



UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

TESI DI LAUREA

Computer Vision per l'Identificazione di Dark Pattern: Uno Studio Preliminare sull'Identificazione di Sneak Into Basket

PRIMO RELATORE

Prof. Fabio Palomba

SECONDO RELATORE

Dott. ssa Giulia Sellitto

Università degli Studi di Salerno

CANDIDATO

Domenico Antonio Gioia

Matricola: 0512106343

Ogni volta che impariamo qualcosa di nuovo, noi stessi diventiamo qualcosa di nuovo

Leo Buscaglia

Abstract

Come un ragazzino birbantello che vuole i biscotti Oreo che gli hai appena detto che non poteva avere, i designer di dark pattern sono maestri nel far scivolare a tua insaputa articoli nel tuo carrello online. Non ce ne accorgiamo, ma quando ci colleghiamo ad un sito web è come se le nostre azioni siano controllate per compiere scelte che non avremmo fatto. Spesso ci ritroviamo ad acquistare cose che non avremmo voluto avere, a sottomettere abbonamenti, a concedere il consenso al trattamento dei nostri dati personali, ad effettuare azioni sbagliate e molto altro. In netto contrasto con il concetto di privacy e in particolare con la tutela e la protezione dei dati personali degli utenti che navigano sul web, i dark pattern sfruttano la pigrizia dell'utente medio o, semplicemente occultano o rendono poco visibili informazioni importanti. Lo scopo principale di questo studio è quello di sviluppare un algoritmo per l'identificazione automatica del dark pattern *Sneak Into Basket*.

Indice

Indice	ii
Elenco delle figure	iv
Elenco delle tabelle	vi
1 Introduzione	1
1.1 Contesto Applicativo	2
1.2 Motivazioni e Obiettivi	5
1.3 Risultati Ottenuti	6
1.4 Struttura della Tesi	6
2 Stato dell'arte	8
2.1 Tassonomia dei Dark Pattern	8
2.1.1 Nagging	9
2.1.2 Obstruction	10
2.1.3 Sneaking	12
2.1.4 Interface Interferences	14
2.1.5 Forced Action	18
2.2 Influenza dei Dark Pattern	20
2.3 Implicazioni sulla privacy	21
2.4 Rilevabilità dei Dark Pattern	22
2.4.1 Rilevabili Automaticamente	23

2.4.2 Non Rilevabili	23
3 Un approccio basato su computer vision per l'identificazione del dark pattern Sneak Into Basket	25
3.1 Primo Approccio Risolutivo: Analisi del DOM	25
3.2 Secondo Approccio Risolutivo: Classificazione per Immagini	27
3.2.1 Algoritmo di Detection	30
4 Valutazione preliminare dell'approccio	33
4.1 Metodologia	33
4.2 Risultati	34
5 Conclusioni e Sviluppi Futuri	37
Ringraziamenti	38
Bibliografia	39

Elenco delle figure

1.1	Esempio Dark Pattern HBO Max	3
1.2	Esempio Dark Pattern Amazon 1.1	4
1.3	Esempio Dark Pattern Amazon 1.2	4
1.4	Esempio Dark Pattern SportsDirect	5
2.1	Tassonomia di Gray <i>et al.</i> [2018]	9
2.2	Esempio del dark pattern Nagging su <i>Apple</i>	10
2.3	Esempio del dark pattern Roach Motel sul sito <i>BostonGlobe</i>	10
2.4	Esempio del dark pattern Price Comparison Prevention sul sito <i>Linkedin</i>	11
2.5	Esempio del dark pattern Intermediate Currency sull'app <i>Brawl Stars</i>	11
2.6	Esempio del dark pattern Forced Continuity sul sito <i>Audible</i>	12
2.7	Esempio del dark pattern Hidden Costs sul sito <i>ProFlowers</i>	13
2.8	Esempio del dark pattern Sneak into Basket sul sito <i>Kinguin</i>	13
2.9	Esempio del dark pattern Bait and Switch nell'applicazione <i>Candy Crush Saga</i>	14
2.10	Esempio del dark pattern Hidden Information sul sito <i>Booking</i>	15
2.11	Esempio del dark pattern Preselection nell'applicazione <i>KeyFinder</i>	16
2.12	Esempio del dark pattern Toying with Emotion sul sito <i>Delish</i>	16
2.13	Esempio del dark pattern False Hierarchy sul sito <i>Reddit</i>	17
2.14	Esempio del dark pattern Disguised Ad come pubblicità dell'applicazione <i>AccuWeather</i>	17
2.15	Esempio del dark pattern Trick Question sul sito <i>RoyalMail</i>	18
2.16	Esempio del dark pattern Social Pyramid nell'applicazione <i>FarmVille</i>	19

2.17 Esempio del dark pattern Privacy Zuckering nell'applicazione <i>WhatsApp</i>	20
2.18 Esempio del dark pattern Gamification nell'applicazione <i>Candy Crush Saga</i>	21
3.1 Carrello Online del sito Ebay con un prodotto	28
3.2 Carrello Online del sito LanaOnline con un prodotto	28
3.3 Carrello Online del sito Ebay con due prodotti	29
3.4 Carrello Online del sito LanaOnline con due prodotti1	29
3.5 Passi Svolti dall'Algoritmo di Detection	31
4.1 Opzioni di vendita caso di test n°3	36
4.2 Pop-up caso di test n°5	36

Elenco delle tabelle

4.1 Dataset utilizzato per il testing dell'algoritmo	34
--	----

CAPITOLO 1

Introduzione

Molto spesso i termini UI (User Interface) e UX (User Experience) vengono confusi tra loro lasciando intendere che siano simili ma questo è un errore grossolano. Lo scopo della User Experience è migliorare l'esperienza che un utente ha con un'azienda tramite i suoi servizi o prodotti. Infatti, il compito dello User Experience Designer è quello di effettuare un processo di ricerca, test e sviluppo per creare risultati di qualità all'interno dell'esperienza utente. Lo scopo della User Interface coincide con il visual design, e si riferisce alla trasformazione di prototipi costruiti nella fase precedente di User Experience in un'interfaccia visivamente accattivante per gli utenti ovvero la creazione dell'aspetto finale del prodotto. Per poter capire l'importanza di UX e UI basta pensare a cosa succede quando si naviga sul web. Gran parte degli utenti va alla ricerca di uno specifico servizio che possa risolvere un suo problema. Nonostante tutti i siti promuovano gli stessi contenuti, uno soltanto sarà quello che si distinguerà e sarà utilizzato in genere anche in futuro. Questo è scelto perché è sicuramente facile da usare ed ha un'esperienza complessiva piacevole. Rendere il più semplice possibile l'interazione con un sito è una parte fondamentale del processo di sviluppo di qualsiasi prodotto software. Una cattiva UX potrebbe sancire l'abbandono di un prodotto semplicemente perché risulta essere inutilizzabile da un utente. Elemento chiave della UX è l'utente in quanto progettare un'interfaccia senza tenere conto delle esigenze di chi andrà a farne uso può portare solo a risultati negativi. Quindi l'obiettivo principale di qualsiasi UX designer è quello di migliorare e rendere maggiormente usabili i prodotti software.

Rendere usabile un prodotto software significa aumentare in maniera vertiginosa i gua-

dagni dell'azienda. Purtroppo, come succede spesso in ogni contesto, l'aumento dei profitti è sempre uno dei principali argomenti di discussione di un'azienda. Per questo, oltre a rendere usabile un prodotto software si tenta di ingannare l'utente durante l'interazione. A tal proposito vengono utilizzati dei modelli chiamati *dark pattern* che manipolano le scelte di un utente al fine di aumentare i ricavi dell'azienda.

1.1 Contesto Applicativo

I Dark Pattern, chiamati così per la prima volta nel 28 luglio del 2010 da Harry Brignull, designer londinese di UX, sono modelli di design accuratamente disegnati e combinati fra di loro volti a confondere l'utente, con il fine di indurlo a compiere azioni non desiderate, come acquistare beni e servizi, sottoscrivere abbonamenti o ad eseguire procedure talmente complesse da scoraggiarlo da qualsiasi controllo effettivo sui suoi dati personali. Frequentemente, senza accorgerci, eseguiamo azioni rapide e automatiche senza pensare a ciò che esse possono farci incorrere. Quante volte ci è capitato di trovare nel carrello online più prodotti di quelli inseriti, quante volte abbiamo cliccato una "X" di troppo e chissà quante volte abbiamo dato il consenso al trattamento dei nostri dati personali? Ebbene, questi sono solo alcuni esempi di dark pattern che possono essere trovati durante la navigazione del web. Molte sono le varie tipologie che possiamo incontrare, ma lo scopo di essi resta solo uno cioè aumentare i guadagni dell'azienda. Quando desideri annullare l'iscrizione ad una mailing list, ma il pulsante "Annulla iscrizione" è minuscolo, a basso contrasto e nascosto in paragrafi di testo nella parte inferiore di un'e-mail, è un segnale forte che l'azienda sta creando sottili ostacoli tra te e cancellazione. Naturalmente però, non tutti i dark pattern sono progettati in modo dannoso ed alcuni designer di UX potrebbero non essere nemmeno consapevoli di aver costruito un'interfaccia che possa ingannare gli utenti. Ovviamente essere consapevoli dei rischi che i design delle app e siti possono nascondere è la chiave per evitare di cadere vittima dei dark pattern. I siti Web e le app hanno ormai degli standard per indirizzare gli utenti su come eseguire l'attività che desiderano svolgere: fai clic su un'icona X per chiudere qualsiasi finestra aperta; un cerchio rosso informa che è in arrivo una notifica; il colore verde indica uno stato di accettazione e il rosso indica uno di rifiuto; e così via. Se un utente non riesce a capire immediatamente come funziona un'app, è molto probabile che si senta frustrato e smetta di usarla. Quindi, per offrire agli utenti un'esperienza piacevole, i designer UX creano il loro software in modo che sia il più intuitivo possibile.

I problemi insorgono quando l'azienda che realizza l'applicativo ha obiettivi diversi

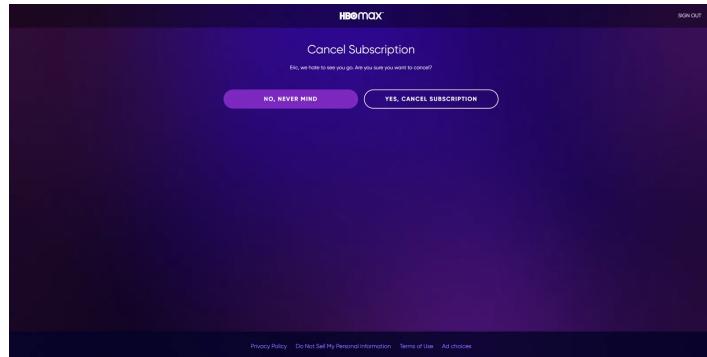


Figura 1.1: Esempio Dark Pattern HBO Max

rispetto alla persona che lo utilizza. Infatti, quando un utente si iscrive ad un servizio di abbonamento con scadenze programmate, la maggior parte delle aziende renderà questo processo del tutto semplice. Invece, se si desidera annullare l'abbonamento, la società potrebbe porre alcuni "ostacoli" per scoraggiare l'azione. A volte possono essere facili da superare, come differenze di colore tra le due opzioni, altre più difficili se si utilizzano giochi di parole. Inerente a questo tipo di dark pattern, il sito di streaming televisivo HBO Max (Figura 1.1) nella schermata di cancellazione all'abbonamento, utilizza due colori differenti per le due scelte possibili. Si può notare che viene impiegato un bottone di colore viola chiaro per poter annullare la disiscrizione ed uno viola scuro per confermarla. Potrebbe sembrare una cosa da poco, ma la maggior parte degli utenti probabilmente sceglierà il pulsante corretto su cui fare clic. Ma se anche un piccolo numero di utenti non presta attenzione e mantiene i propri abbonamenti quando non lo desidera, ciò può significare denaro aggiuntivo per l'azienda.

In alcune situazioni, gli ostacoli all'esecuzione di un comportamento dannoso per le aziende possono essere sorprendentemente difficili. Se vuoi chiudere il tuo account Amazon (Figura 1.2), ad esempio, devi contattare direttamente Amazon e chiedere all'azienda di farlo. Non puoi farlo da solo. E troverai le istruzioni in una pagina di guida che ti mostrano tutti i motivi per cui non dovrresti fare questa scelta. Se si procede, Amazon chiede la compilazione di un modulo che deve essere inviato tramite mail con le motivazioni di chiusura dell'account. L'azienda poi risponde con un'e-mail automatizzata contenente tutti i motivi per cui non si debba cancellare l'account. Se si è davvero sicuri, allora si può fare click su un altro link nascosto in fondo alla e-mail che rinvia ad un'altra pagina nella quale si può effettivamente mandare la richiesta di cancellazione definitiva dell'account. Una sequenza di azioni per svolgere una semplice operazione.

Un altro modello spesso utilizzato è il cosiddetto "Confirm Shaming" in cui un'opzione di rifiuto viene mostrata in modo che l'utente possa provare addirittura vergogna nello

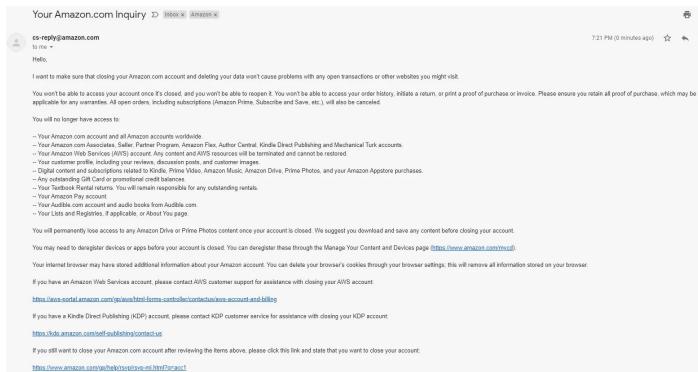


Figura 1.2: Esempio Dark Pattern Amazon 1.1



Figura 1.3: Esempio Dark Pattern Amazon 1.2

sceglierla. Solitamente questa tecnica è impiegata per convincere le persone ad iscriversi a mailing list oppure quando si tenta di uscire da un sito. Ancora una volta, Amazon ha utilizzato anche quest'ultimo tipo di dark pattern. In Figura 1.3, l'azienda cerca di convincere gli utenti ad acquistare l'edizione Kindle di un libro rispetto alla classica servendosi di frasi derisorie. Con molte probabilità un utente distratto sarà sicuramente coinvolto nell'acquisto.

Un particolare modello, chiamato *Sneak Into Basket*, è impiegato per intrufolare oggetti non richiesti nel carrello online senza che l'utente se ne accorga. Naturalmente a seconda di quale oggetto sia inserito, diverso è il rischio per l'utente. Aggiungere un prodotto di costo elevato ha sicuramente un rischio maggiore rispetto ad uno dal costo inferiore. Generalmente vengono inseriti prodotti dal basso costo, così che un utente disattento effettua l'acquisto senza controllare il prezzo del carrello finale. Tale tecnica è impiegata dal sito SportsDirect (figura 1.4) il quale in ogni carrello aggiunge una rivista.

I dark pattern sono tanti e ognuno ha diversi rischi e pericoli per gli utenti. A livello giuridico, essi sono essenzialmente in un limbo e molto spesso rimangono impuniti. Il caso più famoso è quello di LinkedIn, che ha ricevuto una multa da 13 milioni di dollari per

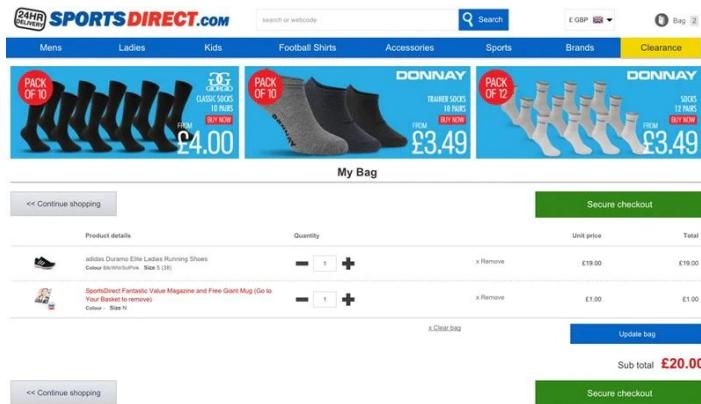


Figura 1.4: Esempio Dark Pattern SportsDirect

aver utilizzato un dark pattern, chiamato "Friends Spam", che forzava l'invito dei contatti dell'utente alla piattaforma. Intanto in molti stati, sono in discussione varie proposte di legge per proibire la creazione di interfacce atte a manipolare le decisioni delle persone. Quando si tratta di dark pattern, le aziende hanno un team variegato di persone dedito a sperimentare quali tecniche ottengono la risposta più desiderabile per l'azienda e non per il cliente. L'unica arma contro tali manipolazioni resta l'istruzione e la conoscenza di questa tematica. Infatti, Brignull in una conferenza dice: *If you know what cognitive biases are and the kind of tricks that can be used to change your mind to persuade you to do things, then you're less likely to have them trick you.* Inoltre, il designer londinese invita a chiamare pubblicamente le aziende, in quanto lamentarsi a voce alta è sicuramente una delle opzioni migliori per contrastare questo fenomeno. Se le lamentele sono pubbliche, molto probabilmente le risposte saranno rapide ed efficienti. I dark pattern sono ovunque e sebbene non tutti i tentativi di manipolazione sono dannosi per l'utente, resta importante essere consapevoli ed informati in quanto non sempre gli interessi dell'azienda sono in linea con i propri. Per alcune società, se possono indurti con l'inganno a fare qualcosa che altrimenti non faresti, lo faranno.

1.2 Motivazioni e Obiettivi

Indurre l'utente con l'inganno a fare cose che altrimenti non avrebbe fatto, è l'obiettivo che molte aziende si pongono per incrementare i loro guadagni. Molte tipologie di dark pattern, infatti vengono utilizzate per tale scopo e molti sono gli utenti disattenti che ne restano vittima. Non limitandoci a pensare alla singola persona, se per ciascun utente viene aggiunto un prodotto nel carrello del costo irrisorio di un euro, l'azienda aumenterà in maniera sostanziosa i suoi guadagni. Molte volte, i consumatori si ritrovano a casa riviste,

articoli correlati ad altri già acquistati precedentemente e altro senza neanche accorgersene.

Perché lasciar fare questo alle aziende? La motivazione di base che spinge questo studio, infatti, è quella di preservare il portafoglio degli utenti da truffe che possono incorrere nel web. Le truffe economiche sono di vario tipo, ma questo lavoro si incentra sull'identificazione di istanze del dark pattern di tipo Sneak Into Basket che è paragonabile al commesso di supermercato che inserisce prodotti nei carrelli della spesa all'insaputa dei clienti. L'obiettivo di questo studio è infatti la creazione di un algoritmo intelligente che possa determinare se un sito implementa o meno il dark pattern Sneak Into Basket.

1.3 Risultati Ottenuti

L'algoritmo creato si basa su computer vision poiché prende in input delle immagini sulle quali si sono sperimentate simulazioni. Uno screenshot effettuato sulla pagina del carrello di un sito web è analizzato al fine di ricavare il numero di prodotti presenti in esso. Se sono contenuti più di un prodotto significa che la pagina implementa un'istanza di Sneak Into Basket. I dettagli dell'algoritmo sono presenti nel capitolo 3.2 del suddetto documento. Una volta creato l'algoritmo non ci tocca che determinare la sua efficacia. Per stabilire l'accuratezza è stato testato su un dataset ideato da Mathur *et al.* [2019] contenente esempi di siti che utilizzano il dark pattern Sneak Into Basket. Per ogni caso di test sono riportati al capitolo 4.2, il motivo di successo o di insuccesso dell'algoritmo nell'identificazione del dark pattern. Dopo un'attenta analisi dei risultati, possiamo ritenere che sommariamente il funzionamento dell'algoritmo è corretto. I casi in cui esso riporta risultati inesatti sono principalmente due: quando durante l'aggiunta al carrello di un prodotto viene richiesta la compilazione di varie opzioni di vendita, e quando al momento dell'esecuzione dello screenshot al carrello è presente un pop-up che oscura la visualizzazione degli elementi al di sotto di esso. Possiamo concludere osservando che l'algoritmo ha un funzionamento corretto nel 60% dei casi, e può essere ritenuto un ottimo risultato per un algoritmo nato da uno studio preliminare sul dark pattern Sneak Into Basket. I casi di insuccesso sono un ottimo punto di partenza per un successivo miglioramento dell'attuale versione dell'algoritmo.

1.4 Struttura della Tesi

La tesi è strutturata nel seguente modo:

- **Introduzione** - È introdotto il termine dark pattern e le motivazioni per le quali è stato scelto come argomento di tesi.
- **Stato dell'Arte** - È riportata una descrizione dei vari tipi di dark pattern suddivisi secondo la tassonomia ideata da Harry Brignull; Viene discusso il problema della violazione della privacy degli utenti; È mostrata la suddivisione dei dark pattern in base al loro tipo di rilevabilità.
- **Un approccio basato su computer vision per l'identificazione del dark pattern Sneak Into Basket** - Viene studiato in maniera approfondita il dark pattern Sneak Into Basket; Viene mostrata la creazione di un algoritmo che lo identifichi.
- **Valutazione preliminare dell'approccio** - Sono riportati i risultati dei vari test effettuati per stimare l'efficacia dell'algoritmo.
- **Conclusioni e Sviluppi Futuri** - Sono riportate le conclusioni e i possibili sviluppi futuri che potrebbero sorgere dopo la creazione dell'algoritmo.

CAPITOLO 2

Stato dell'arte

2.1 Tassonomia dei Dark Pattern

Harry Brignull [2010], designer londinese, ha raccolto e classificato una serie di esempi di dark pattern sul proprio sito www.deceptive.design. Tale sito è organizzato in più sezioni, di cui le più importanti sono: *Hall Of Shame* e *Types of Dark Patterns*. La prima contiene una lista in continuo aggiornamento di segnalazioni effettuate da utenti, tramite l'applicazione *Twitter*, che individuano l'utilizzo di dark pattern all'interno di siti o applicazioni. La seconda comprende l'elencazione della tassonomia ideata dallo stesso Brignull che prevede la divisione dei dark pattern in 12 categorie distinte. Con lo scorrere degli anni, un gran numero di studi ha ampliato questa tassonomia in modo da permettere la comprensione di altri modelli di dark pattern.

I primi studiosi che hanno ampliato la tassonomia di Brignull sono Conti e Sobiesk [2010] che hanno previsto una suddivisione formata da 11 categorie e 20 sottocategorie di tecniche di progettazione di interfacce dannose che manipolano, sfruttano o attaccano gli utenti. Tra le categorie, quelle più rappresentative sono: *Distraction* che consiste nell'utilizzo di colori ed animazioni lampeggianti con lo scopo di attirare l'attenzione dell'utente e distrarlo e *Forced Work* che consiste nel costringere l'utente ad effettuare un'operazione come guardare un annuncio pubblicitario.

Bösch *et al.* [2016] hanno presentato una tassonomia intitolata "Dark Strategies" contenente otto modelli oscuri specifici della privacy. In tale classificazione vengono mostrati nuovi

NAGGING	OBSTRUCTION	SNEAKING	INTERFACE INTERFERENCE	FORCED ACTION
 <p>NAGGING Redirection of expected functionality that persists beyond one or more interactions.</p>	 <p>OBSTRUCTION Making a process more difficult than it needs to be, with the intent of dissuading certain action(s).</p>	 <p>SNEAKING Attempting to hide, disguise, or delay the divulging of information that is relevant to the user.</p>	 <p>INTERFACE INTERFERENCE Manipulation of the user interface that privileges certain actions over others.</p>	 <p>FORCED ACTION Requiring the user to perform a certain action to access (or continue to access) certain functionality.</p>

Figura 2.1: Tassonomia di Gray *et al.* [2018]

modelli come *Forced Registration* che consiste nel richiedere la registrazione dell'account per accedere ad alcune funzionalità e *Hidden Legalese Stipulations* che consiste nel nascondere informazioni dannose in lunghi termini e condizioni. Il linguaggio corposo e lungo che viene utilizzato in molte politiche sulla privacy è probabilmente anch'esso "dark" dal momento che sconforta gli utenti dalla lettura, ostacolandone la comprensione.

La più recente tassonomia è stata proposta nel 2018 da Gray *et al.* [2018] (Figura 2.1), alla Conference on Human Factors in Computing Systems. Essi partendo da ricerche effettuate su blog e social media hanno riformulato quella originariamente creata da Brignull, rendendola più chiara ed estesa, e adattando il significato di alcuni pattern in base al tipo di utente a cui sono rivolti. Tale classificazione è formata da 5 categorie di dark pattern: *Nagging*, *Obstruction*, *Sneaking*, *Interface Interferences* e *Aesthetic Manipulation*.

2.1.1 Nagging

Tale pattern si manifesta con l'interruzione di un'attività utente con l'avvio di uno o più task non direttamente collegati al suo intento originale. La presenza di Nagging si può manifestare con pop-up che oscurano l'interfaccia, pubblicità improvvise a schermo intero oppure qualunque altra cosa che tenta di spostare il focus dell'utente. Come è possibile notare dall'esempio in Figura 2.2, viene mostrato un pop-up che incoraggia l'utilizzo del browser *Safari* interrompendo l'attività che sta svolgendo l'utente. Inoltre, all'interno del pop-up non è presente un'opzione per evitare lo scaricamento del browser per cui successivamente il pop-up sarà nuovamente mostrato.



Figura 2.2: Esempio del dark pattern **Nagging** su *Apple*

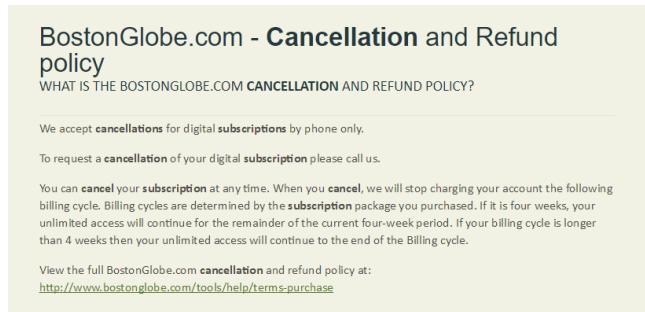


Figura 2.3: Esempio del dark pattern **Roach Motel** sul sito *BostonGlobe*

2.1.2 Obstruction

Si tratta di un “ostacolo” che viene inserito durante l’esecuzione di una determinata attività, con l’intento di dissuadere l’utente dallo svolgimento dell’attività stessa. La categoria Obstruction include i dark pattern *Roach Motel*, *Price Comparison Prevention*, e *Intermediate Currency* definiti da Brignull.

Roach Motel

L’interfaccia utente rende molto facile entrare in una determinata situazione, da cui è particolarmente difficile uscire. L’idea è quella di rendere estremamente facile iscriversi a servizi, ma difficile o addirittura impossibile disiscriversi. Come è possibile notare dall’esempio in Figura 2.3, un utente per disiscriversi dai servizi forniti dal sito *BostonGlobe* dove recarsi alla sezione FAQ per poi effettuare una chiamata al servizio clienti.

Price Comparison Prevention

Quando questo dark pattern è presente, è reso difficile il confronto del prezzo di un articolo con un altro, in modo da impedire all’utente di informarsi per prendere una decisione. L’idea è quella di mostrare informazioni limitate di un prodotto, o rendendo il testo non copiabile, in modo da contrastare la ricerca di esso su altri siti di vendita. Un esempio di questo dark pattern, mostrato nella Figura 2.4, è stato individuato sul sito *Linkedin*, in cui

Career Get hired and get ahead	Business Grow and nurture your network	Sales Unlock sales opportunities	Hiring Find and hire talent
<ul style="list-style-type: none"> Stand out and get in touch with hiring managers See how you compare to other applicants Learn new skills to advance your career Select plan	<ul style="list-style-type: none"> Find and contact the right people Promote and grow your business Learn new skills to enhance your professional brand Select plan	<ul style="list-style-type: none"> Find leads and accounts in your target market Get real-time insights for warm outreach Build trusted relationships with customers and prospects Select plan	<ul style="list-style-type: none"> Find great candidates, faster Contact top talent directly Build relationships with prospective hires Select plan

Figura 2.4: Esempio del dark pattern Price Comparison Prevention sul sito *LinkedIn*



Figura 2.5: Esempio del dark pattern Intermediate Currency sull'app *Brawl Stars*

nella vista di tutti i piani tariffari non viene mostrato il costo di ciascuno di essi. Ciò rende molto più facile ad un utente accettare accidentalmente un prezzo che non è effettivamente disposto a pagare.

Intermediate Currency

Gli utenti sono spinti a spendere soldi veri per acquistare una valuta virtuale (esempio gemme) per utilizzare un servizio o fare acquisti online. L'obiettivo principale di tale dark pattern è quello di confondere l'utente sul valore reale del servizio in modo che egli interagisca in modo differente con la valuta virtuale. Molto spesso questo pattern è presente nei videogiochi dove è possibile effettuare acquisti in-app, e in cui congiuntamente alla valuta virtuale vengono utilizzate esposizioni confusionarie sui beni che si vanno ad acquistare. Lo scopo di questo dark pattern è quello di disconnettere gli utenti dal valore reale dei soldi spesi, il che può far sì che gli utenti spendano la valuta virtuale in modo diverso rispetto a quanto farebbero con denaro reale. Nell'esempio mostrato in Figura 2.5, il pattern è rilevato nell'app *Brawl Stars* in cui tramite "gemme" si ha la possibilità di acquistare nuovi personaggi.

Start your free 30-day trial

- ✓ Free membership for 30 days with 1 audiobook + 2 Audible Originals.
- ✓ After trial, 3 titles each month: 1 audiobook + 2 Audible Originals.
- ✓ Roll over any unused credits for up to 5 months.
- ✓ Exclusive audio-guided wellness programs.

[Click to Try Audible Free](#)

\$14.95 per month after 30 days. Cancel anytime.



Figura 2.6: Esempio del dark pattern **Forced Continuity** sul sito *Audible*

2.1.3 Sneaking

La categoria **Sneaking** include le sottocategorie *Forced Continuity*, *Hidden Costs*, *Sneak into Basket* e *Bait and Switch* definite da Brignull. È una categoria di dark pattern che include strategie per mascherare o ritardare la comunicazione di informazioni che risultano essere importanti per l'utente. L'obiettivo di queste tecniche è quello di far eseguire ad un utente azioni non desiderate che non avrebbe compiuto se avesse avuto conoscenza delle informazioni che gli sono state nascoste.

Forced Continuity

Tale dark pattern si verifica quando la scadenza di servizio viene raggiunta, o quando la prova gratuita di esso termina, ma il rinnovo dell'abbonamento continua ad essere addebitato all'utente automaticamente senza preavviso. Come mostrato in Figura 2.6, il dark pattern è rilevato sul sito *Audible* in cui è prevista la possibilità di iscrizione ad un periodo di prova gratuito che sarà seguito da un'attivazione di un abbonamento mensile se tale servizio non sarà disdetto.

Hidden Costs

Un prodotto o un servizio viene "pubblicizzato" con un prezzo, al quale però successivamente vengono aggiunti ulteriori costi come tasse, commissioni o costi di spedizione elevati. Un utente distratto si ritroverà ad acquistare il servizio ad un prezzo maggiori rispetto a quello che le era stato inizialmente proposto. Tale dark pattern, come mostrato in Figura 2.7, è possibile ritrovarlo sul sito *ProFlowers* in cui al momento dell'inserimento di un prodotto al carrello vengono aggiunti ad esso altri costi come quello di spedizione e di "cura e trattamento".

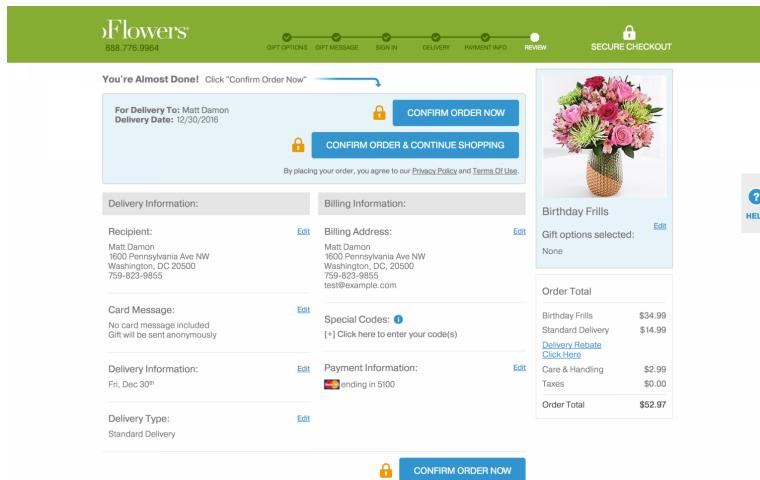


Figura 2.7: Esempio del dark pattern **Hidden Costs** sul sito *ProFlowers*

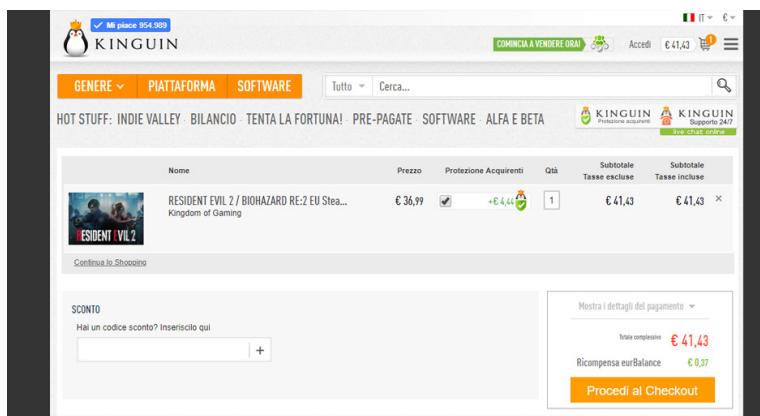


Figura 2.8: Esempio del dark pattern **Sneak into Basket** sul sito *Kinguin*

Sneak into Basket

Generalmente questo tipo di dark pattern si ritrova quando i servizi cercano di aumentare ulteriormente i loro ricavi, aggiungendo prodotti o servizi non scelti dall’utente al suo carrello online. L’inserimento di questi prodotti aggiuntivi è spesso giustificato come suggerimenti correlati a prodotti acquistati precedentemente o al prodotto attualmente presente in carrello. Ciò può indurre un utente distratto ad acquistare involontariamente questi articoli, a meno che non se ne accorga prima dell’effettivo acquisto. Il prodotto extra aggiunto al carrello è quasi sempre un oggetto non fisico. Ad esempio, nel famoso sito di acquisto di giochi online *Kinguin*, come mostrato in Figura 2.8, al momento dell’acquisto viene messo il check automatico su una clausola che porta all’acquisto della “protezione acquirenti”. Altre volte può essere aggiunta un’assicurazione su un biglietto aereo, una tassa di imballaggio aggiuntiva e così via.



Figura 2.9: Esempio del dark pattern **Bait and Switch** nell'applicazione *Candy Crush Saga*

Bait and Switch

Questo tipo di dark pattern è ritrovabile quando un utente si propone di fare una cosa, ma invece accade qualcosa di indesiderato: ad esempio un pulsante “X” rosso esegue un’azione diversa dalla chiusura di una finestra pop-up. Tale tecnica inoltre abitua un utente a compiere una determinata azione e quando l’abitudine prende il sopravvento, l’azione risultante è completamente diversa da quella desiderata. Tale pattern è riconoscibile, come mostrato in Figura 2.9, nell’applicazione *Candy Crush Saga*, nella quale dall’inizio un utente è abituato a cliccare un “grosso bottone” al centro dello schermo per svolgere azioni importanti come iniziare una partita o continuare un livello. Dopo un certo numero di partite, entrerà in gioco il dark pattern perché ora quel “grosso bottone”, se cliccato, indirizzerà l’utente al negozio dell’app.

2.1.4 Interface Interferences

Questa categoria comprende tecniche di manipolazione dell’interfaccia che limitano la possibilità dell’utente di capire che può effettuare determinate azioni. L’utente viene così confuso spingendolo ad effettuare determinate azioni invece che altre. In tale categoria rientrano i dark pattern denominati: *Hidden Information*, *Preselection*, *Aesthetic Manipulation* e *Trick Question*.

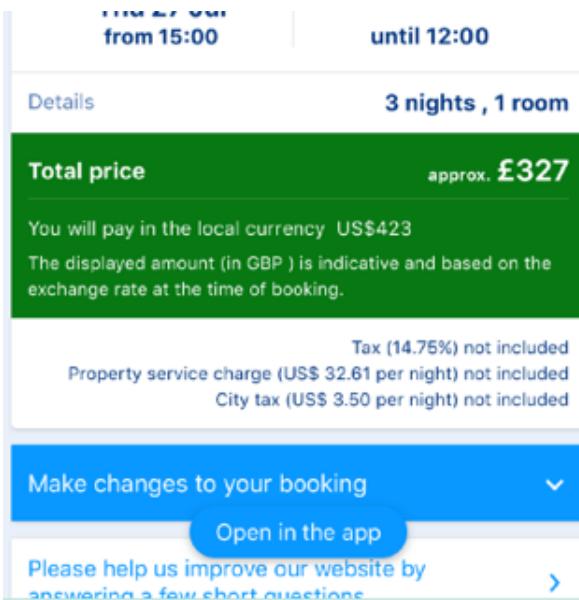


Figura 2.10: Esempio del dark pattern **Hidden Information** sul sito *Booking*

Hidden Information

L’obiettivo di questo dark pattern è quello di far passare informazioni rilevanti come irrilevanti. Si tratta di informazioni che non sono rese note all’utente attraverso contenuti nascosti, testo scolorito o di piccole dimensioni. Questa tecnica, come mostrato in Figura 2.10, è ritrovabile sul sito *Booking* in cui l’occhio dell’utente è attratto dal grande “Prezzo Totale” evidenziato con uno sfondo verde. Questo prezzo, tuttavia, non include le tariffe elencate di seguito nella sezione non evidenziata. Questo induce l’utente a credere di pagare un prezzo inferiore a quello che è realmente proposto.

Preselection

Tale dark pattern è ritrovabile quando un’opzione è già selezionata di default nella pagina forzando così la scelta di un utente. Molto spesso questa tecnica è utilizzata per scopi che vanno contro gli interessi dell’utente, o che causano effetti indesiderati. Questo tipo di dark pattern, come mostrato in Figura 2.11 è riconoscibile nell’applicazione *KeyFinder*. In essa è presente una checkbox già selezionata che permette alla compagnia di contattare l’utente per futuri prodotti e servizi.

Aesthetic Manipulation

Questa sottocategoria, molto simile a *Misdirection* di Harry Brignull, contiene quattro ulteriori sottocategorie: *Toying with Emotion*, *False Hierarchy*, *Disguised Ad* e *Trick Question*.

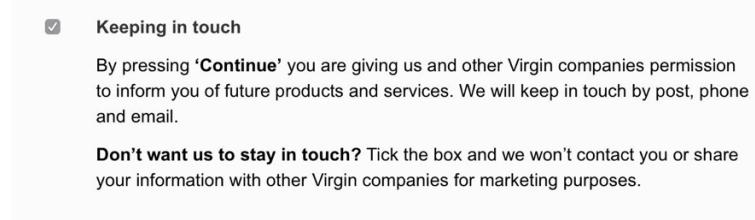


Figura 2.11: Esempio del dark pattern **Preselection** nell'applicazione *KeyFinder*

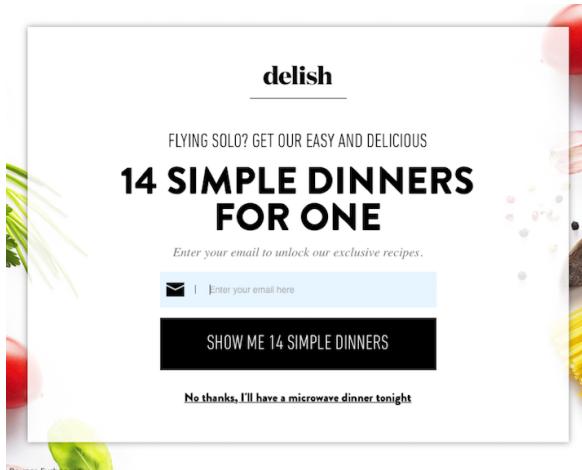


Figura 2.12: Esempio del dark pattern **Toying with Emotion** sul sito *Delish*

Si tratta di manipolazioni dell'interfaccia utente che hanno lo scopo di attirare l'attenzione dell'utente su determinati elementi piuttosto che altri.

Toying with Emotion

Tale dark pattern consiste nel cercare di far suscitare determinate emozioni all'utente tramite l'utilizzo di specifici elementi nell'interfaccia come testo, immagini e colori. Questo dark pattern è ritrovabile sul sito *Delish* che, come mostrato in Figura 2.12, richiede all'utente di iscriversi alla propria newsletter. L'opzione per scegliere "no" è più piccola e utilizza una frase umiliante per far sentire l'utente in colpa per la sua scelta.

False Hierarchy

Con questo dark pattern si cerca di convincere l'utente ad effettuare una scelta piuttosto che un'altra rendendola più appetibile con maggiori decorazioni o più interattività. In particolare, si cerca di dare l'impressione che l'opzione evidenziata sia l'unica o la migliore. Tale dark pattern è possibile incontrarlo sul sito *Reddit* che, come mostrato in Figura 2.13, invoglia l'utente tramite decorazioni grafiche ad installare l'applicazione mobile.

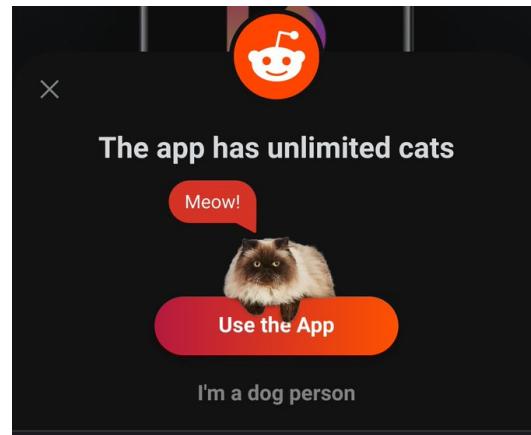


Figura 2.13: Esempio del dark pattern **False Hierarchy** sul sito *Reddit*



Figura 2.14: Esempio del dark pattern **Disguised Ad** come pubblicità dell'applicazione *AccuWeather*

Disguised Ad

Questo tipo di dark pattern è una pubblicità "mascherata" da giochi, pulsanti o altri elementi interattivi che sono presenti in una pagina web o app. Talvolta l'intera pagina web è trasformata in un annuncio in modo da ridirezionare l'utente verso un'altra pagina. Come mostrato in Figura 2.14, un utente può imbattersi in una pubblicità dell'applicazione *AccuWeather*. In questo pop-up cliccando sulla "X", invece di chiudere la pubblicità, si verrà ridirezionati al Google Play Store per effettuare l'installazione dell'applicazione proposta.

Royal Mail, members of [Royal Mail Group](#) and [Post Office](#) would like to contact you about products, services and offers that might interest you. Click on the Register button to submit this form and indicate your consent to receive marketing communications by post, phone, email, text and other electronic means. If you do not wish to receive such communications, please tick the relevant box(es) below.

Post Telephone Email SMS and other electronic means

If you would like to receive information about products, services, special offers and promotions from [carefully selected](#) third parties, please let us know by ticking the relevant box(es) below.

Post Telephone Email SMS and other electronic means

Royal Mail takes your privacy very seriously. The information you provide through the website will be held under the Data Protection Act 1981. Please read our [Privacy Policy](#)

Figura 2.15: Esempio del dark pattern Trick Question sul sito RoyalMail

Trick Question

Questa categoria comprende frasi formulate volontariamente in maniera confusa in modo da manipolare le intenzioni dell’utente. Molte volte, tali frasi presentano doppie negazioni o informazioni che invece significano tutt’altro. Nell’esempio in Figura 2.15, sul sito RoyalMail il primo set di opzioni corrisponde ai mezzi attraverso i quali un utente non desidera ricevere informazioni, mentre il secondo set di opzioni corrisponde ai mezzi attraverso i quali un utente desidera ricevere informazioni. Com’è possibile notare, un utente distratto potrebbe facilmente essere indotto ad iscriversi ad un servizio che non desidera.

2.1.5 Forced Action

Questa categoria spinge un utente ad effettuare una specifica azione per accedere o utilizzare una specifica funzionalità. L’azione da svolgere spesso viene mascherata come un’opzione da cui l’utente ottiene un forte beneficio o si presenta come un passaggio obbligatorio da effettuare per completare un task. Tale categoria contiene tre sottocategorie: *Social Pyramid*, *Privacy Zuckering* e *Gamification*.

Social Pyramid

Questo pattern è usato soprattutto in piattaforme di social media o giochi online in cui gli utenti vengono forzati ad invitare altri utenti ad utilizzare la piattaforma in cambio di potenziamenti o benefici. Inoltre, rende le altre persone socialmente obbligate a giocare anche quando non lo desiderano. Questo dark pattern è stato rilevato, come mostrato in Figura 2.16, nell’applicazione FarmVille. In esso vi è la possibilità di invitare amici in cambio di funzionalità riservate.



Figura 2.16: Esempio del dark pattern **Social Pyramid** nell'applicazione *FarmVille*

Privacy Zuckering

Chiamato così da Tim Jones in omaggio al CEO di *Facebook* Mark Zuckerberg, tale dark pattern inganna l'utente in modo da fargli condividere pubblicamente più informazioni personali di quante ne avrebbe realmente condiviso. All'inizio infatti, *Facebook*, aveva la reputazione di rendere difficile per gli utenti il controllo delle proprie impostazioni sulla privacy, e in generale, rendere molto facile la condivisione eccessiva di dati personali. In risposta ai riscontri negativi dei consumatori ha successivamente creato un'area delle impostazioni sulla privacy più chiara e facile da usare.

Molto spesso questo dark pattern è utilizzato per vendere le informazioni degli utenti ad aziende di terze parti, includendo una clausola nei termini e condizioni o privacy policies dei siti web. Questo dark pattern è stato ritrovato, come mostrato in Figura 2.17, nell'applicazione *WhatsApp*. La sequenza di interfacce mostra un flusso non etico per l'aggiornamento dei Termini e dell'informativa sulla privacy. Nella prima pagina, un utente distratto potrebbe accettare velocemente le condizioni di aggiornamento dei termini senza avere la consapevolezza di star mostrando i propri dati a società di terze parti. Infatti, com'è possibile notare nella seconda pagina c'è una clausola spuntata di default che acconsentirebbe alla vendita di dati personali a *Facebook*.

Gamification

Con questo dark pattern andiamo ad indicare tutte quelle situazioni all'interno di un servizio in cui alcuni aspetti possono essere "guadagnati" soltanto attraverso lo svolgimento

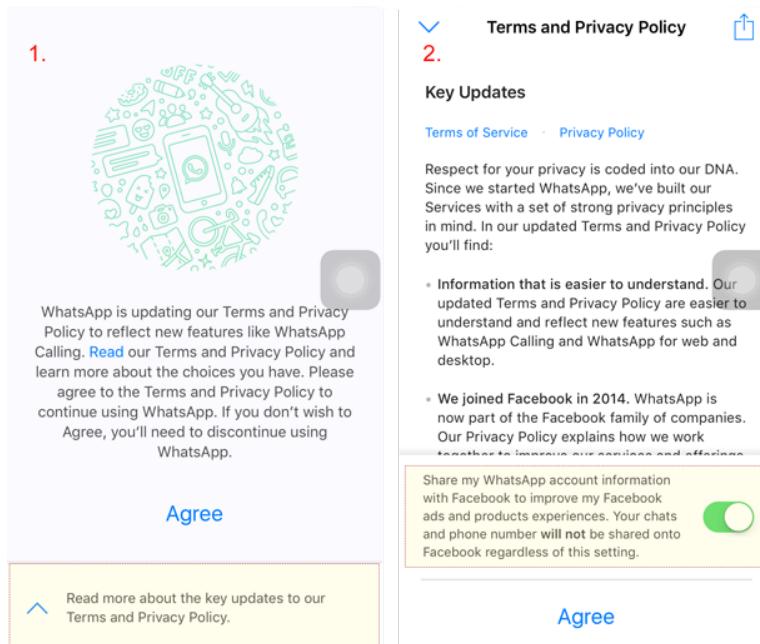


Figura 2.17: Esempio del dark pattern **Privacy Zuckering** nell'applicazione WhatsApp

ripetuto di determinate azioni. Tale pattern è ritrovabile nell'applicazione *Candy Crush Saga* com'è possibile notare dalla Figura 2.18. Il gioco, infatti, offre occasionalmente ai giocatori livelli impossibili da completare per spingere l'acquisto di potenziamenti o vite extra. Se il giocatore non acquista nulla dal gioco, diminuirà lentamente la difficoltà per mantenere la giocabilità.

2.2 Influenza dei Dark Pattern

Nello sviluppo dei dark pattern sono impiegate competenze trasversali che spaziano anche al di fuori del campo informatico coinvolgendo figure professionali come psicologi, antropologi o sociologi. Tali esperti mettono a disposizione la loro competenza al fine di creare pattern basati su bias cognitivi che impediscono all'utente di rendersi conto della presenza di questi modelli manipolatori. Date le potenzialità che i dark pattern hanno di deviare le scelte degli utenti, sono state effettuate numerose ricerche e studi per determinare la percezione e la persuasione che gli utilizzatori delle interfacce hanno di questi modelli. Di Geronimo *et al.* [2020] hanno effettuato un sondaggio online con lo scopo di determinare la percentuale di utenti che è in grado di rilevare la presenza di un dark pattern in un'applicazione mobile. Essi hanno scoperto che il 95% delle applicazioni analizzate contiene uno o più dark pattern ed inoltre che su 584 partecipanti al sondaggio il 55% di essi non è stato in grado identificarli. Se si estendesse questo studio su una platea più ampia di utenti, ovviamente sarebbe facilmente

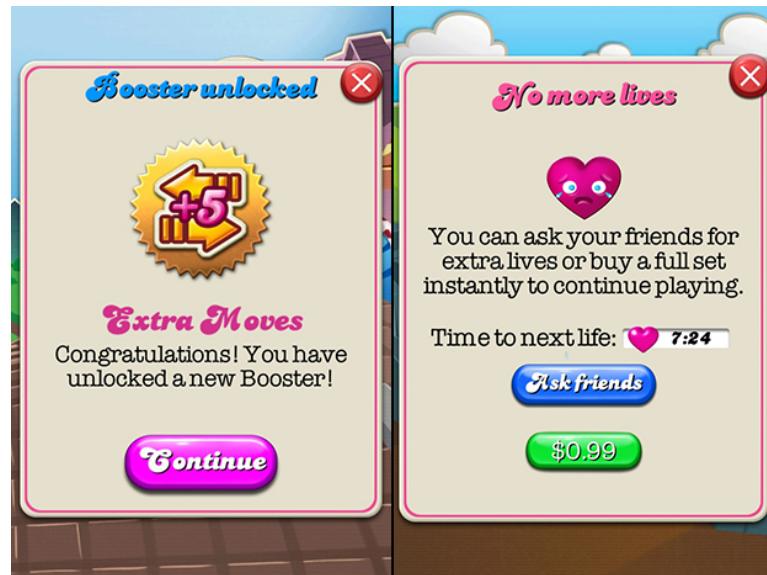


Figura 2.18: Esempio del dark pattern Gamification nell'applicazione *Candy Crush Saga*

rilevabile che la manipolazione delle scelte potrebbe colpire principalmente gli utenti "fragili" della comunità come bambini e anziani. Infatti, molti di essi non sono ben informati sulle potenziali minacce alla privacy e alla sicurezza. Giochi, applicazioni, social media possono contenere tutti questi tipi di dark pattern. Crone e Konijn [2018] hanno infatti mostrato come l'utilizzo tra adolescenti di dispositivi mobili sia aumentato a pari passo con l'avanzamento tecnologico e come i giovani siano facilmente manipolabili. Nonostante ciò, c'è ancora una mancanza di conoscenza dei dark pattern, ed infatti tale studio cerca di colmare un vuoto di ricerca relativo alla quantificazione del rischio della presenza di uno o più dark pattern all'interno di un sito web.

2.3 Implicazioni sulla privacy

A causa dello sviluppo della pandemia mondiale del coronavirus, molte più persone si sono ritrovate ad interagire con piattaforme e dispositivi digitali. Molti lavori condotti da accademici e giornalisti hanno esaminato come i servizi presentino dark pattern in grado di danneggiare la privacy online delle persone. Le informative sulla privacy sono sempre presenti sui siti web e vi è un forte incentivo da parte dei fornitori di servizi a spingere gli utenti ad acconsentire alla condivisione dei propri dati. Sebbene gli inserzionisti spesso affermino il contrario, la maggior parte dei consumatori preferisce non essere monitorata durante le proprie attività. Uno studio condotto da Kulyk *et al.* [2018] ha infatti mostrato che solo il 3% circa degli utenti è disposto ad accettare ad esempio i cookie di tracciamento e che

la maggior parte dei visitatori dei siti acconsente esclusivamente all'utilizzo dei cookie come un "male necessario" per accedere ad essi. A tal proposito Hausner e Gertz [2021] hanno fornito uno studio sul rilevamento di dark pattern nel contesto dei banner dei cookie.

La questione dei dark pattern è finita nel mirino dei governi, che per tutelare la privacy e il rispetto degli utenti, hanno deciso di regolamentarne l'utilizzo. Il primo paese ad adottare una politica di limitazione è stata la California che tramite il *California Consumer Privacy Act* ha proibito l'utilizzo di dark pattern che potrebbero compromettere le scelte opt-out degli utenti nelle situazioni in cui sono coinvolti i loro dati. In Europa, invece, è al vaglio del parlamento europeo il *Digital Service Act* che punta al rispetto di normative più stringenti per quanto riguarda la pubblicità, la moderazione dei contenuti e l'utilizzo dei dark pattern. Per tutelare la privacy degli utenti questo studio mira a fornire uno strumento che possa stimare i rischi della presenza di dark pattern in siti web.

2.4 Rilevabilità dei Dark Pattern

La maggior parte degli studi svolti sulla tematica dei dark pattern sono incentrati sulla creazione di una tassonomia che li dividesse nelle varie categorie. Altri, invece, hanno incentrato il focus sul partizionamento di queste interfacce malevoli in base al tipo di rilevabilità. Curley *et al.* [2021] hanno infatti, proposto una suddivisione di essi in due categorie:

1. Rilevabili automaticamente
2. Rilevabili manualmente

I dark pattern "rilevabili automaticamente" sono generalmente associati a parole o immagini che li rendono facilmente identificabili tramite un algoritmo. Quelli "rilevabili manualmente" sono anch'essi associati a parole o immagini, ma la loro varietà di implementazione li rende particolarmente difficili da identificare tramite un algoritmo. In particolare, questa classificazione è nata durante il corso di Interazione Uomo-Macchina e delle attività di tirocinio; la ripartizione è stata svolta in maniera collaborativa insieme ad altri tre studenti che, individualmente analizzavano esempi dei vari dark pattern per poi confrontarsi e procedere alla suddivisione.

Di seguito è mostrata una ripartizione di essi nelle corrispondenti categorie.

2.4.1 Rilevabili Automaticamente

I dark pattern che possono essere rilevati automaticamente tramite un algoritmo di detection sono:

1. Obstruction

- **Roach Motel:** Trovare nelle pagine bottoni o link con scritte del tipo *Chiudi Account, Elimina Abbonamento*;
- **Price Comparison Prevention:** Verificare se nel file sorgente di un sito di e-commerce è disabilitata la funzionalità del copia e incolla;
- **Intermediate Currency:** Controllare se in una pagina web sono presenti link o bottoni con scritte del tipo *Acquista Gemme, Acquista Monete, Acquista Miglioramenti* o simili;

2. Sneaking

- **Hidden Costs:** Simulare l'acquisto di un prodotto e confrontare il prezzo iniziale e finale per constatare se ci sono state modifiche di esso;
- **Sneak into Basket:** Simulare l'acquisto di un prodotto e controllare se nel carrello online sono stati inseriti più prodotti di quelli aggiunti;

3. Interface Interferences

- **Toying with Emotion:** Utilizzare algoritmi di *Natural Language Processing*;
- **Disguised Ad:** Cercare pulsanti che indirizzano a siti esterni per effettuare download;
- **Trick Question:** Individuare tramite analisi del linguaggio naturale;
- **Preselction:** Individuare checkbox già selezionate all'interno della pagina web;

2.4.2 Non Rilevabili

I dark pattern che non possono essere rilevati tramite algoritmi sono:

1. Nagging: Dal momento che può comparire in qualsiasi istante durante la navigazione di una pagina, lo rende molto difficile da individuare;

2. Sneaking

- **Forced Continuity:** Date le sue caratteristiche non è individuabile;

- **Bait and Switch:** Date le sue molteplici modalità di implementazione non è individuabile;

3. Interface Interferences

- **Hidden Informations:** Date le sue caratteristiche non è individuabile;
- **False Hierarchy:** Date le sue molteplici modalità di implementazione non è individuabile;

4. Forced Action

- **Social Pyramid:** Date le sue caratteristiche e molteplici modalità di implementazione non è individuabile;
- **Privacy Zuckering:** Date le sue caratteristiche non è individuabile;
- **Gamification:** Date le sue molteplici modalità di implementazione non è individuabile.

In base a tale classificazione, tra i dark pattern che possono essere rilevati automaticamente tramite algoritmi, è stato scelto **Sneak Into Basket** come pattern da rilevare.

CAPITOLO 3

Un approccio basato su computer vision per l'identificazione del dark pattern Sneak Into Basket

Il dark pattern Sneak Into Basket è l'equivalente di un lavoratore di un supermercato che inserisce prodotti nel carrello della spesa all'insaputa del cliente, prodotti che vanno all'attenzione solo quando si è raggiunta la cassa. Generalmente, è possibile ritrovare questo modello oscuro quando si naviga su siti di e-commerce che cercano di incrementare i loro ricavi aggiungendo prodotti non scelti dall'utente nel carrello online. L'inserimento di questi articoli è spesso giustificato come suggerimento correlato a prodotti presenti già nel carrello. Ovviamente un utente distratto acquisterà involontariamente questi articoli, a meno che non se ne accorga prima dell'effettivo acquisto.

Questo dark pattern è uno dei più pericolosi perché se utilizzato bene potrebbe causare danni economici ad una vasta gamma di utenti. È quindi necessario creare un algoritmo che possa permettere la sua identificazione. In questo capitolo sono mostrati due approcci risolutivi: il primo tramite analisi del DOM, che si è rivelato inefficiente, ed il secondo basato su classificazione di immagini, che ha avuto ottimi risultati.

3.1 Primo Approccio Risolutivo: Analisi del DOM

Un primo approccio risolutivo dell'algoritmo è stato quello di tentare di analizzare il Document Object Model (DOM) che è una forma di rappresentazione di documenti strutturati come HTML (HyperText Markup Language) e XML (Extensible Markup Language), in un

modello orientato agli oggetti. Ciò significa che il DOM propone una struttura a forma di albero per permettere di organizzare il lavoro di programmazione nel modo più preciso possibile. Esso è un documento che sostanzialmente può essere acceduto per leggerne la struttura, per aggiornarlo dinamicamente tramite un linguaggio di scripting come JavaScript e per tante altre azioni. Dal momento che tutte le pagine web sono nel formato HTML è risultato intuitivo andarne a leggere la struttura per l'identificazione del dark pattern *Sneak Into Basket*.

A partire dalla caratteristica principale del dark pattern da rilevare, cioè che l'aggiunta nel carrello di un prodotto ne determina l'aggiunta di uno o più prodotti all'insaputa del cliente, è risultato logico andare a simulare degli acquisti su siti web. Lo scopo principale di tale simulazione è stato quello di riuscire a trarre caratteristiche simili e differenti tra i vari siti a livello di interfaccia, a livello di struttura del DOM e a livello di sequenza delle azioni per inserire un prodotto nel carrello ed effettuare l'acquisto. Tale analisi è stata effettuata su circa 50 siti di e-commerce di vario genere.

Le peculiarità simili dei siti risultate dall'analisi sono che la maggior parte di essi presenta la stessa sequenza di azioni e sommariamente la stessa interfaccia. La sequenza di azioni svolte da un utente per aggiungere un articolo nel carrello ed effettuare l'acquisto a partire dalla homepage del sito sono: recarsi in una delle categorie di vendita, selezionare un articolo, compilare se presenti delle opzioni di vendita, aggiungere l'articolo al carrello, recarsi nella pagina del carrello ed effettuare l'acquisto. Le interfacce dei siti sono molto simili tra loro per la disposizione degli elementi salienti per svolgere e completare un acquisto.

Le caratteristiche differenti dei siti sono la diversa struttura del DOM sia delle pagine relative ai singoli prodotti sia per la pagina del carrello. Ciò che salta subito all'occhio è la vastità dei modi con la quale sono rappresentati gli elementi nella pagina.

Dopo aver effettuato la simulazione e segnato i risultati si è cercato di costruire un primo algoritmo che tentasse di identificare il dark pattern *Sneak Into Basket* tramite l'analisi del DOM. L'algoritmo prevede l'utilizzo di un Application Programming Interface (API) chiamata Cypress.io che è uno strumento di test front-end basato esclusivamente su JavaScript creato per il Web moderno. Esso ha lo scopo di affrontare e mostrare i punti deboli che gli sviluppatori devono affrontare durante le operazioni di test delle applicazioni. Utilizza una tecnica di manipolazione del DOM ed opera direttamente nel browser in maniera da semplificare l'utilizzo di essa. Tale interfaccia è utilizzata per effettuare la simulazione di acquisto di un articolo. L'algoritmo prevede la simulazione dell'aggiunta di un prodotto qualsiasi nel carrello e la visita della pagina del checkout per analizzare il numero di prodotti

in essa. In input l'algoritmo riceve la pagina di un prodotto e restituisce se il sito implementa o meno il dark pattern. Non prende in input la homepage perché generalizzare l'inserimento di un qualsiasi prodotto risulta essere più difficile a causa delle diverse posizioni di esso tra le pagine del sito. Comunque, aggiungere un prodotto al carrello non è una facile impresa perché molte delle volte sono richieste varie opzioni da scegliere prima di poter concludere l'acquisto. Risulta inoltre complicato, ma non impossibile, generalizzare la ricerca di un elemento come un bottone, o link in una pagina perché a volte non vengono seguite delle buone prassi di programmazione. Infatti, ricercare un ad esempio un bottone cliccabile con la scritta "aggiungi al carrello, "add to cart" è difficile per l'eterogeneità delle pagine web. Molte volte vengono utilizzate classi esterne che danno proprietà e identità particolare agli elementi. Comunque, dopo vari tentativi l'inserimento generico di prodotti al carrello è riuscito. Ora resta soltanto contare gli elementi della pagina di checkout, ma effettuare tale operazione molte delle volte è impossibile perché sono molteplici i modi con cui si può ritrovare tale lista. Infatti, DOM profondamente diversi possono dar luogo ad interfacce che visivamente sono molto simili, per cui un'analisi di questo tipo non è efficiente.

Per questo motivo creare un algoritmo che possa identificare istanze di dark pattern del tipo Sneak Into Basket tramite un'analisi del DOM di una pagina web non è un'ottima strada da percorrere. Per cui, dopo diversi tentativi di implementazione dell'algoritmo intelligente si è deciso di abbandonare tale strada.

3.2 Secondo Approccio Risolutivo: Classificazione per Immagini

Se l'analisi del DOM si è rivelata inefficace nell'identificare istanze di dark pattern del tipo Sneak Into Basket, la classificazione per immagini si è rivelata un ottimo percorso da seguire. Infatti, la Computer Vision è un campo di studi interdisciplinare che studia tecniche e algoritmi per permettere ai computer di simulare processi dell'apparato visivo umano. Non si tratta solo di riuscire a riconoscere oggetti, persone o animali all'interno di una singola immagine, ma di estrarre da essa informazioni per l'elaborazione a livelli più alti di astrazione. In effetti, si tratta della capacità di ricostruire un contesto intorno all'immagine e di darle un proprio significato. Per poter funzionare correttamente, questi sistemi devono essere addestrati con grandi quantità di immagini che, divise tra di loro formeranno il dataset che renderà l'algoritmo intelligente. Più immagini compongono il dataset maggiore sarà l'accuratezza della Image Classification.

Perché si è arrivati ad effettuare un'analisi alle immagini? Il problema principale dell'ap-

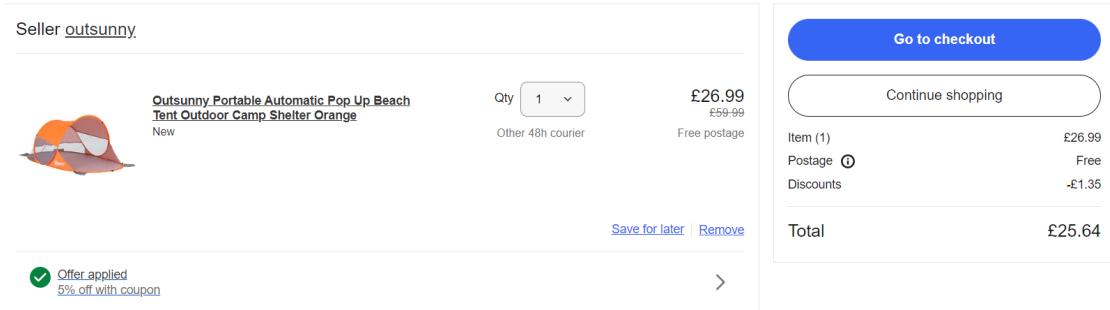


Figura 3.1: Carrello Online del sito Ebay con un prodotto



Figura 3.2: Carrello Online del sito LanaOnline con un prodotto

proccio precedente, ovvero quello dell’analisi del DOM, era l’incapacità di riuscire a contare gli elementi nel carrello di un sito web a causa dei molteplici modi implementativi con il quale esso fosse realizzato. Dal momento che il dark pattern Sneak Into Basket comporta l’inserimento di uno o più prodotti all’interno del carrello all’insaputa del cliente, viene subito in mente che l’unica cosa che debba fare l’algoritmo sia quella di contare gli elementi del carrello. L’algoritmo visiterà un sito web, aggiungerà un prodotto qualsiasi al carrello della spesa, e andrà a calcolare il numero di prodotti in esso. Se il numero di articoli è maggiore di uno allora il sito implementa un’istanza di Sneak Into Basket. Dal momento che si è intrapresa la strada della classificazione per immagini, si è svolta un’attenta analisi visiva dei carrelli online. Sono stati visitati all’incirca 100 carrelli online di vari tipi di e-commerce e si è fatta una stima di quanti somigliassero tra loro. Si è giunti alla conclusione che il 95% di essi ha una struttura simile. Com’è possibile notare dalla Figura 3.1 e Figura 3.2, questa è l’interfaccia maggiormente utilizzata dai designer di siti web per la costruzione di pagine di carrelli online contenenti un solo prodotto per tipo. Invece dalle Figura 3.3 e Figura 3.4 è possibile notare come cambia la struttura quando all’interno di esso ci sono 2 o più prodotti di diverso tipo. Sostanzialmente ciò che muta tra le due tipologie è la presenza o meno di uno spazio

The screenshot shows a shopping cart on the eBay website. It contains two items:

- Seller out sunny:** An Outunny Portable Automatic Pop Up Beach Tent Outdoor Camp Shelter Orange. Price: £26.99 (from £59.99). Shipping: Other 48h courier. Postage: Free postage.
- Seller sashtime:** A LARGE FAMILY SWIMMING POOL GARDEN OUTDOOR SUMMER INFLATABLE PADDLING POOLS /PUMP. Price: £27.95 (from £79.94). Shipping: Other 48h courier. Postage: Free postage.

The cart summary on the right shows a total of £53.59 for 2 items, with postage and discounts applied.

Figura 3.3: Carrello Online del sito Ebay con due prodotti

The screenshot shows a shopping cart on the LanaOnline website. It contains two items:

- CARRELLO**
 - Ferri Dritti Drops Basic - Legno 35cm 4,30 €
 - Diametro Ferro: 5.50 mm.
 - Ferri Dritti Prym - Plastica 40cm 7,80 €
 - Diametro Ferro: 15.00 mm.

The cart summary on the right shows a total of 12,10 € for 2 articles, including shipping at 5,50 €. There is a link to "Hai un codice sconto?" (Do you have a discount code?). The total amount is 17,60 €.

Figura 3.4: Carrello Online del sito LanaOnline con due prodotti

riservato ad una seconda merce. Quindi, come si può notare, la disposizione degli elementi nella pagina cambia radicalmente se il numero di articoli è uno o più di uno. Ecco il motivo del quale si è pensato di creare un algoritmo che possa determinare la presenza del dark pattern Sneak Into Basket tramite l’analisi di uno screenshot della pagina del carrello eseguito dopo l’inserimento di un prodotto in esso. La classificazione per immagini è un compito fondamentale che tenta di comprendere un’intera immagine nel suo insieme. L’obiettivo è quello di assegnarle un’etichetta specifica. In genere, essa è una tecnica utilizzata ad immagini che presentano un solo oggetto. Invece, il rilevamento di più oggetti coinvolge sia la classificazione che le attività di localizzazione e viene utilizzato per effettuare analisi più realistiche in cui possono comparire più oggetti in un’immagine.

Insomma, la classificazione delle immagini sembra essere un buon punto di inizio per la creazione dell’algoritmo di detection.

3.2.1 Algoritmo di Detection

Per classificare gli screenshot del carrello di un sito di e-commerce si è utilizzato uno strumento chiamato Teachable Machine che rende la creazione di modelli di machine learning facile, rapida e accessibile a tutti. Esso addestra un computer per riconoscere immagini, suoni e pose senza dover scrivere alcuna riga di codice per l’apprendimento. Teachable Machine utilizza TensorFlow.js, una libreria per il machine learning in JavaScript, per addestrare ed eseguire modelli realizzati in un browser web. Questo modello utilizza una tecnica chiamata transfer learning. Esiste una rete neurale pre-addestrata e, quando vengono create le classi, queste diventano l’ultimo livello della rete neurale. Nel dettaglio, i modelli di posa e di immagini imparano da modelli di MobileNet pre-addestrati, mentre quelli del suono si basano su Speech Command Recognizer. La Teachable Machine utilizzata in questo progetto usa le impostazioni predefinite. Il dataset di tale strumento è stato riempito di 80 immagini: 40 di esse etichettate come *un prodotto* e le restanti etichettate con *due prodotti*. Le prime sono screenshot di carrelli che presentano un prodotto al suo interno, le seconde sono schermate di carrelli che invece contengono due prodotti. Quando viene data un’immagine di un carrello alla macchina ci informa se essa contiene un prodotto o due.

Gli strumenti principali utilizzati in tale algoritmo sono Cypress.io, Express e Puppeteer. Il primo è uno strumento di test front-end basato esclusivamente su JavaScript creato per il Web moderno. Esso ha lo scopo di affrontare e mostrare i punti deboli che gli sviluppatori devono affrontare durante le operazioni di test delle applicazioni. Il secondo è un framework di applicazioni Web back-end per Node.js, progettato per la creazione di applicazioni Web

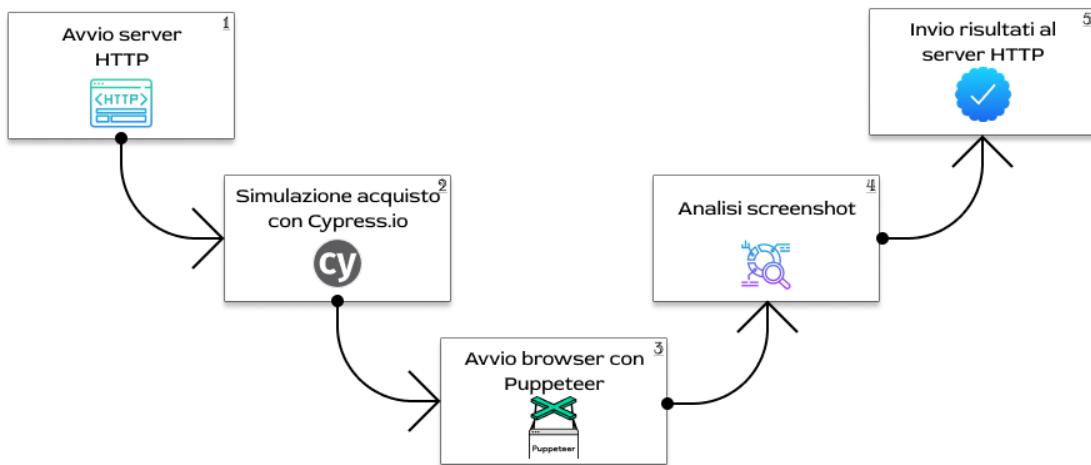


Figura 3.5: Passi Svolti dall’Algoritmo di Detection

e API. Il terzo è una libreria Node che fornisce un’API di alto livello per gestire Chrome o Chromium tramite il protocollo DevTools. Esso viene eseguito in modalità headless per impostazione predefinita, ma può essere configurato per eseguire Chrome o Chromium completi (non headless). Permette di fare la maggior parte delle cose che si possono fare manualmente nel browser.

L’idea alla base dell’algoritmo è quella di simulare l’aggiunta al carrello di un prodotto, di visitare la pagina del carrello e effettuare uno screenshot che sarà successivamente posto all’analisi della Teachable Machine. Prima però bisogna risolvere un po’ di problemi. Dal momento che la Teachable Machine deve necessariamente "girare" in una pagina web serve un modo per poter trasferire lo screenshot tra un ambiente di back-end e un ambiente web. Tale problema è risolvibile utilizzando un server HTTP che trasferisce l’immagine scattata da Cypress, che lavora lato "back-end", alla Teachable Machine. Inoltre, il server HTTP è utilizzato per ottenere i risultati dell’analisi svolta sull’immagine.

Come si può notare in Figura 3.5, l’algoritmo di detection di istanze del dark pattern Sneak Into Basket è suddiviso in 5 fasi principali. Ora analizziamo i passi uno alla volta:

1. Avvio Server HTTP: Viene avviato un Server HTTP tramite Express che è utilizzato principalmente per servire lo screenshot alla Teachable Machine e ottenere i risultati dell’analisi;
2. Simulazione acquisto con Cypress.io: Tramite la libreria Cypress.io viene effettuata la simulazione di acquisto dal momento che essa fornisce un’interfaccia per interagire in maniera programmatica con le pagine web. Viene dato allo strumento l’url di un prodotto venduto dal sito da analizzare, viene aggiunto il prodotto al carrello e viene

visitata la pagina del carrello. Qui viene effettuato uno screenshot che sarà analizzato dalla Teachable Machine;

3. Avvio browser con Puppeteer: Viene avviato un browser senza interfaccia con Puppeteer per poter visitare la pagina web dove è possibile effettuare l'analisi dello screenshot;
4. Analisi screenshot: Viene effettuata l'analisi dello screenshot da parte della Teachable Machine;
5. Invio risultati analisi al server HTTP: I risultati dell'analisi vengono inviati al server tramite una richiesta HTTP effettuata dalla Teachable Machine.

Siccome che i siti di e-commerce possono essere organizzati in infiniti modi, l'algoritmo prende in input la pagina di un prodotto perché risulterebbe essere troppo complesso determinare un algoritmo per cercare suddetta pagina automaticamente. Inoltre, per lo stesso motivo, prende in input anche la pagina del carrello. L'output dell'algoritmo ci darà informazioni riguardanti la presenza o meno di istanze del dark pattern Sneak Into Basket.

Il codice dell'algoritmo è consultabile nel repository GitHub al seguente link: <https://github.com/antgioia/sneak-into-basket-detection>.

CAPITOLO 4

Valutazione preliminare dell'approccio

4.1 Metodologia

Per stabilire l'efficacia e la correttezza dell'algoritmo, è stato testato su un dataset creato da Mathur *et al.* [2019] contenente 1824 esempi di siti che implementano dark pattern. Ogni campo elenca il sito, quale tipologia di dark pattern implementa e le motivazioni per cui esso è etichettato come un dark pattern. Da questi ne sono stati estratti 7, cioè soltanto quelli che implementano la tipologia nominata *Sneak Into Basket*. Siccome il dataset è stato creato un po' di tempo fa, e considerato che ogni link di esso rimanda ad un prodotto venduto dal sito, le aziende purtroppo non hanno più in vendita quei prodotti. Per tale ragione si è reso necessario cambiare questi siti web con quelli che rimandano a prodotti effettivamente in vendita dall'azienda. Tali siti indirizzeranno l'algoritmo sempre alla stessa impresa ma su un prodotto diverso che sarà inserito nel carrello. Nella Tabella 4.1 è possibile vedere il dataset aggiornato e utilizzato per testare l'algoritmo. L'algoritmo è testato su tutte le tuple della tabella e per ognuna di esse sono riportati i risultati dell'algoritmo e le motivazioni di successo o di fallimento di esso in riferimento ad un'indagine svolta sullo screenshot. Per certificare la correttezza dei risultati dell'algoritmo per ogni sito, le operazioni svolte da esso sono replicate manualmente e confrontate.

	Sito	Motivazione
1	https://yourvintagewine.com/product/jericho-canyon-2010/	Shipping insurance is default
2	https://www.airportappliance.com/dishwashers/dishwashers/dish-drawer-dishwashers/DD24DAX9N/	Adds warranty to basket. It's preselected
3	https://www.avasflowers.net/product/dreaming-of-tuscany-bouquet	Adds a card to basket
4	https://www.cellularoutfitter.com/collections/apple-iphone-se-3rd-gen-/2022/products/executive-xxl-/horizontal-leather-case-black	Extra product in cart along with free gift. Sneaked in using checkbox
5	https://www.laptopoutlet.co.uk/lenovo-v-v15-15-6-full-hd-/laptop-amd-athlon-3050u-/4gb-ram-128gb-ssd-grey-/windows-10-home-82c700e4uk.html	With the laptop, you also get an insurance
6	https://www.silencershop.com/oss-rad-9.html	\$1.00 donation is default
7	https://www.templeandwebster.com.au/Rustic-Glass-Pendant-Light-ASOL1004.html	Adds insurance by default

Tabella 4.1: Dataset utilizzato per il testing dell'algoritmo

4.2 Risultati

Di seguito sono riportati i risultati del testing svolti sulle tuple della Tabella 4.1:

1. **Your Vintage Wine:** Sebbene il sito non implementi istanze del dark pattern *Sneak Into Basket*, l'algoritmo non funziona correttamente perché, dopo l'aggiunta di un solo prodotto nel carrello, riporta che esso contiene due articoli.
2. **Airport Appliance:** L'algoritmo funziona correttamente ed individua l'utilizzo del dark pattern *Sneak Into Basket* perché nel carrello insieme alla lavatrice viene aggiunta

un’assicurazione del costo di 109,99\$. Infatti, nella pagina del prodotto c’è una spunta già selezionata che aggiunge automaticamente una garanzia di 3 anni.

3. **Avas Flowers:** Sebbene il sito non implementi più il dark pattern Sneak Into Basket, l’esecuzione dell’algoritmo cessa di funzionare perché è richiesta la compilazione di varie opzioni di vendita prima di aggiungere il prodotto al carrello.
4. **Cellular Outfitter:** L’algoritmo funziona correttamente perché riporta che nel carrello c’è un solo prodotto, ed infatti il sito non implementa istanze del dark pattern Sneak Into Basket.
5. **Laptop Outlet:** L’algoritmo non riesce a identificare la presenza del dark pattern Sneak Into Basket perché al momento del caricamento della pagina del carrello viene visualizzato un pop-up che oscura gli elementi al di sotto di esso. Quindi l’esecuzione dell’algoritmo non va a buon fine perché lo screenshot mostra il pop-up e non il carrello.
6. **Silencer Shop:** L’algoritmo funziona correttamente ed individua l’utilizzo del dark pattern Sneak Into Basket perché nel carrello insieme al prodotto viene inserita di default una donazione di 1\$.
7. **Temple and Webster:** Sebbene il sito non implementi più il dark pattern Sneak Into Basket perché l’assicurazione non viene inserita di default, l’algoritmo funziona correttamente perché riporta che nella pagina del carrello è presente un solo prodotto che è quello che abbiamo aggiunto.

Ora che i risultati del testing sono pronti è possibile scoprire punti di forza e di debolezza dell’algoritmo. L’algoritmo per come è stato ideato inizialmente funziona correttamente. Infatti, i casi di test numero 2, 4, 6 e 7 mostrano i risultati attesi. I casi in cui l’algoritmo riporta risultati inattesi sono due: il caso numero 3, com’è possibile vedere nell’Immagine 4.1, perché è richiesta la compilazione di varie opzioni di vendita prima dell’aggiunta del prodotto al carrello; il caso numero 5 perché al momento dello screenshot viene visualizzato un pop-up, mostrato in Figura 4.2, che oscura gli elementi presenti nel carrello. L’algoritmo riporta un risultato errato sul caso di test numero 1. Quest’ultimo problema può essere risolto andando ad aggiornare il dataset della Teachable Machine con altre tipologie di carrello in modo avere risultati ancora più precisi.

In definitiva possiamo ritenere che l’algoritmo sommariamente funziona in maniera corretta e gli unici casi in cui esso riporta risultati inattesi sono due: quando è presente la

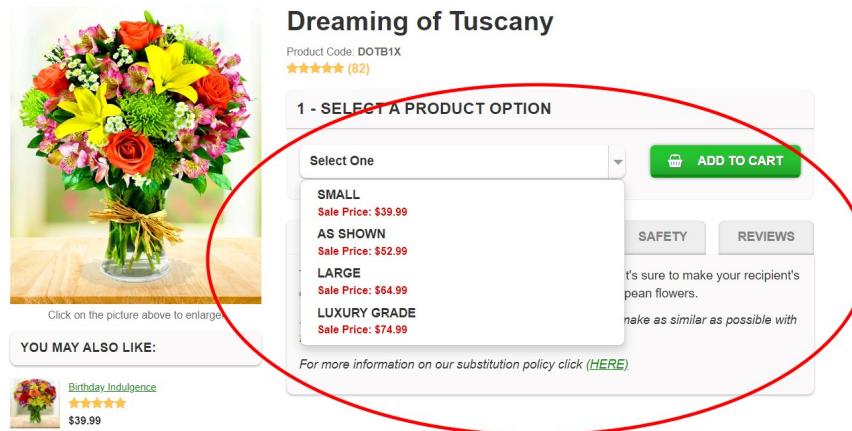


Figura 4.1: Opzioni di vendita caso di test n°3

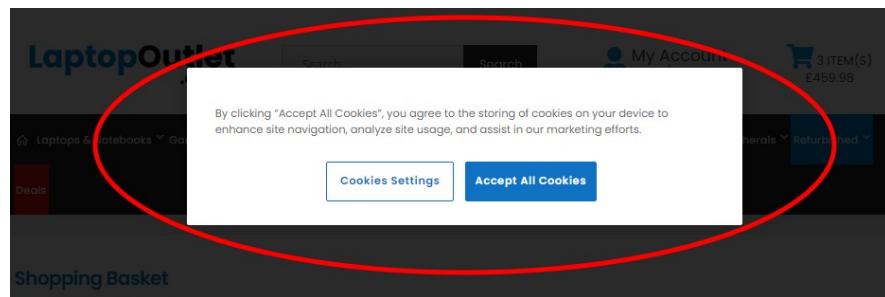


Figura 4.2: Pop-up caso di test n°5

compilazione di campi di vendita e quando al momento dell'esecuzione dello screenshot al carrello è presente un pop-up che oscura la visualizzazione degli elementi al di sotto di esso. A causa dell'eterogeneità dei siti di e-commerce, riguardo i prodotti in vendita, andare a creare un algoritmo che possa andare a compilare i campi di vendita non è un'operazione facile. Basta pensare ad esempio alle abissali differenze di opzioni di vendita tra un paio di scarpe ed una cover di un cellulare.

Possiamo ritenere che l'algoritmo ha funzionamento corretto nel 60% dei casi. Tale percentuale può essere migliorata, come già detto precedentemente, andando ad aggiungere nuove schermate di carrelli nel dataset della Teachable Machine in modo da ottenere di volta in volta risultati più affidabili.

CAPITOLO 5

Conclusioni e Sviluppi Futuri

Questo studio si è focalizzato principalmente sulla creazione di un algoritmo che possa ricercare istanze di dark pattern di tipo Sneak Into Basket in pagine web. Per fare ciò si è partiti dalla lettura di vari documenti che hanno sancito la nascita dello stato dell'arte, che ci permesso di analizzare e studiare tutte le tipologie di dark pattern esistenti. Da qui, dopo un'attenta indagine, è seguita una suddivisione dei dark pattern in base alla loro rilevabilità. Tra i vari tipi che possono essere rilevati tramite un algoritmo di detection è stato scelto Sneak Into Basket come modello da individuare. Dopo aver studiato due approcci risolutivi, è stata scelta come strada da percorrere per l'individuazione del modello quella della classificazione per immagini. Per constatare l'accuratezza dell'algoritmo creato, esso è stato testato su un dataset contenente siti che implementano il suddetto modello in questione. L'analisi ha riportato una correttezza del 60% dei casi, che può essere ritenuto un ottimo risultato per uno studio preliminare. Da questa sono sorte delle limitazioni che saranno risolte successivamente. Comunque, i risultati sono buoni e permettono l'utilizzo dell'algoritmo in Arkan (<https://www.projectarkan.com/>), che è uno strumento ideato durante il corso di Interazione Uomo Macchina. Con esso gli utenti possono interagire in modo attivo e li rende consapevoli dei rischi che potrebbero incorrere durante l'interazione con un sito che presenta istanze di dark pattern. Dal momento che tale strumento permette ad utente di effettuare l'analisi di un sito per la ricerca di istanze di dark pattern, l'algoritmo ideato in questo studio può essere utilizzato per ispezionare siti web all'individuazione di istanze di Sneak Into Basket.

Ringraziamenti

Mi è doveroso ringraziare le persone che hanno contribuito, con il loro instancabile supporto, alla realizzazione di questo elaborato.

In primis, un ringraziamento speciale al mio relatore Fabio Palomba, per i suoi indispensabili consigli, per la voglia di conoscere che mi ha trasmesso fin dal primo momento e per le conoscenze inculcate durante tutto il percorso di stesura dell'elaborato.

Grazie anche alla mia seconda relatrice Giulia Sellitto per avermi suggerito puntualmente le giuste modifiche da apportare alla mia tesi.

Ringrazio la mia grande famiglia che mi ha riservato la possibilità di perseguire questo importante traguardo e per l'appoggio mostrato in ogni mia decisione.

Un immenso grazie ad Antonio, Giovanni e Manuela, che avete dato valore ad ogni singola ora spesa insieme, servite a raggiungere questo traguardo. Un grazie a Kevin per la sua sincerità, per le interminabili chiacchierate e per avermi sempre aperto le porte di casa. Inoltre, ringrazio chiunque ho conosciuto in questo fantastico percorso, senza di voi non sarebbe stata la stessa cosa. Sono così tanti i bei ricordi che mi passano per la testa che è sarebbe impossibile sceglierne soltanto uno da raccontare.

Un grazie a Massimo che ha sempre creduto in me e mi ha spronato nel dare sempre il meglio. Ringrazio gli amici di sempre, così diversi così importanti, ognuno per ragioni uniche e speciali, voglio esprimere la mia più assoluta gratitudine per il costante e duraturo supporto ricevuto nel corso di questi anni.

Per finire, dedico questo lavoro anche a me stesso, al tempo preso e al tempo perso. Lo dedico ai sacrifici che pensavo di non essere in grado di sostenere e alla tenacia che mi ha fatto raggiungere questo traguardo.

Bibliografia

BÖSCH, C., ERB, B., KARGL, F., KOPP, H. e PFATTHEICHER, S. (2016), «Tales from the dark side: Privacy dark strategies and privacy dark patterns», *Proceedings on Privacy Enhancing Technologies*, vol. 2016 (4), p. 237–254. (Citato a pagina 8)

CONTI, G. e SOBIESK, E. (2010), «Malicious interface design: exploiting the user», in «Proceedings of the 19th international conference on World wide web», p. 271–280. (Citato a pagina 8)

CRONE, E. A. e KONIJN, E. A. (2018), «Media use and brain development during adolescence», *Nature communications*, vol. 9 (1), p. 1–10. (Citato a pagina 21)

CURLEY, A., O'SULLIVAN, D., GORDON, D., TIERNEY, B. e STAVRAKAKIS, I. (2021), «The Design of a Framework for the Detection of Web-Based Dark Patterns», . (Citato a pagina 22)

DI GERONIMO, L., BRAZ, L., FREGNAN, E., PALOMBA, F. e BACCHELLI, A. (2020), «UI dark patterns and where to find them: a study on mobile applications and user perception», in «Proceedings of the 2020 CHI conference on human factors in computing systems», p. 1–14. (Citato a pagina 20)

GRAY, C. M., KOU, Y., BATTLES, B., HOGGATT, J. e TOOMBS, A. L. (2018), «The dark (patterns) side of UX design», in «Proceedings of the 2018 CHI conference on human factors in computing systems», p. 1–14. (Citato alle pagine iv e 9)

HARRY BRIGNULL, H. (2010), «Dark Patterns», <https://www.darkpatterns.org/>. (Citato a pagina 8)

- HAUSNER, P. e GERTZ, M. (2021), «Dark Patterns in the Interaction with Cookie Banners», *arXiv preprint arXiv:2103.14956*. (Citato a pagina 22)
- KULYK, O., HILT, A., GERBER, N. e VOLKAMER, M. (2018), «this website uses cookies”: Users’ perceptions and reactions to the cookie disclaimer», in «European Workshop on Usable Security (EuroUSEC)», . (Citato a pagina 21)
- MATHUR, A., ACAR, G., FRIEDMAN, M. J., LUCHERINI, E., MAYER, J., CHETTY, M. e NARAYANAN, A. (2019), «Dark patterns at scale: Findings from a crawl of 11K shopping websites», *Proceedings of the ACM on Human-Computer Interaction*, vol. 3 (CSCW), p. 1–32. (Citato alle pagine 6 e 33)