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 +

STRATEGIE DI MANIPOLAZIONE ONLINE: IL FENOMENO DEI DARK PATTERNS

Chiara Silvani

0349543

Anno accademico 2023/2024

Abstract

Nell'era digitale, la progettazione delle interfacce utente gioca un ruolo cruciale nel determinare come gli utenti interagiscono con i prodotti e i servizi online. Un aspetto emergente e preoccupante in questo campo è rappresentato dai "*dark patterns*", ovvero schemi di design manipolativi creati intenzionalmente per influenzare il comportamento degli utenti in modo ingannevole. Questi schemi, spesso sottili e subdoli, possono indurre gli utenti a compiere azioni che non avrebbero intrapreso volontariamente, come acquistare prodotti indesiderati, iscriversi a servizi non richiesti, o condividere dati personali senza un chiaro consenso.

Attraverso una revisione della letteratura esistente, questa tesina intende sensibilizzare gli utenti e le aziende del settore digitale riguardo ai rischi associati ai *dark patterns*, con particolare attenzione alla raccolta e all'uso dei dati personali. Dopo un'analisi delle diverse tipologie di modelli oscuri, vengono esaminati gli impatti che tali pratiche hanno sul processo decisionale dell'utente. Emerge come queste tecniche, sfruttando i bias cognitivi e le vulnerabilità psicologiche, conducano a scelte apparentemente volute ma, in realtà, fortemente pilotate. In seguito, attraverso una disamina delle normative europee esistenti e delle linee guida etiche proposte per contrastare l'uso dei dark patterns, vengono fornite raccomandazioni pratiche per promuovere un'innovazione tecnologica responsabile e orientata all'utente. Incentivando le aziende ad adottare politiche trasparenti ed educando gli utenti a riconoscere e resistere alle manipolazioni online, è possibile ridurre significativamente la presenza di queste pratiche ingannevoli nelle piattaforme digitali. In un'epoca in cui la fiducia degli utenti è cruciale per il successo delle piattaforme online, garantire un consenso informato e libero rappresenta un passo fondamentale verso un ecosistema digitale più equo e sostenibile.

Indice

Introduzione 4
Capitolo 1 – La tutela del consumatore nell'era digitale 5
Capitolo 2 – I *dark patterns* 7
2.1 Origini e attributi 7
2.2 Classificazione dei *dark patterns* 7
2.3 Modelli ricorrenti 9
Capitolo 3 – L'impatto dei *dark patterns* sul consenso dell'utente 11
3.1 Il processo decisionale in materia di privacy 11
3.2 I bias cognitivi dei *dark patterns* 11
Capitolo 4 – Le strategie di contrasto ai *dark patterns* 14
4.1 Il quadro legislativo 14
4.1.1 Disposizioni del GDPR rilevanti nell'individuazione di *dark patterns* 14
4.1.2 I *dark patterns* nel Digital Service Act 15
4.1.3 L'articolo 5 dell'AI Act 16
4.1.4 Politiche aziendali etiche: *privacy by design e privacy by default* 16
4.2 Educazione dell'utente 17
Conclusioni 19
Bibliografia 20
Sitografia 20

Introduzione

Negli ultimi decenni, l'avvento di Internet e la crescente digitalizzazione delle interazioni umane hanno trasformato profondamente le dinamiche della comunicazione e del commercio globale. Le interazioni digitali sono diventate parte integrante della vita quotidiana, offrendo innumerevoli vantaggi in termini di accesso all'informazione, comodità ed efficienza.

Tuttavia, questo nuovo contesto ha portato con sé non solo opportunità, ma anche una serie di sfide e rischi, tra cui la manipolazione del comportamento dell'utente attraverso tecniche sofisticate ed ingannevoli, note come "*dark patterns*". Tali tecniche possono manifestarsi in varie forme, come l'occultamento di opzioni, l'uso di linguaggio ingannevole e l'ostacolo alla cancellazione di servizi. La loro diffusione è diventata un fenomeno preoccupante nel design delle interfacce digitali, sollevando questioni etiche e legali riguardanti la trasparenza, il consenso informato e la protezione dei consumatori.

Il primo capitolo fornirà una panoramica del tema della tutela del consumatore nel contesto digitale. Nel secondo capitolo verranno esaminate le principali tipologie di *dark patterns* ed alcuni esempi concreti, tratti da siti web e applicazioni reali. A seguire, il terzo capitolo, si concentrerà sul processo decisionale in materia di privacy, analizzando come queste tecniche influenzino le scelte degli utenti riguardo alla condivisione dei propri dati personali, e verranno esaminati i bias cognitivi su cui questi metodi fanno leva. Infine, nel quarto capitolo, verranno discusse le strategie di contrasto, con un'analisi del quadro legislativo esistente e delle iniziative educative volte a sensibilizzare gli utenti sui rischi connessi a tali pratiche.

Capitolo 1 – La tutela del consumatore nell'era digitale

Il tema della tutela giuridica del consumatore non è certo nuovo. Un lungo percorso giurisprudenziale caratterizza già l'evoluzione di tale concetto nel contesto off-line: la figura del contraente-consumatore "debole", in quanto in condizioni di asimmetria informativa nei confronti delle imprese e, più in generale, parte di un rapporto contrattuale con un soggetto dominante, ha ispirato numerose norme sia nella legislazione europea che nazionale.

Con l'avvento delle tecnologie digitali, è emersa una nuova figura, quella del consumatore-utente, che acquista beni e servizi sui mercati online. Certamente questo è visto come un consumatore più evoluto ma che, di fronte alle modalità di funzionamento delle piattaforme digitali, può trovarsi 'disarmato' e privo di strumenti chiari e sufficienti a tutelare la sua posizione, analogamente a quanto accadeva sui mercati tradizionali[1]. È nata quindi la necessità di aggiornare e ampliare le tutele esistenti, includendo nuove forme di protezione per il consumatore digitale, soprattutto in considerazione dello stretto intrecciarsi del tema della tutela dei diritti dell'utente sui propri dati con quello della protezione dello stesso contro le pratiche commerciali scorrette nelle piattaforme online.

Tra le nuove vulnerabilità emergenti in questo ambito, possiamo inquadrare il tema del consenso: molti siti web o servizi digitali, infatti, si basano sul consenso dell'utente finale per l'elaborazione dei dati personali.

In questa prospettiva il primo e finora più rilevante intervento in ambito europeo è il Regolamento Generale sulla Protezione dei Dati (GDPR), che mira a rafforzare la tutela dei diritti dei consumatori nell'era digitale, introducendo nuove regole per garantire la trasparenza e l'equità nel commercio online. Secondo il GDPR, il consenso dell'interessato è una «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento» (art. 4). Inoltre, gli utenti hanno il diritto di accedere ai propri dati, correggerli, cancellarli e limitarne l'uso. Il GDPR si basa, infatti, su diversi principi chiave:

1. Liceità, correttezza e trasparenza: i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

[1] GUERRA G., *L'impatto dei* dark patterns *sul consenso dell'utente: la via europea per affrontare le nuove vulnerabilità*, in *Giustizia civile*, 8, 2022, p. 1-15.

2. Limitazione delle finalità: i dati devono essere raccolti per finalità determinate, esplicite e legittime;
3. Minimizzazione dei dati: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati;
4. Esattezza: i dati devono essere esatti e, se necessario, aggiornati;
5. Limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario rispetto alle finalità per cui sono trattati;
6. Integrità e riservatezza: i dati devono essere trattati in modo da garantire un'adeguata sicurezza, compresa la protezione contro il trattamento non autorizzato o illecito e dalla perdita, distruzione o danno accidentale;

Nei successivi capitoli analizzeremo delle particolari pratiche che possono minare la fiducia degli utenti e violare i principi appena esposti, divenendo delle vere e proprie trappole del consenso.

Capitolo 2 – I *dark patterns*

2.1 Origini e attributi

Con la definizione di "modelli di progettazione ingannevoli" vengono indicate “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”[2]. Detti anche “*dark patterns*”, i modelli di progettazione ingannevoli mirano, dunque, a indirizzare il consumatore verso scelte predeterminate e possono ostacolare la sua capacità di proteggere efficacemente i propri dati personali.

Il termine è stato coniato dallo user experience designer Harry Brignull nel 2010 e da allora è diventato una questione di discussione nel mondo della tecnologia digitale. Harris[3], paragona il potere di manipolazione di queste pratiche al depistaggio di un mago: "… Questo è esattamente ciò che fanno i maghi: danno alle persone l'illusione della libera scelta mentre architettano il menu in modo che vincano loro, indipendentemente da ciò che scegli. … Modellando i menu da cui scegliamo, la tecnologia dirotta il modo in cui percepiamo le nostre scelte e le sostituisce con altre nuove". Dunque, il potere del design manipolativo è tale che le nostre scelte non sempre riflettono le nostre reali preferenze personali.

Queste pratiche sono particolarmente diffuse nel contesto del commercio elettronico, delle piattaforme di social media, e di molte altre applicazioni digitali, dove la competizione per l'attenzione e il denaro degli utenti è feroce.

2.2 Classificazione dei *dark patterns*

Il 24 febbraio 2023, il Comitato europeo per la protezione dati (EDPB) [4] ha pubblicato le linee guida su come riconoscere ed evitare questi sistemi. Il documento offre raccomandazioni

[2] Garante Privacy, “*Dark Pattern (modelli di progettazione ingannevoli”):* https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern

[3] Harris, Tristan. "How technology hijacks people’s minds—from a magician and Google’s design ethicist." *Medium Magazine,* 18, 2016, p. 7.

[4] EPDS, “Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them”, 2022, p. 62 e ss.

pratiche a gestori dei social media, a designer e utenti su come comportarsi di fronte a queste interfacce. In particolare, le linee guida identificano sei macrocategorie di *dark patterns*:

1. **Overloading**: traducibile con "sovraccarico", si ha quando gli utenti vengono bombardati da una grande quantità di richieste, opzioni e possibilità finalizzate a spingerli a condividere più dati possibili e consentire involontariamente il trattamento dei dati personali. All'interno di questa prima categoria rientrano tre tipologie specifiche:
    a. *Continuous prompting:* spingere gli interessati a fornire più dati personali di quelli necessari per la finalità del trattamento;
    b. *Privacy maze:* le informazioni sulla protezione dei dati, anziché essere collocate negli stessi spazi o in spazi vicini, si trovano in diverse schede, traducendosi tutto ciò in disagi per l'utente;
    c. *Too many options*: fornire agli interessati troppe opzioni tra cui scegliere. La quantità di scelte genera negli interessati confusione e rende difficile per essi compiere una decisone consapevole.
2. **Skipping**: si cerca di far dimenticare all'utente qualche aspetto relativo alla protezione dei suoi dati. Rientrano in questa categoria i seguenti due modelli:
    a. *Deceptive Snugness:* prevedere, per impostazione predefinita, l'attivazione delle caratteristiche e delle opzioni più invasive in termini di *data protection* mediante opzioni preselezionate, facendo leva sul fatto che difficilmente gli interessati modificheranno le impostazioni predefinite;
    b. *Look over there*: porre all'attenzione degli interessati un'azione o un'informazione, in grado di distrarlo dalle informazioni o dalle azioni che in prima battuta ricercava.
3. **Stirring**: l'interfaccia è organizzata in maniera tale da agitare o sollecitare l'utente, le sue emozioni e il suo umore. Vi rientrano i seguenti modelli:
    a. *Emotional Stirring:* usare formulazioni o immagini in una prospettiva altamente positiva, cioè, facendo sentire al sicuro l'interessato, o in una altamente negativa, cioè, facendo sentire l'interessato spaventato o colpevole;
    b. *Hidden in plain sight:* utilizzare un visual style in merito alle informazioni e ai controlli che spinga gli interessati verso opzioni meno restrittive e quindi più invasive in termini di *data protection.*
4. **Hindering**: gli utenti si trovano di fronte ad ostacoli o blocchi nel processo informativo e di gestione dei propri dati personali. Ne sono sottocategorie:

a. *dead end*: mancano alcuni link che consentirebbero all'utente di esercitare i propri diritti, o le interfacce sembrano non rispondere ai comandi;
b. *longer than necessary*: che gli interessati sono costretti a fare più passaggi per selezionare opzioni meno invasive rispetto a quanti necessari per l'attivazione delle opzioni più invasive in termini di protezione dei dati personali;
c. *misleading information:* fornire informazioni non in linea con le effettive funzionalità disponibili, spingendo gli interessati a scegliere impostazioni (meno tutelanti) che non intendono scegliere.

5. **Fickle**: l'interfaccia è volutamente poco chiara o poco trasparente. Non vi è un senso logico e l'utente si trova di fronte ad un'interfaccia decontestualizzata. Sono sottocategorie:
   a. *lacking hierarchy:* l'informativa relativa alla protezione dei dati resa all'utente non è suddivisa in sezioni o paragrafi, rendendo difficile l'orientamento nella lettura;
   b. *decontextualising*: si realizza quando un'informazione o la possibilità di controllo della protezione dei dati si trova su una pagina fuori contesto, ha una collocazione non intuitiva.
6. **Left in the dark:** si cerca di spaesare l'utente attraverso interfacce progettate in modo da nascondere una serie di informazioni, oppure gettando incertezza sul trattamento dei dati e sull'esercizio dei diritti. Questa categoria comprende:
   a. *language discontinuity*: fornire le informazioni sul trattamento dei dati personali in una lingua diversa da quella del paese in cui gli interessati vivono, mentre le informazioni sul servizio sono rese in tale lingua;
   b. *conflicting information*: fornire agli interessati pezzi di informazione che in qualche modo sono in conflitto tra loro, ingenerando incertezza e confusione negli interessati;
   c. *Ambiguous wording or information**:*** usare termini ambigui e vaghi, generando negli interessati incertezza su come i dati personali saranno trattati o su come esercitare il controllo sulle informazioni coinvolte.

2.3 Modelli ricorrenti

Analizziamo altri modelli ricorrenti ed interessanti di dark pattern, impiegati dalle diverse piattaforme anche contemporaneamente per amplificare l'effetto desiderato[5]:

[5] Trzaskowski, Jan. "Manipulation by design." *Electronic Markets,* 34.1, 2024, p. 6-8.

- **Friend spam**: un prodotto o un'app chiede all'utente l'accesso ai suoi contatti e-mail o social con il pretesto di cercare amici. Dopo l'approvazione, viene inviato un messaggio dall'indirizzo dell'utente a tutti i contatti per attirare maggiore attenzione sull'azienda o creare nuovi utenti. LinkedIn ha fornito probabilmente l'esempio più eclatante: durante il processo di accesso, LinkedIn chiedeva ai propri utenti di concedere l'accesso ai propri account di posta elettronica con il pretesto di creare una rete più forte per le loro carriere. Dall'indirizzo di posta elettronica di ogni utente sono state poi effettivamente spedite e-mail di invito ai suoi contatti. Nel 2015, LinkedIn ha dovuto pagare 13 milioni di dollari di danni ai propri utenti.
- **Hidden Costs** ("costi nascosti"): i negozi online specificano costi come tasse, costi di spedizione o simili solo nell'ultima pagina prima di confermare l'acquisto. Gli utenti tendono spesso a confermare comunque l'ordine perché hanno già completato l'intero processo di ordinazione.
- **Forced Continuity** ("continuità forzata"): le aziende chiedono ai loro utenti di fornire i dettagli di pagamento quando attivano un abbonamento di prova gratuito. Al termine del periodo di prova, l'abbonamento diventa automaticamente a pagamento senza alcun promemoria. Il processo per cancellare l'abbonamento è spesso molto confuso e macchinoso. Le aziende sperano che l'utente si arrenda e non cancelli l'account.
- **Roach Motel** ("motel di scarafaggi"): l'obiettivo di questo pattern è di rendere per l'utente l'accesso a una determinata situazione il più facile possibile ma anche estremamente complicato uscirne. Le aziende utilizzano spesso questo tipo di dark pattern per gli abbonamenti premium: la possibilità di cancellare questi abbonamenti in modo semplice e veloce è solitamente nascosta e integrata nel sito in modo poco intuitivo per l'utente. Un esempio è dato dal caso Ryanair, che, nel 2010, ha cercato di vendere più assicurazioni di viaggio avvalendosi di questo dark pattern. Durante il processo di prenotazione appariva un campo "Buy AXA Travel Insurance" per il quale non era possibile scegliere tra "Sì" e "No", come accade di solito. L'utente poteva soltanto selezionare il suo paese da un menu a tendina. A prima vista, quindi, sembrava trattarsi di un'assicurazione di viaggio obbligatoria. Solo dopo un esame attento era possibile scoprire l'opzione "No Travel Insurance Required", nascosta tra gli innumerevoli paesi dell'elenco.
- **Confirm shaming** ("umiliazione della conferma"): questo tipo di dark pattern lascia agli utenti una sensazione spiacevole qualora decidano di non utilizzare un determinato servizio. Un esempio è l'abbonamento a una newsletter che concede uno sconto del 15% su un prodotto, ma il pulsante per rifiutare l'abbonamento riporta il testo seguente: "No grazie, non voglio risparmiare".

Capitolo 3 – L'impatto dei *dark patterns* sul consenso dell'utente

3.1 Il processo decisionale in materia di privacy

Gli studiosi della privacy hanno a lungo sostenuto che la maggior parte delle persone prende decisioni razionali sulla divulgazione dei propri dati personali; il loro consenso è dunque un consenso informato. Tuttavia, studi più recenti hanno mostrato come vi siano incongruenze tra le nostre preferenze sulla privacy dichiarate e il nostro effettivo comportamento di divulgazione. Hanno chiamato queste incongruenze il "paradosso della privacy"[6]: gli utenti di Internet affermano un forte interesse per la protezione della propria privacy e allo stesso tempo divulgano informazioni personali sostanziali per magre ricompense.

Oggi abbiamo troppi dati, troppi percorsi di raccolta dei dati e troppa opacità su questi percorsi. In tale contesto, l'informativa sembra non essere in grado di informare gli utenti sulle pratiche aziendali di utilizzo dei dati. Le politiche sulla privacy sono lunghe e imperscrutabili: si stima che un utente impiegherebbe in media 244 ore all'anno per leggere le politiche sulla privacy di ogni sito web che visita, o 54 miliardi di ore all'anno per ogni consumatore degli Stati Uniti per leggere ogni politica sulla privacy che incontra. Pertanto, anche se gli utenti fossero in grado di prendere decisioni razionali in materia di divulgazione, l'incapacità delle politiche sulla privacy di trasmettere adeguatamente le informazioni implica che gli utenti non siano in grado di farlo nella pratica.

Il modello della scelta razionale risulta, dunque, inefficace: gli individui hanno una razionalità limitata, che influisce sulla loro capacità di acquisire tutte le informazioni rilevanti e tradurle in una decisione consapevole. I *dark patterns* sfruttano queste vulnerabilità psicologiche e comportamentali, trasformando gli ambienti online in un'arma per danneggiare i consumatori e la loro privacy.

3.2 I bias cognitivi dei *dark patterns*

I bias cognitivi sono veri e propri errori "semi-automatici" del pensiero in cui il cervello umano incorre facilmente, influenzando le decisioni e i giudizi di ciascuno; sono errori a cui tutti gli esseri umani sono soggetti, indipendentemente dal livello culturale e di istruzione. I bias cognitivi sono utilizzati in correlazione proprio con i *dark patterns* al fine di spingere gli utenti di

[6] Waldman, Ari Ezra. "Cognitive biases, dark patterns, and the 'privacy paradox'." *Current opinion in psychology,* 31, 2020, p. 105-109.

un servizio verso decisioni o scelte apparentemente logiche ed obiettive, ma, in realtà, fortemente condizionate[7]. Esaminiamo i principali ostacoli cognitivi su cui i *dark patterns* fanno leva:

- **Ancoraggio**: si manifesta quando le persone vengono influenzate dalle prime informazioni ricevute ("l'ancora") durante il processo decisionale.
- **Framing**: riguarda il modo in cui un'opportunità viene presentata ai consumatori, vale a dire, come una cosa buona o cattiva. Questo è il motivo per cui le aziende tecnologiche spiegano le loro pratiche di utilizzo dei dati con un linguaggio guidato: "se non consenti i cookie, la funzionalità del sito web sarà ridotta" o "l'opt-in per la raccolta dei dati consentirà nuove e più semplici funzionalità".
- **Sconto iperbolico**: consiste nella tendenza a sovrappesare le conseguenze immediate di una decisione e a "scontare" quelle che si verificheranno in futuro. La divulgazione spesso porta con sé alcuni vantaggi istantanei: comodità, accesso o impegno sociale, per citarne solo alcuni. Ma i rischi della divulgazione di solito si fanno sentire solo molto più tardi.
- **Apatia decisionale:** è la tendenza degli individui a non cambiare le opzioni che sono preselezionate a causa di inerzia.

Sfruttando tali fragilità cognitive, i modelli oscuri hanno l'effetto sostanziale di sovvertire o compromettere l'autonomia, il processo decisionale e la libera scelta dell'utente[8]: gli utenti sono indotti a concedere permessi che, in condizioni di trasparenza, rifiuterebbero. Un consenso estorto con tali modalità è un consenso non informato o forzato, di conseguenza, lesivo dei principi sulla protezione dei dati.

Come già accennato nei precedenti capitoli, secondo il Regolamento europeo sulla protezione dei dati personali, il consenso dell'interessato è una «manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato» (art. 4). Il successivo art. 7 prevede poi che la richiesta di consenso debba essere presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Di conseguenza, se al soggetto interessato non è offerta una reale possibilità di scelta nel decidere se fornire o no il proprio consenso al trattamento o se di fatto lo si obbliga a prestare il proprio consenso, allora tale consenso non sarà considerato come valido, poiché non realmente libero. Più

[7] Mildner, Thomas, et al. "Hell is Paved with Good Intentions: The Intricate Relationship Between Cognitive Biases and Dark Patterns.", 2024, p. 2-7.

[8] Leiser, Mark. "Illuminating Manipulative Design: From" Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive." *Loy. Consumer L. Rev.,* 34, 2022, p. 516-522.

in generale, 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. L'uso di dark pattern per "guidare" gli utenti verso opzioni meno rispettose della privacy è quindi lesivo dei princìpi del GDPR anche sotto questo ulteriore aspetto.

Capitolo 4 – Le strategie di contrasto ai *dark patterns*

4.1 Il quadro legislativo

Un approccio fondamentale per contrastare i *dark patterns* è rappresentato dall'implementazione di un quadro legislativo rigoroso che limiti l'uso di tali pratiche per proteggere i consumatori e promuovere una maggiore trasparenza nelle interazioni digitali.

4.1.1 Disposizioni del GDPR rilevanti nell'individuazione di *dark patterns*

La distinzione tra persuasione e manipolazione è normativa e non sempre facile da stabilire. La differenza sostanziale risiede nell'effetto che tali pratiche hanno sulle preferenze degli utenti: l'obiettivo dei *dark patterns* è quello di far sì che i consumatori ignorino le proprie preferenze e agiscano in modo incoerente con esse; questo è in netto contrasto con gli sforzi del marketing persuasivo che influenza gli utenti a rivedere le loro preferenze. Oltre alle condizioni per il consenso, dettate dall'art. 7 e già discusse nel precedente capitolo, le seguenti disposizioni del GDPR aiutano l'identificazione dei modelli oscuri:

i. **Articolo 5 - *Principi relativi al trattamento dei dati personali*:**
   questo articolo stabilisce i principi fondamentali del trattamento dei dati personali, inclusi il principio di trasparenza, il principio di limitazione della finalità e il principio di accuratezza dei dati. In breve, il trattamento deve essere condotto in modo equo e trasparente nei confronti degli interessati e i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
ii. **Articolo 12 - *Informazioni, comunicazioni e modalità di esercizio dei diritti dell'interessato***:
   «il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni (…) relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori».
iii. **Articolo 15 - *Diritto di accesso dell'interessato***:
   l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai propri dati personali e determinate informazioni, tra cui le finalità del trattamento, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione dei dati personali previsto oppure i criteri utilizzati per determinare tale periodo.

iv. **Articolo 17 - *Diritto alla cancellazione*:**

l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali se sussistono specifici motivi tra cui:

- I dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti o altrimenti trattati.
- I dati personali sono stati trattati illecitamente.
- I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione

v. **Articolo 35 - *Valutazione d'impatto sulla Protezione dei Dati***:

il GDPR richiede che in determinati casi venga condotta un'analisi dell'impatto sulla protezione dei dati prima di intraprendere determinate attività di trattamento degli stessi, in particolare si utilizzano nuove tecnologie che possono comportare un rischio elevato per i diritti e le libertà degli interessati.

Esaminando il comportamento dell'interfaccia utente in relazione ai principi e ai requisiti del GDPR appena elencati, è possibile individuare segnali di *dark patterns* e valutare se vi siano violazioni delle normative sulla protezione dei dati personali.

4.1.2 I *dark patterns* nel Digital Service Act

Il Digital Service Act contiene norme che affrontano esplicitamente i dark pattern[9]: con l'articolo 25 della legge sui servizi digitali l'Unione Europea vieta «…ai fornitori di piattaforme online di progettare, organizzare o gestire le loro interfacce online in modo da ingannare gli utenti, manipolarli o altrimenti distorcere o compromettere materialmente la loro capacità di compiere scelte libere e informate».

In sintesi, il Digital Service Act rappresenta un passo importante verso la creazione di un ambiente digitale più trasparente e sicuro per gli utenti.

[9] Agenda Digitale, "*Divieto di dark pattern nel Digital Service Act"*: *https://www.agendadigitale.eu/mercati-digitali/divieto-di-dark-pattern-nel-digital-service-act-cose-e-cosa-devono-fare-le-aziende/*

4.1.3 L'articolo 5 dell'AI Act

Integrare l'intelligenza artificiale in strategie di progettazione ingannevoli è un fenomeno articolato e complesso. I sistemi AI, per loro natura, sono in grado di elaborare grandi quantità di dati, apprendere da questi dati e prendere decisioni o previsioni basate su di essi. Questa capacità è determinante nello sviluppo e nell'implementazione di tecniche manipolative che possono influenzare sottilmente il comportamento umano[10]. Ad esempio, l'intelligenza artificiale può essere utilizzata per personalizzare l'esperienza dell'utente in modo da influenzare in modo subliminale i processi decisionali; ciò è possibile attraverso algoritmi che analizzano i dati degli utenti per identificare vulnerabilità o tendenze e quindi sfruttarle per intenzioni manipolative.

L'articolo 5 della AI Act costituisce un elemento fondamentale nel contesto della regolamentazione dell'intelligenza artificiale all'interno dell'Unione Europea. Esso stabilisce disposizioni specifiche per garantire che i sistemi AI siano conformi a determinati principi, tra cui trasparenza, accountability e rispetto dei diritti fondamentali degli individui. Nello specifico, l'articolo 5(1)(a) vieta «l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la sua capacità di prendere una decisione informata, inducendo pertanto una persona a prendere una decisione che non avrebbe altrimenti preso, in un modo che provochi o possa provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo».

4.1.4 Politiche aziendali etiche: *privacy by design* e *privacy by default*

Tra gli ulteriori princìpi da considerare nella valutazione dei dark pattern in ambito privacy è poi necessario fare menzione dei princìpi di *privacy by design* e di *privacy by default*[11]. Detti principi sono stati introdotti nel GDPR all'art. 25, il quale impone l'obbligo di avviare un progetto prevedendo da subito strumenti, corrette impostazioni e adeguate misure tecniche ed organizzative a tutela dei dati personali.

Nello specifico l'art. 25 del GDPR prevede che «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure

[10] Leiser, Mark. "Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface." *Journal of AI law and Regulation,* 1.1, 2024, p. 9-17.
[11] CyberLaws, "*Le nuove Linee Guida sui dark patterns: cosa sono e come sono regolamentati": https://www.cyberlaws.it/2022/dark-patterns/*

tecniche e organizzative adeguate (…) volte ad attuare in modo efficace i princìpi di protezione dei dati (…) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

Sinteticamente, con l'espressione "*data protection by design*" si intende, quindi, l'obbligo in capo al titolare di progettare sistemi, prodotti e servizi integrando misure di protezione della privacy direttamente nelle fasi iniziali di design del prodotto o del servizio, anziché aggiungerle successivamente come soluzione a problemi emersi. Ad esempio, un social media potrebbe essere progettato in modo tale da limitare la raccolta e l'elaborazione dei dati personali solo a ciò che è strettamente necessario per fornire il servizio, riducendo così il rischio di abusi dei dati.

Per "*data protection by default*", invece, si intende 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 personali anche se non si attivano autonomamente. Ad esempio, un'applicazione potrebbe rendere le impostazioni di privacy più restrittive per impostazione predefinita, obbligando gli utenti a fare uno sforzo attivo per rendere le proprie informazioni più accessibili.

Integrando i principi di *privacy by design* e *privacy by default*, è possibile, dunque, salvaguardare la privacy e i dati personali delle persone nella misura effettivamente necessaria.

4.2 Educazione dell'utente

Parallelamente alla legislazione, l'educazione digitale è una componente cruciale nella lotta contro i *dark patterns*, poiché fornisce agli utenti gli strumenti e le conoscenze necessarie per riconoscere e resistere alle manipolazioni online. La diffusione della consapevolezza e delle competenze digitali può significativamente ridurre l'efficacia di queste pratiche ingannevoli.

L'integrazione di corsi specifici nei programmi scolastici può educare i giovani, fornendo loro le competenze necessarie per navigare online in modo sicuro. L'educazione è altrettanto importante per gli adulti, molti dei quali non hanno avuto l'opportunità di ricevere un'educazione digitale formale. Offrire corsi di aggiornamento attraverso enti locali, biblioteche pubbliche e organizzazioni non profit può migliorare le competenze digitali della popolazione, rendendola meno vulnerabile alle manipolazioni online. Le campagne di sensibilizzazione sono un altro strumento potente per educare il pubblico sui rischi dei *dark patterns*. Infine, i governi possono lanciare campagne pubbliche attraverso media tradizionali e digitali, raggiungendo un ampio spettro della popolazione.

Gli strumenti tecnologici, come i browser plugin e le estensioni anti-*dark patterns*, rappresentano un ulteriore mezzo per proteggere gli utenti. Questi strumenti possono avvisare gli utenti quando stanno per essere soggetti a un dark pattern, fornendo spiegazioni dettagliate su come e perché il pattern è ingannevole. L'uso di estensioni che bloccano le pubblicità e i contenuti ingannevoli può ridurre significativamente l'esposizione degli utenti a queste pratiche manipolative, contribuendo a un'esperienza online più sicura.

In sintesi, attraverso un'educazione formale nelle scuole, corsi di aggiornamento per adulti, campagne di sensibilizzazione e strumenti tecnologici avanzati, è possibile costruire una comunità di utenti consapevoli e capaci di difendersi dalle manipolazioni online. Questo non solo protegge i diritti dei consumatori, ma contribuisce anche a creare un ambiente digitale più trasparente ed etico.

Conclusioni

L'azione umana e il diritto all'autodeterminazione sono da sempre concetti centrali nella teoria giuridica e nel diritto della protezione dei consumatori, in cui il quadro normativo mira a consentire ai consumatori di agire in conformità con le loro preferenze. Nel corso dell'elaborato abbiamo evidenziato come i *dark patterns* rappresentino una sfida significativa per la tutela dei diritti dei consumatori nell'era digitale: questi schemi manipolativi, progettati per ingannare gli utenti e influenzare il loro comportamento, sollevano importanti questioni etiche e legali. L'impatto dei *dark patterns* sul consenso degli utenti è particolarmente preoccupante: l'illusione del libero arbitrio, generata da scelte apparentemente volontarie ma in realtà pilotate, mina la fiducia degli utenti nei confronti delle piattaforme digitali. Attraverso l'analisi delle diverse normative vigenti, emerge chiaramente uno sforzo crescente da parte delle autorità di vigilanza per arginare questi fenomeni e garantire che gli utenti abbiano un controllo reale sui propri dati personali. Tuttavia, la complessità e la rapidità con cui evolvono le tecniche di manipolazione richiedono un continuo aggiornamento delle normative e una maggiore consapevolezza da parte degli utenti.

L'educazione digitale e la trasparenza dovrebbero essere al centro delle strategie di design delle interfacce utente, promuovendo un ambiente online più equo e rispettoso dei diritti degli individui. Questo include spiegazioni comprensibili delle politiche sulla privacy, delle condizioni d'uso e delle conseguenze di ogni decisione presa online. La trasparenza non solo favorisce la fiducia tra utenti e piattaforme, ma può anche fungere da differenziatore competitivo per le aziende che si impegnano a operare eticamente.

In definitiva, la lotta contro i *dark patterns* richiede uno sforzo congiunto da parte di utenti, aziende e regolatori. Solo attraverso la collaborazione e l'impegno collettivo sarà possibile creare un ecosistema digitale che valorizzi la trasparenza, il rispetto e la fiducia, garantendo così una protezione adeguata dei diritti dei consumatori e una concorrenza leale nel mercato digitale.

Bibliografia

EPDS, “Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them”, 2022, p. 62 e ss.

GUERRA G., *L’impatto dei* dark patterns *sul consenso dell’utente: la via europea per affrontare le nuove vulnerabilità*, in *Giustizia civile*, 8, 2022, p. 1-15.

Harris, Tristan. "How technology hijacks people’s minds—from a magician and Google’s design ethicist." *Medium Magazine,* 18, 2016, p. 7.

Leiser, Mark. "Illuminating Manipulative Design: From" Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive." *Loy. Consumer L. Rev.,* 34, 2022, p. 516-522.

Leiser, Mark. "Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface." *Journal of AI law and Regulation,* 1.1, 2024, p. 9-17.

Mildner, Thomas, et al. "Hell is Paved with Good Intentions: The Intricate Relationship Between Cognitive Biases and Dark Patterns.", 2024, p. 2-7.

Waldman, Ari Ezra. "Cognitive biases, dark patterns, and the ‘privacy paradox’." *Current opinion in psychology,* 31, 2020, p. 105-109.

Trzaskowski, Jan. "Manipulation by design." *Electronic Markets,* 34.1, 2024, p. 6-8.

Sitografia

Agenda Digitale, “*Divieto di dark pattern nel Digital Service Act”*: https://www.agendadigitale.eu/mercati-digitali/divieto-di-dark-pattern-nel-digital-service-act-cose-e-cosa-devono-fare-le-aziende/

CyberLaws, “*Le nuove Linee Guida sui dark patterns: cosa sono e come sono regolamentati”: https://www.cyberlaws.it/2022/dark-patterns/*

Garante Privacy, “*Dark Pattern (modelli di progettazione ingannevoli)”:* https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern