ad acconsentire involontariamente alle attività trattamentali, contro le proprie aspettative.	"Sollecitazioni continue"; "Labirinto della privacy"; "Troppe opzioni".
Salto	Progettazione dell'interfaccia o dell'esperienza utente in modo che quest'ultimo dimentichi o non pensi (in parte o del tutto) agli aspetti riguardanti la protezione dei suoi dati personali.	"Ingannevole intimità"; "Guarda laggiù".
Agitazione	Tecnica che cerca di influenzare le scelte degli utenti, facendo leva sulle loro emozioni o utilizzando spinte visive.	"Guida emotiva"; "Nascosto in bella vista".
Ostruzione	Gli utenti vengono ostacolati oppure bloccati nel processo di informazione o di gestione dei loro dati personali, rendendo tali azioni difficili o impossibili da realizzare.	"Vicolo cieco"; "Più lungo del necessario"; "Azione ingannevole".
Volubilità	Il design dell'interfaccia è progettato in modo incoerente e non chiaro, rendendo difficile per l'utente navigare tra gli strumenti di controllo relativi alla data protection, nonché comprendere lo scopo dell'attività trattamentale.	"Mancanza di gerarchia"; "Decontestualizzazione"; "Interfaccia incoerente"; "Discontinuità linguistica".
Abbandonati nel buio	L'interfaccia è progettata in modo da nascondere le informazioni o gli strumenti di controllo riguardanti la protezione dati, oppure in modo da lasciare gli utenti nell'incertezza rispetto all'attività trattamentale e a quali azioni potrebbero esercitare per la tutela dei loro diritti.	"Informazioni contrastanti"; "Formulazione o informazioni ambigue".

[C. Todaro "*Dark Pattern*: cosa sono e come orientarsi tra i modelli oscuri del web", Data & IT Law 21/03/2023, https://www.smartius.it/data-it-law/dark-patterns-cosa-sono/]

1.2) Tipologie di *Dark Pattern*

A seconda dell'obiettivo, le aziende e i gestori di siti web ricorrono a diversi tipi di *dark pattern*, a volte usati anche contemporaneamente per una maggiore efficacia e per camuffare la reale intenzione.

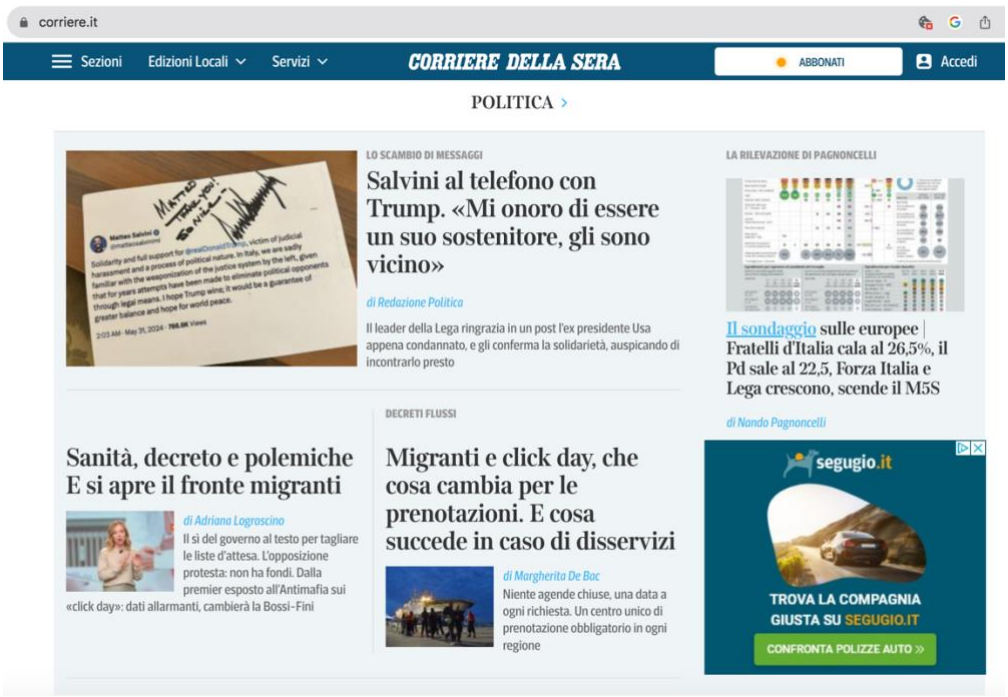
Ad oggi esistono dodici diverse categorie di manipolazione utilizzati nell'*UX design*[8,9], che si incontrano molto frequentemente nell'utilizzo quotidiano della rete:

- *Bait and Switch* (esca e cambia, ossia uno specchietto per le allodole): questo metodo di dark pattern funge come un'esca infatti il visitatore di un sito effettua un'azione online attendendosi un risultato, ma ne riceve un altro.
  È il caso di un sito che pubblicizza un prodotto gratuito o in edizione limitata (*bait*) ma che in realtà è presente in quantità molto bassa oppure non è disponibile e viene sostituito da un'alta offerta, generalmente meno vantaggiosa (*switch*). Visivamente nel sito web si troverà:
  - nella *Home Page* in primo piano un grande banner con la pubblicità dell'annuncio
  - nella pagina del prodotto comparirà un messaggio del tipo: "prodotto esaurito" mettendo però in evidenza un link che riporta a pagine alternative con "prodotti simili" ma aventi prezzi molto più alti e con descrizioni che cercano comunque di convincere l'utente.

  L'utente rimarrà sicuramente deluso ma essendo a quel punto già predisposto all'acquisto del prodotto, potrebbe decidere di procedere con l'ordine di un altro simile pur non essendo la sua scelta iniziale.
- *Disguised Ads* (annunci nascosti): gli annunci pubblicitari sono integrati nel design in modo che l'utente non li riconosca subito come tali; assomigliano infatti al contenuto del resto del sito, o addirittura compaiono come parte della navigazione. Il visitatore si ritrova così a leggere alcuni degli annunci, che solitamente promuovono un prodotto o un servizio.
  Un esempio si trova sul sito web del "Corriere della Sera" nel quale, come mostrato nella figura sottostante, si nota che la pubblicità è posizionata in modo da essere perfettamente integrata nel *layout* del sito portando a non farla distingue a prima vista dai contenuti editoriali aventi anche un *design* simile. Usando questa tecnica ingannevole, si cerca di mascherare la natura pubblicitaria del contenuto integrando visivamente con il resto del sito e facendo sì che gli utenti siano indotti ad interagire con esso credendo sia un contenuto informativo.

[8] H. Brignull, "*Deceptive Patterns Exposing the Tricks Tech Companies Use to Control You*", https://www.deceptive.design, 2023

[9] C. Gray et al., "*The Dark (Patterns) Side of UX Design*", Proceeding of the Conference *CHI 2018,* April 21–26, 2018, Montreal, QC, Canada, DOI: https://doi.org/10.1145/3173574.3174108



- *Forced Continuity* (continuità forzata): si verifica quando un utente si iscrive ad un servizio con una prova gratuita, per cui è necessario fornire i dati della propria carta di credito. Quando la prova gratuita arriva al termine, automaticamente parte la fatturazione del servizio. È un processo *dark* perché le aziende spesso non inviano alcun promemoria per ricordare l'imminente scadenza del periodo di prova e le persone spesso dimenticano di cancellarsi, pagando per qualche mese prima di rendersi conto dell'addebito sulla propria carta di credito. Può anche capitare che le aziende rendano difficile la cancellazione del rinnovo, o che il processo per cancellare l'abbonamento sia molto confuso e macchinoso, facendo sì che l'utente si arrenda e non cancelli l'account.

  È una strategia utilizzata molto frequentemente, anche da piattaforme come *Netflix* e *Amazon Prime*. Questa tipologia di *dark pattern* manipola chiaramente il processo decisionale del cliente, costretto a spendere soldi se non si ricorda di interrompere il servizio dopo il periodo di prova gratuita.
- *Friend Spam* (spammare gli amici): si verifica quando una piattaforma o un servizio online chiede agli utenti il loro indirizzo di posta elettronica in cambio dell'accesso dell'utente ad un altro servizio. Il *dark pattern* accede quindi ai contatti dell'utente ed invia messaggi per attirare l'attenzione oppure per creare nuovi utenti e amplificare così la visibilità dell'azienda.

Questa tipologia sfrutta le connessioni social e si può scomporre in tre macrofasi:

1. durante o dopo la registrazione, all'utente viene chiesto di avere l'accesso ai propri contatti in modo da "connettersi con i tuoi amici";
2. una volta accettata questa condizione, il servizio può automaticamente inviare messaggi a tutti i contatti acquisiti pur non avendo un'esplicita dichiarazione di consenso da parte di quest'ultimi;
3. i messaggi inviati possono sembrare autentici e spingere i destinatari ad iscriversi al servizio in considerazione.

- *Hidden Costs* (costi nascosti): molto spesso i negozi online specificano alcuni costi, come le tasse, le spese di spedizione o di servizio solo nell'ultimo passaggio prima di confermare l'acquisto. Gli utenti solitamente tendono a confermare comunque l'ordine dal momento che hanno già praticamente completato l'intero processo di acquisto pur essendoci stata un'introduzione di costi non trasparenti nel corso del processo.
- *Misdirection* (sviamento o direzione sbagliata): lo scopo di questo dark pattern è quello di sviare l'attenzione dell'utente da un contenuto ad un altro, utilizzando pratiche di design ingannevoli per focalizzare l'attenzione dell'utente su un elemento particolare in modo che trascuri qualcos'altro.
  Un tipico esempio è dato dall'acquisto di un biglietto aereo "Ryanair" dove vengono proposte un'infinità di altri servizi (non banali da evitare), come l'assicurazione di viaggio, acquistata da molti utenti anche se non desiderata solamente perché non è immediato trovare l'opzione di rinuncia.
  Un altro esempio, più visivo, è l'iscrizione all'abbonamento di *Disney Plus*. In questo caso le opzioni meno costose, *Standard* con pubblicità e *Standard*, sono presenti ma con un design meno attraente o addirittura sembrano "non cliccabili" e quindi non disponibili avendo un color petrolio spento e le scritte grigie a differenza della *Premium* che risulta avere l'intera colonna addirittura evidenziata e con il titolo di un celeste acceso, attirando quindi maggiormente l'attenzione. Questa tecnica di depistaggio inganna l'utente e lo influenza nella scelta, portandolo verso un'opzione più costosa e meno conveniente per lui.

- *Price Comparison Prevention* (prevenzione del confronto dei prezzi): si verifica quanto i rivenditori online nascondono i prezzi unitari dei prodotti, rendendo così più difficile il confronto dei prezzi di un prodotto con un altro e impedendo di conseguenza una decisione ponderata ed informata. Questo metodo di *dark pattern* è stato usato dagli operatori di telefonia mobile già all'inizio degli anni 2000.
- *Privacy Zuckering*: questo *dark pattern* prende il nome dal fondatore di *Facebook* poiché inizialmente il *social network* usava di proposito delle impostazioni sulla *privacy* non chiare in modo da raccogliere più dati possibili da parte degli utenti. Gli utenti si ritrovano dunque ad accettare termini e condizioni che permettono alle aziende di vendere i dati ottenuti.
  Il termine è rimasto con questo nome, anche se in seguito il regolamento generale sulla protezione dei dati è cambiato, richiedendo un consenso esplicito per il trattamento dei dati personali.
- *Roach Motel* (motel degli scarafaggi, ossia un alloggio di basso costo): è un dark pattern che permette all'utente di accedere ad una determinata situazione con un percorso estremamente facile ma da cui risulta particolarmente difficile uscire. Un tipico esempio sono gli abbonamenti ad una *newsletter* o ad un servizio, dove l'iscrizione avviene in modo molto semplice e veloce ma la cancellazione risulta praticamente impossibile. Con questa tecnica le aziende riescono a tenere un numero alto di iscritti, anche se non tutti sono realmente interessati. È un processo *dark* perché le aziende cercano di trattenere gli utenti il più a lungo possibile, rendendo difficile la cancellazione o la disattivazione dell'account. Il primo esempio di *Roach Motel* è stato *Skype*, dove per poter

cancellare l'account è necessario contattare il *Customer Service* e non sempre si riesce ad avere la completa disiscrizione.

- *Sneak into Basket* (intruso nel carrello): si verifica al momento del pagamento, quando l'utente si ritrova nel carrello un oggetto o un servizio non richiesto perché le aziende includono automaticamente una casella di controllo che gli acquirenti dovrebbero deselezionare (*opt-out*) per evitare costi e/o prodotti aggiuntivi. Un tipico esempio è l'inserimento di un servizio aggiuntivo come la protezione della privacy o la protezione/assicurazione di un viaggio. Infatti, per manipolare maggiormente l'utente, spesso la casella da deselezionare è preceduta da un messaggio ingannevole del tipo: "goditi il viaggio senza preoccupazioni! L'assicurazione di viaggio ti protegge da eventuali imprevisti". L'unico modo per eliminarli è fare molta attenzione al carrello nella fase conclusiva e deselezionare quanto non richiesto così da pagare solo per i servizi di cui si ha dato un consenso esplicito e cosciente.
- *Trick Questions* (domande trabocchetto): si verifica quando all'utente viene posta una domanda che a prima vista ha un significato, ma letta attentamente in realtà chiede un'altra cosa, non sempre strettamente connessa alla prima interpretazione. Questo accade perché spesso i moduli online utilizzano domande che sono ambigue, sfruttando l'abitudine di leggere molto velocemente le informazioni senza porre troppa attenzione e inducono quindi l'utente ad una risposta sbagliata. Un tipico esempio è l'accettazione dei termini e condizioni di un sito web, dove molto spesso viene automaticamente dato il consenso ad un servizio non richiesto ma di tornaconto per l'azienda che lo promuove.
- *Confirm Shaming* (umiliazione della conferma): è una delle tipologie di *dark pattern* più diffuse e cerca di colpevolizzare l'utente inducendolo a compiere una scelta, come condividere la propria *mail* oppure iscriversi ad una *newsletter*, in un modo che l'alternativa risulti decisamente indesiderabile. È fondamentalmente una manipolazione emotiva, che fa letteralmente provare vergogna in caso di non accettazione dell'offerta.

  Un esempio di questa tipologia è l'abbonamento ad una newsletter con uno sconto su un prodotto, ma con la scelta di rifiutare l'offerta tramite un pulsante con la dicitura "No, non voglio risparmiare".

La comprensione e la consapevolezza delle varie categorie di *dark pattern*, appena analizzate, sono essenziali per gli utenti poiché permettono difendersi e riconoscere

le pratiche manipolative così da non perdere la fiducia nelle piattaforme digitali e viversi al meglio l'esperienza su di esse.

1.3) Effetti dei *Dark Pattern* sul comportamento degli utenti

Gli effetti dei *dark pattern* sugli utenti sono molteplici e riguardano diversi aspetti, sia da un punto di vista etico che comportamentale ma anche giuridico:

a) Aspetto etico: l'utilizzo di *dark pattern* solleva notevoli preoccupazioni etiche, dal momento che risulta ingannevole e manipolativo e pertanto può portare a danneggiare la fiducia e la soddisfazione degli utenti. Nonostante nel breve termine si possano avere molti vantaggi nell'uso di *dark pattern*, questi ultimi possono danneggiare la reputazione di un'azienda e portare addirittura alla perdita di clienti nel lungo termine.

b) Aspetto comportamentale: i *dark pattern* possono essere considerati una violazione della *privacy* e dell'autonomia degli utenti, poiché quest'ultimi vengono indotti in errore, impedendo loro di prendere decisioni consapevoli, con conseguenze negative come spese eccessive, violazioni dei dati o abbonamenti indesiderati. Questi metodi ingannevoli limitano quindi la capacità degli individui di compiere scelte informate, ledendo la loro autonomia e il controllo sui propri dati personali. Inoltre possono essere efficaci nel modellare il comportamento degli utenti, ma anche in questo caso possono portare a risultati negativi, con una diminuzione della fiducia e della soddisfazione degli stessi che si sentono manipolati. I *dark pattern* risultano quindi molto importanti e possono lasciare effetti deleteri sia sui visitatori del sito web che sull'azienda o l'organizzazione che fornisce un servizio rendendo i clienti estremamente frustrati e facendo perdere loro tutta la fiducia in un'azienda. L'esperienza del cliente, così come la fiducia, è uno dei fattori più importanti per la decisione di acquisto e i *dark pattern* rappresentano, essenzialmente, una pessima *customer experience*.

c) Aspetto giuridico: l'utilizzo dei *dark pattern* può portare anche a conseguenze legali: nell'Unione Europea, infatti, il Regolamento Generale sulla Protezione dei Dati (GDPR) vieta l'uso di pratiche di progettazione ingannevoli o manipolative e le aziende trovate in violazione del regolamento possono incorrere in multe e sanzioni significative.

Capitolo 2: Caso studio

2.1) Dalla teoria alla realtà

Negli ultimi anni è aumentata la consapevolezza negli utenti che l'utilizzo della tecnologia possa mettere a rischio i dati personali. Non è infatti raro che per finalità di marketing il principio della trasparenza non venga sempre rispettato. Al contrario è sempre più diffuso l'utilizzo di strategie per lo sviluppo dei siti di *e-commerce* che utilizzano non solo tecniche di *marketing* ma anche elementi di psicologia comportamentale. In sostanza un mix che unisce *neuro-marketing*, scienza cognitiva e abitudini comportamentali, a pratiche commerciali che spesso sono da considerarsi poco etiche. Non si tratta semplicemente di tecniche "ingannevoli" per indurre l'utente a compiere una determinata azione ma di strategie pensate per rendere più difficile il compimento di altre soprattutto se sfavorevoli per il fornitore del servizio. Una volta chiarita la definizione e l'ambito di applicazione dei *dark pattern* con la consapevolezza che si tratta di strategie facilmente identificabili per loro natura, è dunque importante comprendere come queste pratiche trovano utilizzo concreto nel "mondo reale".

2.2) Esempi di utilizzo dei dark pattern

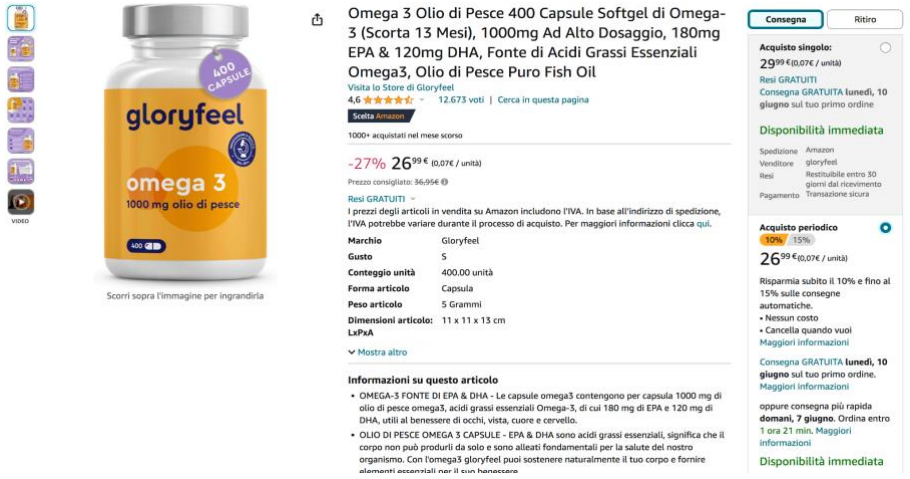
Vengono di seguito presentati brevemente alcuni esempi significativi ed attuali di *dark pattern* e le strategie manipolative utilizzate dalle aziende nonché le rispettive sanzioni ricevute.

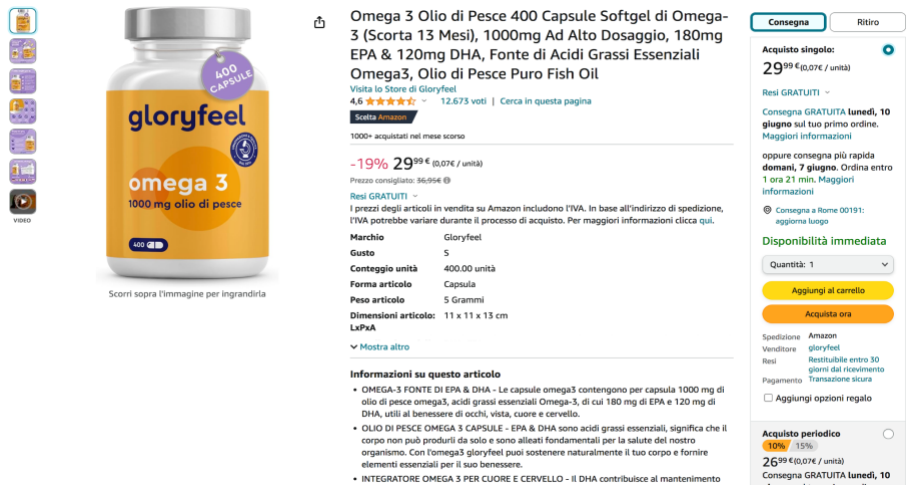
2.2.1) Amazon Italia – AGCM

Un esempio significativo riguarda il caso di *Amazon Italia*. L'azienda è leader mondiale nel commercio online e nel mese di aprile del 2024 è stata oggetto di numerose critiche e sanzioni per l'uso dei *dark pattern*. Nello specifico, come riporta l'Autorità Garante della Concorrenza e del Mercato (AGCM)[10], *Amazon* ha attuato una pratica commerciale scorretta selezionando in automatico l'acquisto periodico per un'ampia selezione di prodotti così che i consumatori ricevessero articoli a intervalli di tempo regolari. Il servizio, che di per sé potrebbe anche risultare conveniente in alcune situazioni, induce gli utenti in errore essendo un servizio selezionato *per default*, predefinito, e modificato dopo anni di "acquisti singoli" avvenuti senza dover

[10] Autorità Garante della Concorrenza e del Mercato (AGCM), https://www.agcm.it/media/comunicati-stampa/2024/4/PS12585

deselezionare nulla. Viene quindi limitata la libertà di scelta dei consumatori che vengono indotti in errore. I clienti di un'azienda *leader* e multinazionale come *Amazon* devono poter effettuare scelte commerciali libere e consapevoli attraverso una pagina web/applicazione chiara e trasparente. L'AGCM[11] delibera che *Amazon* ha effettuato una pratica commerciale scorretta ai sensi degli articoli 10-14-15 del Codice del consumo[12] e per questo conferisce all'azienda una sanzione amministrativa di 10.000.000 di Euro. Un esempio è riportato nelle figure sottostanti: nella superiore è illustrato il prodotto come si vedeva dal sito fino ad inizio 2024, con l'impostazione dell'acquisto periodico come predefinita; nella inferiore è presente quello che effettivamente compare oggi, giugno 2024, dopo la sanzione ad *Amazon*.





[11]Autorità Garante della Concorrenza e del Mercato (AGCM) - Caso Amazon, https://www.agcm.it/dotcmsdoc/allegati-news/PS12585_Amazon_CHIUSURA.pdf

[12] Codice del Consumo, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-09-06;206!vig=

Questo caso evidenzia l'importanza della trasparenza e della correttezza nelle pratiche commerciali online così da garantire ai consumatori di prendere decisioni consapevoli senza manipolazioni.

2.2.2) Low cost airlines - Ministero Consumo spagnolo

Un altro esempio recentissimo (maggio 2024) ed ancora aperto è il caso delle quattro compagnie di volo low cost *Ryanair*, *Vueling*, *Volotea* e *Easyjet* che sono state sanzionate dal Ministero dei Diritti Sociali e del Consumo spagnolo con un'ammenda di 150.000.000 Euro per pratiche illecite e penalizzanti per i consumatori[13].

Si fa riferimento in modo particolare:

- ad informazioni non trasparenti sui prezzi: le compagnie pubblicizzano prezzi di volo molto bassi che non includono una serie di costi aggiuntivi. I consumatori vengono spesso a conoscenza di questi costi occulti solo dopo aver iniziato il processo di prenotazione rendendo il prezzo finale significativamente più alto rispetto al prezzo iniziale pubblicizzato.
- ad addebiti nascosti per servizi essenziali: vengono spesso addebitati costi aggiuntivi per servizi essenziali come il *check-in* in aeroporto, l'assegnazione del posto a sedere e il trasporto di bagagli a mano che i consumatori si aspettano siano inclusi nel prezzo del biglietto.
- difficoltà nel recesso e nella modifica delle prenotazioni. In questo caso le politiche di cancellazione e di modifica delle prenotazioni sono spesso poco chiare e complicate, con costi elevati per i cambiamenti o le cancellazioni dei voli.

Anche questo esempio evidenzia l'importanza della trasparenza e dell'onestà nelle pratiche commerciali, soprattutto in settori come quello delle compagnie aeree *low cost* dove la concorrenza è intensa e i margini sono sottili. Inoltre le sanzioni imposte rappresentano un segnale forte mostrando che le autorità sono pronte a intervenire

[13][https://www.lamescolanza.com/2024/06/03/spagna-multa-di-oltre-150-mln-a-quattro-compagnie-aeree-low-cost-per-pratiche-illecite/];
[https://www.financialounge.com/news/2024/04/24/multa-da-10-milioni-ad-amazon-per-pratica-commerciale-scorretta/?y=401];
[https://finanza.lastampa.it/News/2024/05/31/low-cost-in-spagna-150-milioni-di-multa-a-quattro-compagnie-aeree/MjM5XzIwMjQtMDUtMzFfVExC]

per proteggere i consumatori e garantire pratiche commerciali leali mantenendo una regolamentazione più rigida.

2.3) Caso studio *Verisure*

2.3.1) L'azienda

Verisure[14] è un'azienda multinazionale leader nel settore della sicurezza residenziale e commerciale, specializzata nell'utilizzo di sistemi di allarme con controllo da remoto. Nel 1988 ha infatti sviluppato il primo sistema di allarme collegato 24 ore al giorno per 365 giorni l'anno ad una centrale operativa portando così l'azienda ad essere pioniera nell'innovazione tecnologica e nell'offerta di alta sicurezza. Nel momento in cui viene rilevato un allarme, i professionisti di *Verisure* valutano nel minor tempo possibile la situazione e se lo ritengono necessario, inviano una squadra d'intervento oppure contattano le autorità del posto per garantire la sicurezza dei propri clienti.

È una società in continua crescita ed espansione conta infatti un ritmo di crescita di circa 300 nuovi ingressi l'anno proteggendo ad oggi oltre 5 milioni di clienti in 17 paesi d'Europa e America Latina di cui più di 280.000 sono clienti italiani.

2.3.2) Analisi della sentenza dell'AGCM

Il 18 luglio 2023 è stato avviato il procedimento PS1255815 nei confronti di Verisure Italy S.r.l. "per valutare con riferimento alle condotte poste in essere da Verisure nei confronti dei consumatori, almeno a partire dal 2021". L'azienda è stata sanzionata dall'AGCM (Autorità Garante della Concorrenza e del Mercato) con una maxi-multa di 4 milioni e 250 mila Euro per quattro condotte in violazione del Codice del consumo, riportate qui di seguito.

1. L'ingannevolezza dell'attività promozionale del sistema d'allarme attraverso vari canali di comunicazione (spot televisivi, cartellonistica, sito web, applicazione, canali social etc..). Vi è infatti un'assenza di riferimenti chiari e trasparenti sul fatto che l'impianto di allarme, che viene comprato, è fornito in comodato d'uso gratuito, ovvero un contratto per il quale una parte consegna

[14] *Verisure* - la storia, https://www.verisure.it/su-di-noi/la-nostra-storia
[15] Procedimento PS12558 https://www.agcm.it/dotcmsdoc/allegati-news/PS12558%20chiusura.pdf

all'altra un bene affinché se ne serva per un tempo o per un uso determinato, con l'obbligo di restituire lo stesso bene ricevuto[16], e non in proprietà;

Figura 1.1 – (i) Cartelloni pubblicitari 2021[40] e (ii) 2022[41], (iii) volantino 2021[42]

i-Cartellone pubblicitario 2021

[16] Comodato d'uso gratuito, https://www.agenziaentrate.gov.it/portale/web/guest/schede/fabbricatiterreni/registrazione-contratti-di-comodato/scheda-informativa-registrazione-contratti-comodato#:~:text=Il%20comodato%20d'uso%20gratuito,restituire%20lo%20stesso%20bene%20ricevuto

Figura 1.3 Cartellone pubblicitario

Figura 1.4. Sito Verisure – Homepage (prima schermata) prima dell'avvio del procedimento[45]

Tramite le immagini appena visionate, che sono state usate con fini promozionali, il consumatore è indotto a pensare che il sistema d'allarme sia un acquisto di proprietà e che i pagamenti iniziali per l'attivazione e l'installazione del sistema siano il prezzo per l'acquisto effettivo per prodotto.

Come si può vedere dalle figure sopra riportate, il comodato d'uso è indicato solamente su alcune versioni dei cartelloni, comunicazioni pubblicitarie via web ma con caratteri del tutto illeggibili per la grandezza microscopica e senza esser evidenziati in maniera adeguata. Peraltro negli spot televisivi e su alcuni volantini erano del tutto assenti queste informazioni.
Inoltre il *claim* "offerta speciale - 50% + Telecamera HD Gratis" contribuisce in modo significativo a rafforzare il convincimento che il sistema d'allarme sia un acquisto di proprietà. A seguito dell'intervento delle autorità e del provvedimento, il design per le sponsorizzazioni pubblicitarie è ben diverso infatti come si può notare nella figura sottostante, mette in evidenza che il sistema è in comodato d'uso gratuito.

Figura 4. (i) Nuova cartellonistica settembre 2023 e (ii) nuovo spot televisivo o

(i)

Tenendo conto dell'ingannevolezza e omissività dell'informazione sui mezzi utilizzati di comunicazione, l'AGCM ha sanzionato *Verisure* (su questa singola condotta) con 1.200.000 euro per l'uso di una pratica commerciale scorretta ai sensi degli articoli 20-21-22 del Codice del Consumo[12], che verranno analizzati nel capitolo seguente.

2. La difficoltà all'esercizio del diritto di recesso dal contratto con conseguente pagamento, da parte del consumatore, di un servizio non più richiesto. *Verisure* ostacola la capacità dei consumatori dall'interruzione del contratto tramite ritardi del professionista per lo smontaggio e rimozione del sistema d'allarme,

continuando ad addebitare quote di un abbonamento anche mesi dopo il suo recesso, nonostante sia scritto esplicitamente che “Nelle condizioni generali del contratto di sistema di sicurezza *Verisure* in vigore dal 2020, il recesso esercitato da ciascuna parte sarà efficace decorsi 30 giorni dal ricevimento della relativa comunicazione”. Alla scadenza di questo periodo di preavviso dovrebbe quindi avvenire la fine della fatturazione. In realtà lo smontaggio o disinstallazione è stato effettuato in un periodo di tempo che va tra i 10 e i 200 giorni dalla data di efficacia del recesso, arrivando in qualche caso anche a 500 giorni.

Per i ritardi relativi allo smontaggio che portano una spesa economica onerosa per i clienti, *Verisure* si è giustificato affermando di avere una carenza di personale e che in alcuni periodi, come nel mese di settembre 2022, c’è stato un “picco di recessi”. In questo caso, l’AGCM ha sanzionato l’azienda per la condotta in esame ai sensi degli articoli 20-24-26 del Codice del Consumo[12] con 2.500.000 Euro.

3. L’immediato inizio della fornitura con l’avvio del servizio prima ancora della scadenza dei 14 giorni previsti dalla legge per esercitare il diritto di ripensamento porta confusione ai consumatori sui loro diritti di annullamento senza penali. Più nel dettaglio, nelle Condizioni Generali di Servizio (CGS) del "Contratto di sistema di sicurezza *Verisure*" in vigore fino al 29 ottobre 2023, *Verisure* ha inserito una clausola non conforme al Codice del Consumo (articolo 18 CGS). Infatti, sebbene nella prima parte della clausola il diritto di ripensamento sia stato dichiarato chiaramente al consumatore in termini di forme e contenuti, nella seconda parte non c’è la possibilità di richiedere liberamente l'avvio immediato della prestazione del servizio. La clausola, infatti, prevede che, con la sottoscrizione del contratto, il consumatore autorizzi automaticamente l'inizio della prestazione durante il periodo di recesso previsto (quattordici giorni fino al 2019, e 30 giorni dal 2020 in un’ottica più favorevole per il consumatore), precisando che, in caso di successivo esercizio del recesso, il consumatore si impegna a pagare un importo proporzionale ai servizi forniti fino a quel momento dalla Società.

   La sanzione ricevuta per la condotta appena esaminata è di 500.000 Euro.

4. La scarsa chiarezza ed ambiguità della clausola delle Condizioni generali del "contratto di sistema di sicurezza *Verisure*" dell'indicazione del foro competente in caso di eventuali controversie con consumatore e professionista. Non viene infatti comunicato chiaramente al consumatore che la competenza territoriale appartiene al giudice del luogo di residenza o domicilio del consumatore.

   Per quest'ultima condotta *Verisure* ha ricevuto una sanzione di 50.000 Euro.

Questo caso studio sottolinea l'importanza della comunicazione chiara ed onesta nelle pratiche commerciali per tutti ma soprattutto per un'azienda i cui focus sono la fiducia e l'affidabilità.

Capitolo 3: Regolamentazione e tutela legale contro le pratiche manipolative

I servizi della società dell'informazione ed in particolare i servizi intermediari sono diventati una componente significativa dell'economia dell'Unione europea e della vita quotidiana dei suoi cittadini: i modelli di business ed i servizi nuovi e innovativi, quali i social network e le piattaforme online che consentono ai consumatori di concludere contratti a distanza hanno permesso alle imprese, agli utenti commerciali e ai consumatori di accedere alle informazioni, diffonderle ed effettuare transazioni in modi nuovi. Attualmente la maggior parte dei cittadini dell'Unione utilizza tali servizi quotidianamente. La trasformazione digitale e il maggiore utilizzo di tali servizi hanno tuttavia anche dato origine a nuovi rischi e sfide per i singoli destinatari dei vari servizi, per le imprese e per la società nel suo insieme. Per questo motivo il Parlamento europeo ha emanato un nuovo regolamento finalizzato a stabilire una serie mirata di norme obbligatorie uniformi ed efficaci volte a tutelare e migliorare il funzionamento del mercato interno con l'obiettivo a lungo termine di creare un ambiente digitale sicuro e affidabile, che tuteli in modo concreto i diritti dei consumatori e allo stesso tempo aiuti l'innovazione e la competitività.

3.1) Il Digital Service Act (DSA)

Il "Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo al mercato unico dei servizi digitali (detto anche «Regolamento sui servizi digitali» - *Digital Service Act* o DSA)[17] ha introdotto nell'ordinamento europeo delle norme volte a garantire un ambiente online sicuro, prevedibile e affidabile, in cui i diritti fondamentali degli utenti dei servizi digitali 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 illeciti o nocivi può generare. Rientrano in tale ambito la

[17] "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)", Gazzetta Ufficiale dell'Unione Europea L 277/1 del 27.10.2022 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065

regolamentazione dei *dark pattern* e la trasparenza nel mercato della pubblicità online.

Il DSA[18] è stato definito dalla Presidente della Commissione Europea Ursula von der Leyen come un accordo storico "in termini sia di rapidità che di sostanza".

Con il *Digital Services Act* (DSA, la legge sui servizi digitali) che affianca il *Digital Markets Act* (DMA, la legge sui mercati digitali)[19] viene consacrato il principio che "*ciò che è illegale offline lo deve essere anche online*".

Il DSA è entrato pienamente in vigore il 17 febbraio 2024 e si applica a tutti i fornitori di servizi intermediari. Il nuovo Regolamento era già operativo dal 25 agosto 2023 per i 19 grandi fornitori di servizi digitali, con più di 45 milioni di utenti/mese, identificati come dominanti dello spazio online. Per questi ultimi la responsabilità della vigilanza è della Commissione Europea, che ha già iniziato a muoversi dall'autunno dello scorso anno per valutare possibili infrazioni del *Digital Services Act*. Gli attori principali sono i 2 grandi motori di ricerca (VLOSE: *Very Large Online Search Engines*) *Bing* e *Google Search* e le 17 grandi piattaforme online (VLOP: *Very Large Online Platforms*) quali i *social media* (*Facebook*, *Instagram*, *X-Twitter*, *TikTok*, *Snapchat*, *LinkedIn*, *Pinterest*), i servizi di commercio elettronico (*Alibaba AliExpress*, *Amazon Store*, *Apple AppStore*, *Zalando*), i servizi *Google* (*Google Play*, *Google Maps* e *Google Shopping*) e anche *Booking.com*, *Wikipedia* e *YouTube*.

Dal 2024[20] anche le piattaforme e i motori di ricerca con meno di 45 milioni di utenti/mese sono tenute a rispettare queste indicazioni dell'UE, tra cui i sistemi di profilazione e raccomandazione di contenuti, *privacy* e sicurezza dei minori online, contenuti illegali ed effetti negativi sulla libertà di espressione e di informazione, accesso ai dati per i ricercatori attraverso un meccanismo speciale.

---

[18] DSA, https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package; https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

[19] DMA, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[20] EUnews, https://www.eunews.it/2024/02/16/digital-services-act-in-vigore-ue/#:~:text=Il%20Digital%20Services%20Act%20entrer%C3%A0,primavera%20di%20due%20anni%20fa

Per l'attuazione, il DSA ha istituito una struttura di *governance* ed una nuova architettura di vigilanza europea, di cui la Commissione Europea è l'autorità competente in stretta collaborazione con i coordinatori nazionali dei servizi digitali (per l'Italia l'AGCOM[21]), che sono i diretti responsabili per la vigilanza di piattaforme e motori di ricerca più piccoli.
Un Centro europeo per la trasparenza algoritmica fornirà assistenza a tutti gli attori di vigilanza per valutare se il funzionamento degli algoritmi sia in linea con le linee guida della legislazione comunitaria mentre un Comitato europeo per i servizi digitali fornirà consulenza e assistenza per la corretta applicazione del Regolamento.
Gli utenti dovranno ricevere informazioni "chiare" sul motivo per cui vengono raccomandate loro determinate informazioni e avranno il diritto di rinunciare ai sistemi di raccomandazione basati sulla profilazione (sempre vietata invece per i minori), mentre gli annunci pubblicitari non potranno essere basati sui dati sensibili dell'utente (origine etnica, opinioni politiche, orientamento sessuale). Per quanto riguarda la protezione dei minori, le piattaforme dovranno riprogettare i loro sistemi per garantire un "elevato livello" di *privacy* e sicurezza.
Con l'attuazione del DSA la Commissione UE ha dato impulso alla regolamentazione dei *dark pattern* (modelli di progettazione ingannevoli ovvero interfacce e percorsi di navigazione concepiti per influenzare l'utente, spesso sfruttando pregiudizi cognitivi, affinché intraprenda azioni inconsapevoli o non desiderate, ma convenienti per la piattaforma online) e alla trasparenza nel mercato della pubblicità *online*. Si è dunque entrati in una fase nuova del sistema normativo europeo.
In sintesi, per i temi ritenuti rilevanti sul fronte dei servizi digitali e del mercato digitale, i grandi *player* avranno come interlocutore diretto, costante e *multitasking*, la Commissione UE.

3.1.1) Cosa prevede il DSA riguardo i *dark pattern*

Secondo quanto indicato al punto 67 del DSA, "I *dark pattern* distorcono o compromettono in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate e possono essere utilizzati per convincere i destinatari del servizio a adottare comportamenti indesiderati o decisioni indesiderate che abbiano conseguenze negative per loro". A tal fine, l'obiettivo del Regolamento è quello di impedire alle

[21] AGCOM DSA, https://www.agcom.it/dsa

piattaforme online di ingannare i destinatari del servizio o di distorcerne o limitarne l'autonomia e il processo decisionale, o ancora di condizionare la scelta dei destinatari del servizio attraverso la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa.

Tra i vari articoli del DSA si riportano di seguito quelli ritenuti più significativi e di interesse per la tesina in oggetto:

- L'art. 25 vieta espressamente ai fornitori di piattaforme online di progettare, organizzare o gestire le loro interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi o da falsare materialmente o da compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate.
- L'art. 26 impone alcune misure volte a favorire la trasparenza, prevedendo che ci sia un'indicazione chiara, concisa, inequivocabile ed in tempo reale sul fatto che l'informazione sia una pubblicità, sul soggetto per conto del quale la pubblicità viene presentata, sul soggetto pagante se diverso e sulle informazioni rilevanti sui parametri utilizzati per determinare il destinatario della pubblicità.
- L'art. 27 obbliga il fornitore della piattaforma a inserire nelle condizioni generali del proprio servizio, utilizzando un linguaggio chiaro e intellegibile, i principali parametri utilizzati nei sistemi di raccomandazione ed eventuali opzioni a disposizione dei destinatari del servizio per modificare o influenzare i parametri principali.
- L'art. 52 per cui l'entità delle sanzioni per violazione di questo divieto (come delle altre norme) viene decisa dagli Stati membri. Le norme statali devono stabilire soglie che le rendano effettive, proporzionate e dissuasive. L'importo massimo potrà essere pari al 6% del fatturato annuo mondiale del fornitore di servizi intermediari interessato nell'esercizio finanziario precedente.

3.1.2) Cosa prevede la norma

La norma prevede che la Commissione UE può emanare orientamenti su pratiche specifiche, in particolare:

1. attribuire maggiore rilevanza visiva ad alcune scelte quando si richiede al destinatario del servizio di prendere una decisione;

2. chiedere ripetutamente che un destinatario del servizio effettui una scelta laddove tale scelta sia già stata fatta, specialmente presentando *pop-up* che interferiscano con l'esperienza dell'utente;
3. rendere la procedura di disdetta di un servizio più difficile della sottoscrizione dello stesso.

Il primo punto si riferisce a pratiche di occultamento di informazioni ottenute usando un carattere minuscolo o colori a basso contrasto o inserendo informazioni chiave in un luogo oscuro.

Il secondo punto fa pensare ai tantissimi *pop-up* con inserti pubblicitari da cui non si riesce a uscire quando si naviga.

Il terzo punto sembra invece descrivere il servizio a pagamento *Amazon Prime*, dove fino al 2022 la procedura di cancellazione era decisamente più lunga e meno intuitiva di quella dell'iscrizione.

Nel frattempo, sono state emanate le linee guida del Comitato Europeo EDPB (*European Data Protection Board*)[7] sui modelli di progettazione ingannevoli nelle interfacce dei social media. Sono state individuate un'ampia serie di casistiche, fornito numerosissimi esempi ed indicato un elenco di buone pratiche (febbraio 2023).

L'EDPB raccomanda ai gestori dei *social* di astenersi da comportamenti come *l'overloading*, lo *skipping*, lo *stirring*, *l'obstructing*, il *flickle* e il *left in the dark* descritti inizialmente nel paragrafo 1.1.

3.2) Quadro Normativo nell'ambito della privacy

Nell'ambito della privacy sono presenti altre normative e principi che regolano e violano l'uso dei *dark pattern* su siti web e applicazioni.

Primo tra tutti il GDPR (*General Data Protection Regulation*)[22] un regolamento dell'Unione Europea che disciplina il modo in cui aziende e organizzazioni trattano i dati personali. Gli articoli principali sono:

[22] GDPR, https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

- Articolo 5 per cui i dati devono essere “trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»), raccolti per finalità determinate, esplicite e legittime”
- Articolo 7 il quale si basa sulle condizioni per il consenso che deve essere libero, specifico ed inequivocabile. Il titolare del trattamento deve infatti essere sempre in grado di dimostrare che l’utente ha dato il proprio consenso.
- Articolo 12 per cui le informazioni devono essere date in “forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro”.

Gli articoli appena esaminati del GPDR stabiliscono un quadro rigoroso per garantire che il trattamento dei dati personali avvenga in modo trasparente e lecito, proteggendo gli utenti da pratiche ingannevoli come i dark pattern.
Tuttavia, la protezione degli utenti nell'ambiente digitale è ulteriormente rafforzata da altre normative chiave a livello europeo e nazionale.

Oltre al GDPR, la Direttiva sulle pratiche commerciali sleali 2005/29/CE[23] del Parlamento Europeo e del Consiglio dell’11 Maggio 2005 vieta qualunque pratica commerciale ingannevole che possa quindi indurre i consumatori in errore. La suddetta direttiva “tutela direttamente gli interessi economici dei consumatori dalle pratiche commerciali sleali tra imprese e consumatori.” Essa quindi spinge ad avere una concorrenza leale tra le aziende tutelando infatti in modo indiretto le “attività legittime” da quelle che non rispettano le regole previste dalla direttiva promuovendo così la fiducia e l’equità dei consumatori nel mercato interno dell’UE.
La direttiva fornisce una definizione precisa di ciò che considera azioni ingannevoli:

- una pratica commerciale che contiene informazioni errate, non veritiere o che la sua presentazione inganni un consumatore medio, ad esempio mentendo sulla natura del prodotto, sulla disponibilità, sulla composizione, sulla manutenzione ecc.., portandolo così a prendere decisioni di natura commerciale che probabilmente non avrebbe preso;
- una pratica commerciale che pur avendo presentato tutte le caratteristiche e circostanze, induce comunque l’utente, attraverso ad esempio attività di

[23] Direttiva sulle pratiche commerciali sleali 2005/29/CE, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:it:PDF

marketing, a prendere una decisione di natura commerciale che non avrebbe preso.

Gli stati membri dell'UE sono tenuti a garantire l'applicazione della direttiva e stabilire sanzioni efficaci e proporzionate per eventuali violazioni. È presente una sanzione amministrativa che va dai 5.000 euro ai 500.000 euro in base alla gravità e alla durata della violazione[24].

La Repubblica italiana ha emanato nel 2005 il Codice del Consumo[12], una raccolta di leggi che, come la direttiva sulle pratiche scorrette, sono destinate a tutelare i diritti dei consumatori e a garantire una concorrenza leale nel mercato. Le disposizioni sugli articoli 18, 21 e 23 sono particolarmente rilevanti per contrastare queste tecniche manipolative, garantendo che i consumatori possano prendere decisioni informate e consapevoli:

- l'articolo 18 stabilisce le definizioni fondamentali relative alle pratiche scorrette;
- gli articoli 21 e 23 descrivono e definiscono le pratiche commerciali ingannevoli.

[24] Decreto Legislativo 2 agosto 2007, n. 146, https://leg13.camera.it/parlam/leggi/deleghe/testi/07146dl.htm#:~:text=Con%20il%20provvedimento%20che%20vieta,e%20della%20durata%20della%20violazione

Capitolo 4: Conclusioni

Il tema dei *dark pattern*, ossia l'utilizzo di tecniche di *design* per indurre gli utenti online ad alcune scelte condizionate, è diventato negli ultimi anni sempre più attuale.

I relativi rischi sono stati prontamente valutati dalle Istituzioni. Non si tratta di limitare o reprimere il fenomeno dei *dark pattern* ma di garantire un ambiente *online* sicuro, prevedibile e affidabile, in cui i diritti fondamentali degli utenti dei servizi digitali siano efficacemente tutelati e l'innovazione sia agevolata. L'obiettivo è certamente quello di mantenere alta la fiducia degli utenti e delle imprese verso i nuovi strumenti di commercio ed informazione digitali, contrastando la diffusione di contenuti illegali online e i rischi per la società. La risposta delle Istituzioni è stata repentina ed al passo dei cambiamenti che la transizione al digitale sta apportando nell'intera società tanto che il DSA, approvato subito dopo il parere dell'EDPD, è stato definito dalla Presidente della Commissione Europea Ursula von der Leyen come un accordo storico "in termini sia di rapidità che di sostanza" che ratifica il principio che "*ciò che è illegale offline lo deve essere anche online*".

Bibliografia

[1] H. Brignull, "*Dark Patterns: inside the interfaces designed to trick you*", 2013 https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you; "*Dark Patterns*", https://darkpatterns.org

[2] A. Mathur et al., "*Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*", Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Article 81, 2019, https://dl.acm.org/doi/10.1145/3359183

[3] A. Mathur et al., "*What Makes a Dark Pattern… Dark?*", Proceeding of the Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan, https://dl.acm.org/doi/10.1145/3411764.3445610

[4] T. Kollmer and A. Eckhardt, "*Dark Pattern – Conceptualization and Future Research*", https://doi.org/10.1007/s12599-022-00783-7

[5] D. Kelly and V. L. Rubin, "*Identifying Dark Patterns in User Account Disabling Interfaces: Content Analysis Results*", Social Media + Society January-March 2024: 1–24, DOI:10.1177/20563051231224269

[6] GPDP, "*Modelli di progettazione ingannevoli (Dark Pattern)*", Bus Inf Syst Eng 65(2):201–208 (2023) https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern

[7] EDPB, "*Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*" 2023, 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

[8] H. Brignull, "*Deceptive Patterns Exposing the Tricks Tech Companies Use to Control You*", https://www.deceptive.design, 2023

[9] C. Gray et al., "*The Dark (Patterns) Side of UX Design*", Proceeding of the Conference *CHI 2018,* April 21–26, 2018, Montreal, QC, Canada, DOI: https://doi.org/10.1145/3173574.3174108

[10] Autorità Garante della Concorrenza e del Mercato (AGCM), https://www.agcm.it/media/comunicati-stampa/2024/4/PS12585

[11] Autorità Garante della Concorrenza e del Mercato (AGCM) - Caso Amazon, https://www.agcm.it/dotcmsdoc/allegati-news/PS12585_Amazon_CHIUSURA.pdf

[12] Codice del Consumo, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-09-06;206!vig=

[13] [https://www.lamescolanza.com/2024/06/03/spagna-multa-di-oltre-150-mln-a-quattro-compagnie-aeree-low-cost-per-pratiche-illecite/]; [https://www.financialounge.com/news/2024/04/24/multa-da-10-milioni-ad-amazon-per-pratica-commerciale-scorretta/?y=401];

[https://finanza.lastampa.it/News/2024/05/31/low-cost-in-spagna-150-milioni-di-multa-a-quattro-compagnie-aeree/MjM5XzIwMjQtMDUtMzFfVExC]

[14] *Verisure* - la storia,
https://www.verisure.it/su-di-noi/la-nostra-storia

[15] Procedimento PS12558
https://www.agcm.it/dotcmsdoc/allegati-news/PS12558%20chiusura.pdf

[16] Comodato d'uso gratuito,
https://www.agenziaentrate.gov.it/portale/web/guest/schede/fabbricatiterreni/registrazione-contratti-di-comodato/scheda-informativa-registrazione-contratti-comodato#:~:text=Il%20comodato%20d'uso%20gratuito,restituire%20lo%20stesso%20bene%20ricevuto

[17] "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)", Gazzetta Ufficiale dell'Unione Europea L 277/1 del 27.10.2022
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065

[18] DSA,
https://digital-strategy.ec.europa.eu/it/policies/digital-services-act-package;
https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

[19] DMA,
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[20] EUnews,
https://www.eunews.it/2024/02/16/digital-services-act-in-vigore-ue/#:~:text=Il%20Digital%20Services%20Act%20entrer%C3%A0,primavera%20di%20due%20anni%20fa

[21] AGCOM DSA,
https://www.agcom.it/dsa

[22] GDPR,
https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

[23] Direttiva sulle pratiche commerciali sleali 2005/29/CE,
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:it:PDF

[24] Decreto Legislativo 2 agosto 2007, n. 146,
https://leg13.camera.it/parlam/leggi/deleghe/testi/07146dl.htm#:~:text=Con%20il%20provvedimento%20che%20vieta,e%20della%20durata%20della%20violazione