GIUSTIZIA CIVILE.com

L'IMPATTO DEI DARK PATTERNS SUL CONSENSO DELL'UTENTE: LA VIA EUROPEA PER AFFRONTARE LE NUOVE VULNERABILITÀ

di **GIORGIA GUERRA**

Approfondimento del 19 agosto 2022

ISSN 2420-9651

L'articolo esamina i problemi posti dalle architetture digitali "manipolative" all'acquisizione del consenso libero e informato dell'utente. Il tema della tutela giuridica del consenso non è certo nuovo. Un lungo percorso giurisprudenziale caratterizza già, anche nel nostro ordinamento, l'evoluzione di tale concetto nel contesto off-line. Emergono, però, anche profili di novità, soprattutto in considerazione dello stretto intrecciarsi del tema della tutela dei diritti dell'utente sui propri dati, profilo informativo, con quello della protezione dello stesso contro le pratiche commerciali scorrette attinente, invece, all'ambito della tutela del consumatore.
A partire da tale constatazione, lo scritto descrive le principali forme di dark patterns, recentemente identificate dal parere dello European Data Protection Board 3/2022, per capire come tali meccanismi siano tipicamente usati nel web ed impattino sul comportamento dell'utente. Dopo aver inquadrato le nuove vulnerabilità emergenti in tema di consenso nel quadro legislativo europeo, l'articolo considera i recenti interventi delle Autorità Garanti per la protezione dei dati e della giurisprudenza europea per mettere in luce il divario emergente tra tutela formale, che si realizza con la compliance normativa delle interfacce digitali, e la tutela effettiva dell'autonomia dell'utente in contesti digitali caratterizzati dalla presenza delle strategie qui in esame.

1. Introduzione

Originariamente inteso come uno dei tanti modi per acquisire un valido consenso, il meccanismo *notice and choice* introdotto, sia in Europa che negli USA, dalle leggi in materia di privacy negli anni Settanta, è divenuto la modalità dominante in Internet [1]. Oggi, quasi ovunque, vengono sottoposti all'attenzione dell'utente online, complessi formulari, o cookie banners, relativi alla tutela della loro privacy, affinché possano acconsentire, o rinunciare, ad usare il servizio desiderato. Il ricorso, così massiccio, a tale meccanismo non era prevedibile cinque decenni fa dagli "architetti della privacy" [2]. In pratica, oggi tale prassi non risulta ottimale per assicurare la protezione della privacy e del libero flusso di informazioni.

Anticipando un'osservazione centrale di questo scritto, nell'era dei Big Data lo scenario appena descritto si complica: aumentano le combinazioni di dati, e per l'utente diventa più difficile aver piena consapevolezza del modo in cui verranno usate le sue informazioni personali nel momento dell'accettazione del banner. Inoltre, secondo la Comunicazione sul Piano d'azione per la democrazia europea [3] l'impatto dei nuovi fenomeni da combattere, tra i quali i messaggi polarizzanti, è amplificato dall'uso di algoritmi opachi controllati da piattaforme di comunicazione frequentemente utilizzate. I dati, utilizzati dagli algoritmi per attuare le tecniche di microtargeting [4] o di profilazione comportamentale, possono essere ottenuti in modo improprio. Non tutti gli usi di quelle informazioni sono rappresentati all'utente nel momento in cui si presta il consenso [5].

Non è un caso, infatti, che dal 2016, con lo scandalo Facebook/Cambridge Analytica, siano emerse anche le preoccupazioni della società digitale intorno alle pratiche di manipolazioni online [6]. I cookie banners, detti anche piattaforme di gestione del consenso (Consent Management Platforms, d'ora in poi: CMPs), assumono quotidianamente un'importanza cruciale per gli utenti e per gli operatori, poichè raccolgono le informazioni personali e tracciano i servizi di cui l'utente usufruisce. Essi possono anche raccogliere l'adesione degli utenti per conto dei siti web. A livello teorico, tali banners dovrebbero garantire la scelta libera ed autonoma degli utenti; tuttavia, nella prassi essi spesso orientano le scelte degli utenti "guidandoli" alla prestazione del consenso. In alcune circostanze, tali strategie, configurano dei c.d. *dark patterns* [7] che influiscono sui processi decisionali dei consumatori, e conseguentemente sulla loro decisione di prestare, o meno, il consenso. Si utilizzano, in

pratica, elementi dell'interfaccia grafica il cui scopo è quello di indurre l'utente a compiere azioni non desiderate, o ad eseguire procedure talmente complesse da scoraggiare l'utente da qualsiasi controllo effettivo sui suoi dati personali.

La maggior parte dei *dark patterns* interferisce con l'interfaccia grafica, altra parte, invece, ostruisce la fruibilità dei contenuti informativi. Nel primo caso, si tratta di una sorta di manipolazione grafica che, per esempio, induce a preferire la visualizzazione di un comando, piuttosto che altri. Nel secondo, i *design* impediscono all'utente di usufruire facilmente delle opzioni di scelta più favorevoli alla tutela della privacy (v. *amplius* § 2).

Si pensi a tutti i casi in cui alcuni messaggi spingono gli utenti all'acquisto di determinati prodotti falsamente indicati in stock, oppure icone persistenti recanti false notifiche. Altri esempi sono il fenomeno di web scraping (letteralmente “raschiare”) o di web data extraction, una tecnica mediante cui dati e informazioni pubblicate su alcuni siti web vengono estratte automaticamente per essere poi riportate su altri siti. In sostanza, si tratta di uno script legato ad un programma per elaboratore che, come un normale visitatore, accede al sito e, anziché procedere con il “copia” e “incolla” manuale del contenuto, “raschia” automaticamente le informazioni che lo interessano, con percorsi simili ad un motore di ricerca che indicizza le pagine web. Inserire nelle condizioni contrattuali del sito web il divieto all'uso di tecniche di web scraping, robots, crawler e simili, è senz'altro una misura preventiva, tra quelle adottate che si è rivelata d'aiuto. Tuttavia, se la pagina web è accessibile pubblicamente, sfuggire del tutto al “raschiamento” dei dati diventa impossibile (vedi *infra* § 6).

In ogni caso, oggi, l'uso di web scraping e di crawler o altri strumenti automatizzati per la raccolta di contenuti on-line è, purtroppo, diffuso. Ad esempio, i motori di ricerca usano continuamente “webbot”, “crowler” o “spider” per visitare miliardi di pagine web e questo permette di fornire all'utente risultati di ricerca pertinenti e accurati. Altri siti utilizzano, inoltre, queste tecniche per offrire agli utenti un confronto sui prezzi dei prodotti presenti online, monitorando costantemente siti terzi, con o senza il loro consenso. Ecco perché tali architetture digitali giocano un ruolo importante nelle scelte di acquisto e di tutela dei dati degli utenti [8]. Quando, infatti, le tecniche per spronare gli utenti a comprare di più o sottoscrivere un maggior numero di servizi diventano *dark patterns*, essi possono essere occasionalmente utilizzati dai service providers per far condividere agli utenti più dati, o scegliere opzioni, che consentano un maggior grado di

intrusione nella *privacy*.

L'acquisizione del consenso dell'utente in presenza di tali strategie, che per certi versi rappresentano pratiche al confine con quelle qualificate come pratiche sleali o ingannevoli, possono in ogni caso incidere e diminuire gli interessi economici dell'utente. L'insidia più profonda consiste, però, nel minare l'interesse ed il valore tutelato per eccellenza dal principio del consenso informato: la libertà di autodeterminazione dell'utente (vedi *infra* § 3).

Le pagine che seguono hanno, pertanto, lo scopo di esplorare i rischi che tali pratiche pongono all'acquisizione dei dati personali e alle potenziali violazioni della normativa in vigore, in primis quella del Regolamento generale sulla protezione dei dati (d'ora in poi: GDPR) [9], e quella in materia consumeristica, dal momento che gli individui sono costretti a prendere decisioni complesse basate su informazioni limitate, mentre chi processa i dati può, forse troppo facilmente, ricorrere al *notice and choice*, con esonero della loro responsabilità.

Sebbene nell'economia dello scritto la prospettiva principale adottata sia prevalentemente europeistica, va dato conto che l'intento di limitare gli effetti negativi dei *dark patterns* sugli utenti non è un obiettivo esclusivamente europeo. Negli anni più recenti, diversi contesti geopolitici hanno affrontato i profili più pervasivi dell'economia basata sui dati, rafforzando, prima di tutto, la tutela del diritto di autodeterminazione correlato all'informazione, attraverso l'imposizione del dovere di trasparenza in capo ai soggetti responsabili della raccolta, archiviazione ed elaborazione dei dati [10]. Ne è un esempio il *California Consumer Privacy Act* (CCPA) [11], entrato in vigore nel 2020, il quale chiarisce che non è sufficiente il consenso ottenuto attraverso pratiche di *dark patterns*, senza peraltro specificare quali di esse saranno identificate come tali. Anche il contesto australiano, pur non avendo ancora legiferato in materia, è attento alle scelte optate in materia dai legislatori europeo e americano e nel dicembre del 2020 ha dato avvio ad una procedura di revisione del Privacy Act 1988 (Cth) (Privacy Act) [12], anche per verificare quali usi dei *dark patterns* potrebbero essere di per sé contrari alla legge e quindi sanzionabili.

Lo scritto è strutturato nel seguente modo: il § 2 descrive la principale tassonomia dei *dark patterns* secondo le più recenti indicazioni espresse nelle linee guida 3/2022 dello European Data Protection Board [13], e identificando, successivamente, quali strategie impatterebbero maggiormente sul quadro giuridico vigente in materia di consenso, sia

nella prospettiva della protezione dei dati (§ 3), che in quella della tutela dell'utente quale consumatore (§ 4). Le questioni più critiche vengono analizzate prevalentemente alla luce delle recenti pronunce della giurisprudenza europea (§ 5), aggiungendo un breve riferimento ad un recentissimo intervento delle Corti americane (§ 6). Infine, alcune considerazioni conclusive contestualizzano il tema entro il più ampio dibattito relativo alle implicazioni della violazione dell'autonomia decisionale dell'utente, per delineare sinteticamente l'importanza dell'aspetto educativo del "cittadino digitale" circa le nuove vulnerabilità nelle quali potrebbe incorrere (§ 7).

2. Le nuove vulnerabilità: dagli algoritmi opachi delle piattaforme di comunicazione alla manipolazione dei dati. Un panorama articolato

Il linguaggio informatico sotteso ai *dark patterns* introduce una vasta gamma di criticità nella costruzione di una c.d. *human-centered interaction (HCI)* tra utente e mondo digitale [14]. Una corretta progettazione degli strumenti tecnologici dovrebbe, infatti, porre al centro l'uomo e la tutela dei suoi diritti, compreso quello all'autodeterminazione garantendo il rispetto sostanziale di princìpi anche etici, oltre che normativi. Tali architetture digitali, invece, con *design* persuasivi inducono gli utenti a compiere determinate azioni senza una piena consapevolezza [15]. Ne consegue che, molto spesso ciò che, a prima vista, sembra configurare una malriuscita architettura digitale di un sito web è, in realtà, il risultato di scelte fatte specificatamente per sfruttare i c.d. *bias* cognitivi degli utenti, aumentando i profitti dei providers [16].

I *dark patterns* sono numerosi e sempre in aumento. Vi sono diversi tentativi di classificazioni tra le quali, ad esempio, tassonomie che riprendono la struttura tassonomica proposta dalla direttiva sulle pratiche commerciali sleali [17]. Qui pare utile prendere le mosse dalla descrizione offerta da un recente parere dello European Data Protection Board espresso nelle Linee Guida 3/2022 intitolate *Dark patterns in social media platform interfaces: how to recognise and avoid them* [18], le quali identificano sei categorie distinte sulla base della modulazione del contenuto o dell'interfaccia [19].

Si tratta di linee guida adottate sulla base dell'art. 60 del GDPR e indirizzate ai designer per evitare l'inserimento di *dark patters* all'interno di siti, piattaforme social e delle piattaforme di gestione del consenso (CMPs, Consent management platforms), le quali sono, in breve, piattaforme centralizzate che possono essere inserite all'interno del sito internet per gestire il consenso degli utenti in materia di privacy [20].

La prima tipologia di *dark patterns* consiste nel c.d. *overloading* (sovraccarico) in cui l'utente viene sottoposto ad una grande quantità di informazioni, richieste o opzioni che lo inducono a fornire più dati del necessario, oppure a consentire involontariamente al trattamento dei propri dati personali.

All'interno di questa prima categoria rientrano tre tipologie specifiche: i *continuous prompting*; il *privacy maze*;e le *too many options*. Entro la prima subcategoria, il *continuous prompting* va inclusa la prassi di riproporre ad ogni accesso la stessa richiesta di informazioni che l'utente ha rifiutato di concedere in un primo momento. Ne consegue che l'utente sarà portato a dare le informazioni richieste pur di non vedere riapparire la richiesta.

Il c.d. *privacy maze* basato sul contenuto si manifesta, per esempio, nel caso in cui le informazioni sulla protezione dei dati, anziché essere collocate negli stessi spazi o in spazi vicini si trovino in diverse schede, traducendosi tutto ciò in disagi per l'utente. Tale situazione si può verificare quando l'informativa privacy, che ai sensi del GDPR può certamente essere costruita su più livelli, viene strutturata per rendere più difficile all'utente la lettura e la comprensione delle informazioni contenute [21].

Per quanto riguarda il *too many options pattern***,** si tratta di un'ipotesi in cui la piattaforma contiene più schede che si occupano della protezione dei dati, compromettendo la capacità dell'utente di fare scelte immediate e consapevoli.

La classe degli *skipping pattern* induce l'utente a saltare alcuni passaggi relativi alla policy dati. Sono sottocategorie il c.d. *deceptive snugness* ed il *look over there*. Il primo è esclusivamente relativo all'interfaccia. Un esempio è dato da funzionalità e opzioni più invasive per i dati abilitate per impostazione predefinita: ciò costituisce un dark pattern poiché solitamente l'utente mantiene l'opzione preselezionata, senza valutare le altre disponibili. Il secondo, il *look over there* riguarda l'interfaccia: è un sistema utilizzato per deviare l'attenzione dell'utente su elementi estranei alla protezione dei dati. Uno degli esempi riportati dalle linee guida è quello relativo alla presentazione di un cookie banner con un link alla cookie policy ed il pulsante per accettare i cookies.

La categoria degli *stirring patterns* fa leva sulle emozioni poichè influisce sulle scelte degli utenti anche attraverso l'impatto visivo delle interfacce. Ne sono sottocategorie gli *emotional steering* e gli *hidden in plain sight patterns*. Nel primo rientrano gli effetti negativi di una ipotetica scelta indotta; nel secondo, le opzioni visive che mettono in mostra l'opzione meno restrittiva a discapito di quella più restrittiva, così che l'utente

ignori l'alternativa, o abbia difficoltà a leggerla.

Gli *hindering patterns*, ostacolano gli utenti in vari modi, come ad esempio rendendo delle azioni difficili, o impossibili. Ne sono sottocategorie i *dead end*, *longer than necessary* e *misleading information*: nel primo caso mancano alcuni link che consentirebbero all'utente di esercitare i propri diritti, o le interfacce sembrano non rispondere ai comandi; nel secondo caso si mettono in discussione delle scelte operate ed il prolungamento inutile del processo di scelta; nell'interfaccia, con la proliferazione dei passaggi dell'opt-out rispetto all'opt-in; nel terzo si usano informazioni ingannevoli, le quali si realizzano con i contenuti facendo credere all'utente che l'informazione da fornire sia indispensabile ad ottenere un risultato. In questo caso specifico, il dark pattern viola il principio di minimizzazione che impone di raccogliere e trattare solo i dati strettamente necessari al raggiungimento delle finalità.

I *fickle patterns* hanno un design poco chiaro: l'interfaccia è incoerente e rende difficile all'utente navigare tra gli strumenti di controllo della protezione dei dati e comprendere lo scopo del trattamento. Sono sottocategorie il c.d. *lacking hierarchy* ed il *decontextualising*. Il primo caso si realizza quando, per esempio, l'informativa resa all'utente non è suddivisa in sezioni o paragrafi, rendendo difficile l'orientamento nella lettura, o nel caso in cui la piattaforma del social differisce dal solito modello di progettazione solo per alcuni aspetti. A livello di interfaccia, ciò avviene quando nelle diverse versioni per dispositivo della piattaforma social le impostazioni sono visualizzate con un simbolo diverso. Il secondo caso, il c.d. *decontextualising***,** decontestualizzazione, si realizza quando un'informazione o la possibilità di controllo della protezione dei dati si trova su una pagina fuori contesto, e diventa difficile da trovare per l'utente perché ha una collocazione non intuitiva.

Il *left in the dark pattern* si ha quando prevale l'incertezza. Sono sottocategorie il c.d. *language discontinuity, conflicting information* o *ambiguous wording* o *information*. La discontinuità linguistica si verifica quando le informazioni sulla protezione dei dati non sono fornite nelle lingue ufficiali del Paese in cui vivono gli utenti, al contrario del servizio.

Le informazioni contrastanti lasciano l'utente incerto su cosa debba fare e sulle conseguenze delle proprie azioni: ad esempio, il social network informa l'utente del controllo sulle proprie preferenze di condivisione ma nello stesso momento specifica che non è possibile modificarle sui contenuti pubblicati [22].

Infine, è *dark* anche l'utilizzo di parole o informazioni ambigue: ad esempio l'uso del condizionale o di una formulazione vaga, che lascia l'utente incerto sull'utilizzo dei dati e finalità di raccolta dei dati. Oppure, attraverso l'utilizzo di un linguaggio specifico o tecnico difficilmente comprensibile da un utente medio.

Da questo sintetico quadro descrittivo emerge che la varietà e diversità delle circostanze configurano problemi che, a seconda delle stesse, possono divenire temi che si intersecano sia con la disciplina della protezione dei dati, che con quella consumeristica [23].

Anche dal punto di vista etico, le preoccupazioni degli utenti aumentano in considerazione del fatto che chi raccoglie i dati ha gli strumenti per manipolare le informazioni degli individui [24]. Conoscere, o dedurre, le preferenze, gli interessi, le amicizie di una persona permette di esercitare una considerevole influenza sulla persona stessa: è possibile conoscere i loro obiettivi, quali sono le loro debolezze e vulnerabilità e quando essi siano meglio influenzabili.

Dal momento che le tecnologie informatiche generano, collezionano e analizzano i dati facilmente, ed in modo conveniente dal punto di vista economico, la stessa preoccupazione ci rende profondamente vulnerabili. Come ricorda Shoshana Zuboff, nel suo libro *The Age of Surveillance Capitalism* [25] le tecnologie informatiche possono dar luogo a modificazioni comportamentali, essendo pervasive, e centrali nel funzionamento della moderna economia dell'informazione, poiché siamo entrati in una nuova epoca della politica economica. Pertanto, pare che in gioco ci sia qualcosa di molto più profondo in gioco rispetto alle pratiche commerciali sleali. L'idea che le interfacce manipolando l'utente, possano rendere il consenso non valido, si basa sugli studi di *behavioral economics*, i quali, contrariamente alle ipotesi di base della teoria economica tradizionale, dimostrano che quando qualcuno compie scelte di mercato (e di altro tipo), i limiti intrinseci delle capacità cognitive umane fanno sì che tali scelte non riflettano il miglior interesse del decisore stesso. Pertanto, l'economia comportamentale probabilmente influenzerà anche la comprensione da parte dei regolatori e dei tribunali di ciò che costituisce un *dark pattern* inammissibile.

I rischi associati a questi tentativi di persuasione aumentano man mano che le piattaforme e i commercianti online combinano l'uso estensivo dei dati personali con interfacce progettate per modellare l'architettura delle scelte. Secondo diversi studiosi, le piattaforme online stanno attuando diverse forme di sorveglianza e manipolazione

degli utenti [26].

Alcuni commercianti stanno, inoltre, utilizzando sempre più spesso pratiche commerciali basate sui dati per sviluppare sollecitazioni artificiali più efficaci e attirare l'attenzione dei consumatori e influenzarli: si parla di *hypernudging* [27], come una forma manipolativa, la quale comporta la compromissione dell'autonomia degli utenti, dal momento che mina sia l'autenticità delle informazioni, sia la capacità decisionale interferendo con la stessa.

3. Dark patterns e consenso dell'utente nel quadro legislativo plurisettoriale europeo

La scelta di un'architettura digitale influisce sulla presentazione delle informazioni all'utente e, conseguentemente, sulle decisioni di quest'ultimo. Tale situazione pone il tema del consenso al crocevia di diverse discipline: principalmente quella della protezione dei dati e quella consumeristica delle pratiche commerciali scorrette dal momento che molti *dark patterns* potrebbero coincidere con alcune di esse, o configurare i tratti tipici, o presentare caratteristiche analoghe a quelle di clausole classificate come sleali.

Per chiarezza espositiva, il presente paragrafo sarà dedicato all'analisi della tematica entro la normativa europea dedicata alla protezione dei dati; mentre, invece, il successivo paragrafo esplorerà il tema nella prospettiva della tutela dei consumatori (cfr. § 4).

Il profilo del consenso dell'utente in queste situazioni rimane tra i temi più delicati e controversi nel contesto europeo, così come in altri contesti stranieri.

In generale, si può osservare che, sebbene la tutela del libero consenso sia stata già prevista dalla direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [28], i cambiamenti introdotti dal GDPR muovono dalla consapevolezza che gli utenti si trovano spesso di fronte a politiche di privacy standard e offerte "prendere o lasciare" [29].

A fronte del fenomeno in esame, le Autorità Garanti della protezione dei dati in Europa si sono chieste se il rispetto della normativa sulla privacy sia sufficiente, ovvero se sia, invece, necessaria una verifica più approfondita del rispetto sostanziale delle disposizioni alla luce delle nuove sfide [30]. In Europa, già è possibile individuare e qualificare alcuni *dark patterns* sulla base della mancanza di *compliance* al

Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio (c.d. General Data Protection Regulation o GDPR). Tra questi, vi è certamente l'utilizzo di impostazioni di default invadenti per la privacy, l'occultamento di opzioni "*privacy friendly*" e la previsione di percorsi eccessivamente complessi per l'utente per poter intervenire sul trattamento dei propri dati.

Ad una prospettiva generale, il GDPR stabilisce i principi fondamentali per la validità del consenso. Tra questi princìpi vi è certamente quello che circoscrive il consenso alle sole finalità dichiarate.

Come noto, il consenso deve essere un atto positivo con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare i trattamenti dei propri dati personali legati esclusivamente alla finalità per la quale il consenso è stato richiesto (26; art. 4(11). D'altro canto, il consenso, ai sensi dell'art. 6, prg. 1, lett. *a*) del GDPR, rappresenta una delle condizioni di liceità per il trattamento dei dati personali.

In particolare, la libertà di autodeterminazione è presupposto imprescindibile del consenso, ne forgia il valore e ammanta di significato giuridico la sua manifestazione all'esterno.

Risulta, quindi, di fondamentale importanza stabilire quando il consenso possa considerarsi effettivamente libero, di guisa da costituire idonea base giuridica del trattamento dei dati.

Sul punto, sia l'art. 7 del GDPR che le Linee guida del Working Party 29 (c.d. WP29) [31] in materia di consenso adottate dallo European Data Protection Board, considerano l'esistenza di eventuali condizionamenti un indice di carenza di libertà nel consenso. Infatti, a chiarire meglio il significato di tali requisiti entro le architetture del web più recenti, come i social media, sono state le Linee Guida 05/2020 sul consenso ai sensi del Regolamento (UE) 2016/679 che si rivolgono ai providers dei social media, i quali richiedono il consenso degli utenti per diverse finalità [32]. Le piattaforme di social media non devono eludere la capacità degli interessati di prestare liberamente il consenso, attraverso disegni grafici o formulazioni che impediscono loro di esercitare tale volontà. A questo proposito, l'art. 7 (2) GDPR afferma che la richiesta di consenso deve essere presentata in un modo che sia chiaramente distinguibile da altre questioni, in una forma intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Gli utenti delle piattaforme di social media possono fornire il consenso per gli annunci o tipi speciali di analisi durante il processo d'iscrizione, e in una fase successiva

attraverso le impostazioni di protezione dei dati. In ogni caso, come dichiarato nel considerando 32 del GDPR, il consenso deve sempre essere fornito con un chiaro atto affermativo, in modo che le caselle pre-selezionate, o l'inattività degli utenti, non siano considerati alla stregua di un atto di consenso [33]. Merita qui un cenno un aspetto che verrà trattato più diffusamente nel prosieguo (vedi *infra* § 4): le caselle pre-selezionate, le quali richiedono un'azione positiva per l'opt-out, sono esplicitamente individuate nel GDPR come una forma non valida di consenso (26, considerando 32). Normalmente, la revoca del consenso dovrebbe essere semplice come la sua prestazione [34]: per un modello valido, dopo il conferimento del consenso, ad ogni accesso dovrebbe essere disponibile lo stesso modulo per il ritiro dello stesso consenso, cosa che invece non avviene.

Per quanto riguarda l'aspetto specifico dell'adesione dell'utente ad un'interfaccia di un social media, il principio di riferimento è l'art. 5 del GDPR ("Principi applicabili al trattamento dei dati personali"), il quale pone dei prerequisiti per la valutazione di eventuali *dark patterns*. Tra questi, particolare rilevanza assume il principio di trasparenza, che viene esplicitato, altresì, nel Considerando 39 del Regolamento dove si afferma che «dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati» [35]. L'equo trattamento dei dati è alla base del principio di trasparenza come già evidenziato nelle linee guida sulla trasparenza: ciò rende il trattamento dei dati più comprensibile per gli interessati e, in ultima analisi, permette loro di avere il controllo sui dati. Tuttavia, disporre di più informazioni non significa necessariamente che si tratti di informazioni più chiare. Troppe informazioni irrilevanti o confuse possono oscurare aspetti importanti del contenuto o ridurre la probabilità di trovarli. Quindi, il giusto equilibrio tra contenuto e presentazione comprensibile dello stesso è cruciale: la mancanza di tale equilibrio potrebbe configurare un dark pattern.

Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili, e gli utenti dovrebbero essere sensibilizzati ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento». Nel Considerando n. 58 si specifica, inoltre, che «il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato

siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione» [36].

Il giudizio di validità del consenso si base sulle disposizioni di cui all'art. 4 ("Definizioni") e art. 7 ("Condizioni per l'accesso") del GDPR o altri obblighi specifici, come l'articolo 12 ("Informazioni, comunicazioni, e modalità trasparenti per l'esercizio dei diritto dell'interessato") GDPR. Tale ultima disposizione richiede ai responsabili del trattamento di adottare misure adeguate per fornire qualsiasi comunicazione relativa ai diritti degli interessati, nonché qualsiasi informazione, in una forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Questo requisito non è, tuttavia, limitato alle comunicazioni sulla protezione dei dati o ai diritti degli interessati, ma si applica piuttosto a qualsiasi informazione e comunicazione relativa al trattamento dei dati personali.

Infine, dato il modo in cui si presentano i *dark patterns*, è opportuno ricordare i requisiti di protezione dei dati per progettazione e per impostazione predefinita ai sensi dell'articolo 25 ("Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita") del GDPR: essi giocano un ruolo fondamentale, poiché applicarli prima di lanciare un progetto di interfaccia aiuterebbe i fornitori di social media a evitare di porre in essere strategie di *dark patterns* [37].

Per una piena *compliance* alla normativa privacy è, infatti, importante che già in fase di progettazione si tengano in particolare considerazione elementi che consentono all'utente di avere un'effettiva consapevolezza delle modalità del trattamento e della qualità dei dati del trattamento stesso, fornendo all'utente la possibilità reale di intervenire attraverso l'esercizio dei diritti ad esso riconosciuti dalla normativa vigente.

Corretta informazione e pieno controllo sulla qualità dei dati trattati sono elementi essenziali per garantire un'effettiva ed efficace protezione dei dati personali. Tale protezione nell'ambito dei servizi tecnologici inizia già con una "responsabile" progettazione dell'interfaccia utente (o UI, *User Interface*), ossia con la corretta progettazione di ciò che si frappone tra una macchina e un utente, consentendo l'interazione reciproca e rendendo più intuitiva e scorrevole la navigazione e l'utilizzo di servizi.

Attraverso un'attenta progettazione dell'interfaccia utente, infatti, è possibile incoraggiare o scoraggiare gli utenti all'esercizio dei propri diritti, anche in materia di privacy, o orientare le loro scelte in una direzione di interesse per il fornitore del

servizio.

Sinteticamente, con l'espressione "*data protection by design*" si intende, quindi, l'obbligo in capo al titolare di social network o delle piattaforme di mettere in atto misure tecniche ed organizzative adeguate per integrare nel trattamento dei dati, le necessarie garanzie volte a tutelare i diritti degli interessati ergo, l'esclusione di forme manipolative. Il titolare dovrà, quindi, adottare misure tecniche ed organizzative che spingano verso una maggiore riservatezza del dato [38].

Ad interferire prepotentemente con l'acquisizione di un consenso valido ai sensi delle disposizioni fin qui richiamate, vi sono i *cookies* e altri strumenti di tracciamento i quali rappresentano un aspetto centrale, essendo file di testo creati da un web server del sito che contengono dati e informazioni sull'utente. Sul punto, a livello nazionale, le recenti Linee guida del 10 giugno 2021 adottate dal Garante per la protezione dei dati personali [39] sono intervenute per assicurare la conformità di tutti i siti web con il GDPR e la direttiva ePrivacy (direttiva 2002/58/CE) [40]. Le Linee distinguono i diversi tipi di cookies: quelli tecnici, i quali rendono il sito web veloce e performante; ed i cookies di profilazione utilizzati per raggruppare gli utenti in profili omogenei, e impostare messaggi personalizzati. In particolare, è importante diversificare gli strumenti che possono essere gestiti attivamente dall'utente, ad esempio attraverso il rifiuto del consenso, come i cookies tecnici che identificano gli utenti che hanno già visitato il sito in precedenza; ed i cookies di profilazione che consentono di ottenere più informazioni sulle attività svolte dall'utente; dagli altri identificatori passivi, e cioè quelli che non possono essere gestiti autonomamente dall'utente, come il *fingerprinting*.

La validità del consenso dipende, quindi, dalle modalità di raccolta dello stesso: se si tratta di un'operazione di scrolling, o scroll-down, per esempio, non si configura un'operazione positiva ai fini di prestare il consenso valido. L'obiettivo è dunque quello di evitare i "falsi positivi", ovverosia l'errata interpretazione di azioni casuali come appunto l'espressione positiva del consenso tramite lo scrolling [41].

In pratica le linee guida hanno cercato di implementare regole più severe e dettagliate sulla protezione dei dati personali degli utenti.

Unica eccezione riconosciuta dal Garante Privacy: qualora vengano adottate delle soluzioni sul sito web idonee a manifestare in maniera inequivoca la volontà da parte dell'utente di fornire il proprio consenso al trattamento dei dati anche in presenza di strategie come quelle in esame, esse si potranno ritenere "in linea con i requisiti di

legge". Tuttavia, anche le modalità informative rilevano ed incidono in particolar modo sulla validità del consenso acquisito: se, infatti, gli utenti sono destinatari di una quantità eccessiva di informazioni funzionale a disincentivare la lettura, il consenso apprestato può essere considerato alla stregua di "consenso forzato" alle condizioni speciali ivi indicate. E, analogamente, se il rifiuto del consenso implica automaticamente il rifiuto del servizio, tale consenso non può essere considerato libero, "granulare", e specifico, come richiede il GDPR: in altri termini, il consenso "impacchettato" con l'accettazione dei termini e delle condizioni di un fornitore di social media non si qualifica come "liberamente dato", e implica che il responsabile del trattamento dei dati gestisca e controlli dati personali che non sono necessari per l'esecuzione del contratto.

4. (Segue): dark patterns e tutela dell'autonomia decisionale del consumatore-utente

Come anticipato in apertura al paragrafo precedente, il quadro dei principali riferimenti normativi applicabili ai casi di violazione del consenso dell'utente dovuti alla presenza di architetture "dark" dev'essere completato con la diversa prospettiva della tutela dei consumatori, la quale analogamente a quella dedicata alla protezione dei dati, mira a potenziare gli strumenti di tutela a disposizione degli utenti-consumatori, in linea con gli obiettivi del *New deal for consumers* adottato dalla Commissione europea per modernizzare le regole adattandole agli sviluppi del mercato [42].

Anche la disciplina consumeristica europea attribuisce un valore prioritario all'autonomia decisionale del consumatore [43]: considerata la situazione di asimmetria informativa [44].

È bene partire da una constatazione che permetta di capire il legame tra le due discipline. Nelle more dell'entrata in vigore del GDPR, molti data controller colsero l'occasione, non solo per aggiornare le loro policy in materia di privacy, ma anche per riconsiderare il fondamento giuridico sul quale poggiava il loro processo di utilizzo e raccolta dei dati personali: diventando più stringente l'onere della prova per ottenere il consenso dell'utente all'uso dei dati personali, molti providers hanno riconsiderato il fondamento del consenso richiamando, non più l'art. 6(1(a) del GDPR, bensì l'art. 1(b), quale condizione necessaria per l'esecuzione del contratto. Da tale cambiamento consegue che al *data subject* che ha sottoscritto il contratto per prestazione di servizi acconsentendo al trattamento dei suoi dati può venire applicata la disciplina

consumeristica, poiché l'utente è considerato anche alla stregua di consumatore. Le regole relative alle pratiche commerciali si estendono, così, ai modi in cui vengono processati i dati [45].

Sul piano generale, la protezione apprestata all'utente dalla disciplina consumeristica del consumatore è molto più estesa di quella apprestata dalla *data protection regulation* poiché, per esempio, include gli advertising e le circostanze precontrattuali. Sul punto la giurisprudenza tedesca ha avuto occasione di affermare che lo scopo della tutela dei dati dell'utente potrebbe essere ricompreso nello scopo della protezione del consumatore [46]. Conseguentemente, seguendo questa linea interpretativa, ogni interfaccia grafica che orienta l'utente-consumatore ad accettare i termini contrattuali delinea una barriera materiale che, al pari di ogni termine contrattuale, può indurre il consumatore alla conclusione del contratto.

Per di più, considerando i recenti interventi legislativi che consacrano il valore economico del dato personale, l'utilizzo di un dark pattern per operazioni di *nudging* in relazione all'acquisto di un bene o alla sottoscrizione di un contratto per prestazioni di servizi online, potrebbe configurare una pratica sleale.

Il report pubblicato nello scorso aprile 2022 in materia di *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization*, ad opera dell'EU Innovation Council and SMEs Executive Agency su mandato della Commissione europea, ha enfatizzato la mancanza di consapevolezza nei consumatori circa il carattere sleale di molte pratiche online [47]. La valutazione giuridica condotta per questo studio mostra che la regolamentazione delle pratiche commerciali sleali nell'ambiente digitale si colloca all'intersezione tra la protezione dei consumatori, la protezione dei dati e altri strumenti pertinenti del quadro giuridico dell'UE, compresa la legislazione nuova e futura come il Digital Services Act, il Digital Markets Act, l'AI Act e il Data Act.

Anche la European Consumer Organization (BEUC) [48] è recentemente intervenuta con il documento *Dark patterns and the EU Consumer Law Aquis* [49], per esprimere delle raccomandazioni circa la necessità di rafforzare la tutela offerta dalla direttiva 2005/29/CE sulle pratiche commerciali sleali [50], unitamente alla direttiva 2011/83/EU sui diritti dei consumatori [51], e la direttiva 93/13/CEE concernente le clausole abusive nei contratti stipulati con i consumatori [52], e successive modifiche avvenute ad opera della direttiva (Ue) 2019/2161 [53].

In linea teorica, è ingannevole la pratica commerciale che contenga informazioni false o non veritiere o sia tale da indurre in inganno il consumatore medio – anche in ipotesi di informazione corretta – ovvero sia tale da indurlo a decisioni che altrimenti non avrebbe assunto.

La giurisprudenza ha, nel tempo, chiarito che fattori cognitivi ed economici possono compromettere la libertà di autodeterminazione: quando un consumatore mediamente avveduto percepisce il rischio associato ad un determinato comportamento, può essere indotto ad assumere scelte non in linea con l'opzione più ragionevole [54]. Per fare un esempio concreto, si può tornare a considerare ancora una volta il valore economico dei dati e, più in dettaglio, delle informazioni riguardanti le preferenze dei consumatori: se il consumatore non viene informato che i dati richiesti per l'accesso al servizio scelto saranno usati per fini commerciali, ciò può configurare una pratica commerciale sleale ai sensi dell'art. 7 della direttiva 2005/29/Ce, poiché vengono celati profili che hanno un impatto sulla transazione. Usare un'architettura digitale per offuscare l'elaborazione di dati personali equivale ad omettere informazioni, e tutto ciò non solo viola l'obbligo di trasparenza previsto dal GDPR, ma altresì l'art. 7(2) e Annex I (n. 22) della Direttiva 2005/29/Ce. Ancora una volta emerge la maggior estensione della tutela consumeristica che disciplina il processo di elaborazione dei dati nell'ambito precontrattuale, lasciato, invece, privo di tutela dalla disciplina in materia di trattamento dei dati.

A tal proposito il BEUC raccomanda di introdurre un obbligo generale di "lealtà by design", e di includere, nell'Annex I della direttiva 2005/29/Ce il divieto della pratica *confirm-shaming* che implica l'utilizzo di linguaggio ad impatto emotivo per orientare l'utente a compiere una determinata scelta.

Sebbene a fronte della diversa estensione della tutela la disciplina della protezione dei dati e quella consumeristica hanno, per contro, svariati profili di assonanza e punti di contatto in materia di consenso. Dal punto di vista terminologico, ad esempio, il considerando 42 del GDPR prevede «una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e *non contenga clausole abusive*» [55]. Tale specificazione ricordata, altresì, nell'art. 7 (2) [56], e 12 (1) [57] del medesimo Regolamento, richiama il criterio impiegato per valutare se una pratica sia da considerare sleale, ossia contraria alle norme di diligenza professionale, o falsa, o idonea a falsare in misura rilevante il comportamento economico del consumatore

medio, previsto dall'art. 5 della Direttiva sulle clausole commerciali sleali 2005/29 [58], la cui portata è oggetto di numerose interpretazioni e chiarimenti ad opera della Corte di Giustizia europea [59].

Infine, per completare il quadro della tutela consumeristica specificatamente dedicata all'utente online, va dato conto che il *Digital Services Act* (DSA) [60], come emendato dalla Commissione europea il 20 gennaio 2022 [61] costituisce, in combinazione con il *Digital Markets Act* (DMA), la riforma più significativa che mira ad esaminare l'allineamento delle rispettive agende politiche in materia di protezione dei dati e privacy, protezione dei consumatori e diritto della concorrenza.

Uno dei principali obiettivi del DSA è quello di creare uno spazio digitale più sicuro in cui i diritti fondamentali di tutti gli utenti dei servizi digitali siano protetti. L'atto introduce riforme per la gestione di contenuti online dannosi, la protezione dei diritti fondamentali degli utenti online, le restrizioni sulla raccolta di dati personali per scopi pubblicitari e le limitazioni sulla pubblicità comportamentale [62](*web trackers* e *behavioral advertising*), strumenti sempre più utilizzati per tracciare i nostri comportamenti online e raccogliere dati personali.

Vi è chi propone l'adozione di una *Consent for Advertising Direttiva* (CAD) che possa andare oltre le lacune della *Cookie Law* attualmente vigente, migliorando la protezione dei dati a prescindere dalla tecnologia usata per aumentare la trasparenza circa le modalità di raccolta dati ed evitare violazioni del GDPR [63].

Relativamente agli specifici cambiamenti introdotti nel DSA per far fronte ai *dark patterns*, i providers dei servizi di intermediari saranno soggetti a restrizioni nell'impiego di determinate interfacce (struttura, design o funzionalità), per non compromettere la capacità degli utenti di prendere decisioni o fare scelte libere, autonome e informate (*ex* art. 13-a). I destinatari dei servizi dovrebbero essere autorizzati a prendere decisioni su questioni come l'accettazione e le modifiche di termini e condizioni, pratiche pubblicitarie, privacy e altre impostazioni e sistemi di raccomandazioni senza essere soggetti a pratiche che, sulla base di pregiudizi cognitivi, spingono gli utenti ad acquistare beni o servizi che non vogliono, o a rivelare informazioni personali che preferirebbero non rivelare (considerando 39-a) del DSA.

Nonostante i termini generici dell'intervento, l'Atto specifica da quali pratiche dovranno astenersi i providers, bandendo, in particolare, quelle volte a: attribuire diversa visualizzazione alle opzioni per il consenso dell'utente (c.d. *misdirection technique*);

chiedere ripetutamente l'accettazione della clausola di consenso quando essa è stata previamente rifiutata (ad esempio con le forme di pop-up che interferiscono con la navigazione); mettere pressione all'utente affinché cambi configurazione o setting dopo aver espresso una scelta, o rendere difficile, o nascondere, una procedura di cancellazione di un servizio rispetto alla procedura di accettazione [64].

Con queste iniziative il legislatore europeo non interferisce con i requisiti del consenso per processare i dati personali previsti dal GDPR, ma intende contribuire a chiarire le "zone grigie" del GDPR intorno all'uso dei *dark patterns* che influiscono sull'ottenimento del consenso dell'utente. Ciò, per esempio, si estrinsecherà nel divieto di *dark patterns* che rendono il procedimento per rifiutare i c.d. *cookie walls* più difficile rispetto alla loro accettazione, attraverso tecniche come per esempio la necessità di cliccare più e più volte lo stesso comando per rigettare l'opzione, o utilizzando colori pallidi per il comando di rigetto, rispetto ai colori accesi del comando per l'accettazione [65]. I siti web dovranno, quindi, in seguito all'entrata in vigore delle norme del DSA assicurare la medesima conformazione grafica per le opzioni di rifiuto e accettazione del consenso.

Infine, il DSA prevede che le piattaforme online offrano sistemi di supporto per gli utenti (attraverso suggerimenti, ranking e informazioni prioritarie, utilizzo di testi o tecniche di visualizzazione per informazioni che richiedono più attenzione), assicurando, in altri termini, di non influire sul suo comportamento del consumatore attraverso strategie di *dark patterns*.

5. La tutela del consenso dell'utente tra percorsi giurisprudenziali già tracciati e nuovi

Quando si esaminano gli sviluppi della digitalizzazione, il dato interpretativo giurisprudenziale è fondamentale per capire in quale misura vengono responsabilizzati i soggetti che sono nella miglior posizione per garantire la tutela dell'utente, quali providers e responsabili del trattamento dei dati, in conformità agli obiettivi espressi nella normativa.

Se consideriamo il valore fondamentale tutelato dal diritto di essere informato in capo all'utente, ossia la libertà di autodeterminazione [66], pare utile prendere le mosse dalla constatazione che si tratta di una linea interpretativa per la quale la giurisprudenza ha certamente giocato un ruolo chiave in passato.

Considerando l'evoluzione della giurisprudenza domestica in settori chiave del diritto

civile, come per esempio quello della responsabilità medica, si coglie chiaramente che, in circostanze critiche, nel giudizio di bilanciamento dei diritti fondamentali sottesi alla protezione apprestata, il bene ultimo tutelato è il diritto alla libera autodeterminazione del soggetto che presta il consenso [67].

La giurisprudenza europea in materia di tutela del consenso dell'utente-consumatore nel contesto online, convoglia sia posizioni ormai consolidate circa la natura del consenso del data-subject sulla disposizione dei propri dati, sia recenti linee interpretative che affrontano i profili più innovativi in materia, per tutelare l'autodeterminazione dell'utente vittima di meccanismi *dark patterns*, e più in generale meccanismi di c.d. web scraping. Tra questi ultimi, per esempio, il c.d. consenso implicito, che si verifica quando si continua ad utilizzare un sito web senza opporsi attivamente a una *notice*, non stabilirà una base giuridica valida per considerare i cookies o il processo di raccolta dei dati come una condizione sufficiente per raccogliere il consenso dell'utente [68], poiché non comporta un'azione dell'utente.

In merito alla natura del consenso sulla protezione dei dati, i giudici di Lussemburgo confermano che ai sensi dell'art. 8 par. 2 della Carta dei diritti fondamentali, l'istituto è finalizzato a tutelare i dati personali, ed in quanto tale, deve essere libero, specifico e inequivocabile come previsto dall'art. 6 del GDPR [69]. D'altro canto, lo stesso GDPR e le linee guida del WP29 si pongono in continuità con principi consolidati in tema di consenso libero, anche ad opera delle singole giurisdizioni degli Stati membri [70]. I giudici di legittimità italiani, ad esempio – con il caso deciso da Cass. civ., sez. I, del 2 luglio 2018, n. 17278 – hanno nel tempo introdotto delle distinzioni importanti tra la nozione di consenso entro la disciplina negoziale del codice civile e quella ai fini della normativa sulla protezione dei dati [71]: quest'ultima, infatti, in analogia a quanto avviene nell'ambito medico, prevede che il consenso sia prestato da un soggetto informato ai sensi degli artt. 13 e 14 del GDPR. A tal fine, per esempio, la Suprema Corte ha precisato che, in presenza di determinate circostanze, non tutti i condizionamenti inficiano la volontà di autodeterminazione dell'utente, e quindi la validità del consenso prestato, poiché non è necessariamente condizionato il consenso al trattamento dei dati non funzionali alla stipula di un servizio fungibile e rinunciabile di cui si chiede la prestazione, anche se il consenso è condizione per poter usufruire del servizio medesimo.

La Corte di giustizia europea ha contribuito all'identificazione delle specifiche

condizioni in presenza delle quali il consenso risulta effettivamente libero ed informato al fine di costituire idonea base giuridica del trattamento dei dati.

Per esempio, la stessa Corte di Lussemburgo ha già avuto occasione di scoraggiare le pratiche di *dark patterns* quali condizioni che ostacolano la libera determinazione dell'utente, rimarcando il fatto che, ai fini di essere valido, il consenso dev'essere espresso con un'azione positiva, distinta rispetto all'attività che l'utente vuole perseguire. Nel caso di specie una società tedesca aveva utilizzato una casella di spunta preselezionata mediante la quale gli utenti abituali, che aspiravano a partecipare a giochi a premi, esprimevano il consenso all'installazione di cookies diretti a raccogliere informazioni a fini pubblicitari. La Corte ha sostenuto che il consenso all'installazione e consultazione di cookie sull'apparecchiatura terminale del soggetto interessato non è validamente manifestato in presenza di una casella di spunta preselezionata che l'utente deve, peraltro, deselezionare al fine di negare l'autorizzazione al trattamento dei propri dati [72].

D'altro canto tali caselle, analogamente a quanto avviene per il modulo del consenso informato utilizzato in medicina (formulario)[73], sono state valutate come una forma non valida di consenso già prima della metà degli anni Novanta.

Inoltre, la necessità di un'azione positiva che provi la comprensione dell'informativa da parte dell'utente è stata già enfatizzata anche con riguardo alla terminologia impiegata: meccanismi di consenso che enfatizzano termini come “agree” o “allow”, più di termini quali “reject” o “block”, rappresentano un approccio che non è conforme, poichè il sistema sta influenzando gli utenti affinché optino per l'opzione di accettazione [74].

Dev'essere valorizzato in pratica, in armonia con la logica del Gdpr, il carattere realmente comprensibile delle informazioni senza le quali, appunto, il consenso (fosse anche quello contrattuale) viene privato della sua vera natura di manifestazione di volontà tanto libera quanto consapevole, alimentando, invece, la c.d. “*consent (and reading)-fatigue*” [75].

Varie autorità europee hanno affrontato, in tempi recenti, casi significativi in questa prospettiva. In materia di trasparenza delle informazioni, una delle prime autorità europee che ha sanzionato Facebook è stata l'Autorità garante della concorrenza italiana la quale, alla fine del 2018, ha multato il celebre *social network* per 10 milioni di euro riconoscendo che la stessa aveva posto in essere pratiche commerciali scorrette. La sanzione dell'Antitrust è stata poi rivista dal T.A.R. Lazio, sez. I, nella sentenza del 18

dicembre 2019 – 10 gennaio 2020, n. 260 e 261 [76]. La condotta rilevata dall'Antitrust riguardava il *claim "È gratis e lo sarà per sempre"* con cui Facebook induceva l'utente a registrarsi sulla propria piattaforma. Il T.A.R. Lazio ha confermato la sanzione dell'AGCM sul punto, affermando che Facebook avrebbe dovuto informare l'utente che con l'attivazione di un account in realtà cedeva i propri dati personali anche per finalità commerciali. Secondo il T.A.R., il *social network* è infatti tenuto a rispettare gli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore [77].

È significativo in questa sede richiamare, altresì, l'operato della nostra giurisprudenza di legittimità che, recentemente – in particolare con l'Ordinanza 14381/2021 – si è spinta a valutare il contenuto dell'informazione nei casi di decisioni automatizzate (*ex* art. 22 GDPR), in relazione all'applicazione degli artt. 13(2)(f) e 14(2)(g) del GDPR focalizzandosi, quindi, sul contenuto dell'informativa ai fini della validità del consenso. La Corte ha, in queste circostanze, chiarito che in ipotesi di processo automatizzato, è importante che l'utente sia informato circa le logiche usate dall'algoritmo qualora queste incidano significativamente sulla sua persona [78].

6. La decisione della U.S. Ninth Circuit of Appeals del 18 aprile 2022

Nell'economia di queste pagine non è previsto un approfondimento generale del tema in ordinamenti diversi da quello europeo. Ciò non toglie che, come anticipato in apertura, sia doveroso dar conto del fatto che molte altre giurisdizioni sono proattive nell'implementazione di raccomandazioni e proposte legislative per tutelare l'utente dai *dark patterns*, e nella ricerca di soluzioni operative. Tra tutte, l'esperienza americana appare particolarmente significativa in materia di protezione del diritto dell'utente ad essere informato circa l'utilizzo dei suo dati, basando la relazione business-user con riguardo alla tutela dei dati personali su presupposti contrattuali informati all'approccio *notice and choice*, ed avendo già avviato, da tempo, un vivace dibattito dottrinale sull'adeguatezza dei rimedi contrattuali ordinari esperibili dall'utente danneggiato da disseminazione non autorizzata o indesiderata dei propri dati [79].

Per anni, infatti, i casi di web scraping di dati sono stati denunciati sul presupposto della violazione del *Computer Fraud and Abuse Act (CFAA)* [80], originariamente emanato dal Congresso nel 1986 per combattere varie forme di crimini informatici, come hackeraggio e intrusioni non autorizzate nei sistemi informatici o database. Nel tempo,

tale Act è stato oggetto di numerosi emendamenti in senso espansivo, poiché i legislatori hanno identificato nello stesso lo strumento idoneo per rispondere alle nuove criticità emergenti dagli sviluppi tecnologici. Anche l'interpretazione giurisprudenziale ha, per lungo tempo, incluso nella protezione apprestata dall'*Act* molte forme di accesso non autorizzato a siti e dati. Un caso di scuola, in tal senso, è rappresentato da *Facebook v. Power.com* [81], laddove Facebook citava in giudizio una piccola startup – Power.com – che aggregava social media per accedere a tutti i diversi account ivi presenti attraverso un'unica interfaccia e pubblicare, così, messaggi su più piattaforme. Per farlo, gli utenti dovevano fornire il proprio login a Power.com, che accedeva agli account ivi presenti, estraendo i dati. In questo caso, l'utente concedeva volontariamente i propri dati di accesso. Su ricorso di Facebook, la Corte ravvisò violazione del CFAA ordinando la dismissione del servizio offerto da Power.com, e dando, così, indirettamente luogo all'aumento del potere di Facebook rafforzando la sua posizione dominante.

Solo in tempi più recenti, nonostante molti casi rimangano ancora problematici, sia a livello normativo che giurisprudenziale, si assiste ad un'inversione di rotta volta a circoscrivere più dettagliatamente le situazioni di web scraping da sanzionare e vietare. A partire dal 1° gennaio 2023, ad esempio, entrerà in vigore il *California Consumer Privacy Rights Act* (CPRA) [82] il quale interviene specificatamente sull'impatto dei *dark patterns* per delineare la validità del consenso dell'utente nel processo di elaborazione dei dati: riformando il preesistente *California Consumer Privacy Act* (CCPA) [83], il CPRA afferma che «l'accordo ottenuto attraverso l'uso di *dark patterns* non costituisce consenso valido ai sensi del CCPA» [84].

Nel marzo 2021, inoltre, il California Office of Administrative Law ha approvato il divieto di utilizzare dark patterns volti ad oscurare la procedura di opt-out dall'accordo con il quale si dispone delle proprie informazioni personali o che compromettono l'opzione dell'utente di non sottoscrivere il servizio. In pratica, per rispettare il nuovo California Consumer Privacy Act (CCPA) le aziende dovrebbero ripensare alle modalità di ottenimento da parte dei consumatori per precludere l'ipotesi di consenso ottenuto attraverso l'uso di dark patterns.

È il formante giurisprudenziale che più di ogni altro ha concretizzato la suddetta inversione di rotta, prediligendo un orientamento volto a circoscrivere le ipotesi di violazione del consenso in casi come quelli in esame: la novità più rilevante è opera di

un recentissimo *landmark case* dello scorso 18 aprile 2022, con il quale la US Corte d'appello del nono circuito ha chiuso una lunga battaglia legale condotta da LinkedIn per impedire alla compagnia rivale Hiq Labs di utilizzare i dati dei profili pubblici dei propri utenti (web scraping) al fine di analizzare le relazioni tra professionisti [85]. Diversamente dal caso Power.com, la Corte del nono circuito ha riaffermato la sua decisione originaria negando che l'estrazione di dati ad accesso pubblico degli utenti di LinkedIn da parte della società Hiq Labs, costituisse violazione del *Computer Fraud and Abuse Act*, CFAA.

La differenza sostanziale rispetto al precedente Power.com sta nella natura pubblica dei dati degli utenti: HiQ, per esempio, non ha bisogno di accedere a LinkdIn attraverso un processo di log-in per poter disporre dei dati degli utenti. Va tenuto conto che il giudizio della Corte d'Appello è avvenuto a seguito del rinvio della Suprema Corte [86], la quale chiese di riconsiderare il caso alla luce della famosa decisione Van Buren che, l'anno precedente, si era preannunciata sulle difformità interpretative con la legge federale, il *Computer Fraud and Abuse Act, 18 U.S.C. Section* 1030 ("CFAA") [87], finalizzata, *inter alia*, a proteggere i computer del luogo di lavoro, e le informazioni in essi memorizzate, da diversi tipi di accesso non autorizzati, sia da parte di dipendenti, come avvenuto nel caso del ricorrente Nathan Van Buren (vicenda nota come *Van Buren's "gates-up-or-down inquiry"*), sia da parte di ex dipendenti o concorrenti [88]. In sintesi, si tratta di un caso della Corte Suprema degli Stati Uniti che ha riguardato il *Computer Fraud and Abuse Act* (CFAA) e la sua definizione di "accesso autorizzato". Nel giugno 2021, la Corte Suprema si era pronunciata in merito al requisito che "supera l'accesso autorizzato" per accedere a file e altre informazioni in relazione all'accesso intenzionale a un sistema informatico. Il linguaggio della CFAA aveva da tempo creato una spaccatura nella giurisprudenza, e la decisione della Corte ha ristretto l'applicabilità della CFAA nel perseguire i crimini informatici e di cybersecurity.

In linea di continuità, con il precedente Van Buren, dunque, in *LinkedIn v. HiQ*, la Corte d'appello del nono circuito ha rigettato l'interpretazione di LinkedIn, osservando che il CFAA è meglio inteso come una legge "anti-intrusione" e non come un atto basato sul concetto di "appropriazione indebita", per questo motivo qualora il caso riguardi un sito ad un accesso pubblico, il CFAA non è violato.

Ancora la Corte osserva che il CFAA delinea tre tipi di "scenari" informatici: (1) computer per i quali l'accesso è aperto al pubblico in generale e l'autorizzazione non è

richiesta; (2) computer per i quali l'autorizzazione è richiesta ed è stata concessa; e (3) computer per i quali l'autorizzazione è richiesta ma non è stata concessa (o, nel caso del divieto di superare l'accesso autorizzato, non è stata concessa per la parte del sistema a cui si accede). I profili pubblici di LinkedIn, disponibili a chiunque abbia una connessione a Internet, rientrano nella prima categoria. Per quanto riguarda i siti web resi liberamente accessibili su Internet, l'analogia con la "violazione di domicilio", così spesso invocata durante l'esame del Congresso, non è configurabile e il requisito dell'autorizzazione è inadeguato.

Questa recentissima soluzione giurisprudenziale è, in ultima analisi, interessante poiché permette di notare l'impatto che i problemi creati da fenomeni digitali hanno sulle categorie tradizionali del diritto. Lo *US Computer Fraud and Abuse Act (CFAA)*, il quale sanziona comportamenti illeciti e non autorizzati sui sistemi informatici, è interpretato allo scopo di apprestare tutela a casi di violazioni contrattuali. Tale collegamento tra sanzioni penali e inadempimento contrattuale indirettamente “sfuma” la distinzione tra diritti contrattuali e diritti proprietari [89], apre nuovi scenari di tutela e merita ulteriori e approfondite analisi della *scholarship* in materia.

7. Conclusioni

Il consenso, principale istituto a protezione della libertà di autodeterminazione dell'utente-consumatore, presenta numerose criticità entro il corrente ecosistema digitale, identificato come web 2.0 click-wrap.

In pratica, alla tutela formale non pare corrispondere una tutela effettiva della stessa libertà, *in primis*, per gli ostacoli posti dalle architetture digitali manipolative qui esaminate.

Agli utenti viene, infatti, richiesto di esprimere il proprio consenso con modalità che paiono rispettare i requisiti previsti dal GDPR, assumendo che ciò basti a garantire la piena tutela. Si tratta, però, di una visione ottimistica che non corrisponde a ciò che accade realmente: dalla *compliance* con la norma non si può dedurre, infatti, che qualora gli utenti fossero informati circa l'iter specifico di processo e raccolta dei loro dati opterebbero per le medesime scelte.

Edwards nota che prima dell'entrata in vigore del GDPR, il requisito del consenso «*was a magic wand that could be waived by any popular online service to secure itself a revenue stream of personal data whilst remaining legally compliant*» [90], a ciò

aggiungendo che, anche dopo l'entrata in vigore dello stesso Regolamento, il grado di effettività non è migliorato.

In generale, si può osservare che l'impiego di dark patterns rende problematica la valutazione dei criteri essenziali sui quali poggiano i rimedi tradizionali. Si pensi, per esempio, ai rimedi basati sul giudizio di trasparenza o di correttezza: si tratta di principi fondanti la libertà di cui all'art. 8 della Carta dei diritti fondamentali il cui contenuto, tuttavia, in relazione al trattamento dei dati personali rimane elusivo quando oggetto di giudizio sono le architetture digitali manipolative sia per i consumatori medi che per quelli vulnerabili.

La tutela di un diritto fondamentale come quello della libertà di autodeterminazione non dipende, perciò, solo dal quadro giuridico esistente, e dal comportamento responsabile del soggetto cui i dati si riferiscono (il soggetto interessato), ma anche dalle caratteristiche di progettazione del servizio e dalla conformità sostanziale dello stesso con i princìpi di *data protection*. La corretta progettazione degli strumenti tecnologici dovrebbe, infatti, porre al centro l'uomo (*human centered*) e la tutela dei suoi diritti, garantendo il rispetto sostanziale di princìpi anche etici oltre che della normativa vigente.

Innovazioni significative su questo terreno potranno derivare dalla sinergia tra un'effettiva responsabilizzazione delle piattaforme e una maggiore consapevolezza, da parte degli utenti, del valore dei propri dati dato che tra gli utenti è diffusa la consapevolezza del fatto che l'utilizzo di queste tecnologie può mettere a serio rischio i dati personali, ma ad essa raramente segue un comportamento attivo per cercare di mantenere un controllo sul trattamento degli stessi.

Lo studio sperimentale condotto dallo *European Innovation Council and SMEs Executive Agency* (v. § 4) ha sottolineato che, nonostante la presenza di un solido quadro normativo dell'UE, tra cui la direttiva sulle pratiche sleali, considerata sufficientemente flessibile per coprire la maggior parte delle pratiche commerciali sleali, potrebbero essere necessari alcuni adeguamenti legislativi per far fronte ai problemi posti dai *dark patterns*. Oltre alle proposte rimediali basate sulla protezione dei dati, le quali si concentrano sulla panacea dei ricorsi semplificativi al consenso [91], occorre piuttosto riflettere sulle maggiori opportunità di tutela offerte dalla normativa consumeristica, anche alla luce dei recenti riconoscimenti avvenuti ad opera del *New Deal for Consumers* dell'Unione Europea, secondo cui i dati personali hanno un

inconfutabile valore economico [92].

In sintesi, il regime di protezione dei consumatori offre utili ausili per tutelare concretamente la persona del consumatore-utente: a differenza del giudizio in materia di protezione dei dati, in cui i diversi diritti e interessi in gioco sono posti sui piatti della bilancia, in un giudizio in materia consumeristica, viene valutato, *inter alia*, il diverso potere contrattuale delle parti, entro il quale gioca un ruolo importante l'asimmetria informativa. Analizzare l'architettura complessiva del sistema, l'esperienza dell'utente e le interfacce consentirebbe di valutare, attraverso gli istituti del diritto dei consumatori, se il processo di prestazione del consenso è avvenuto correttamente. Questo potrebbe tener meglio in considerazione anche il fatto che, come sottolineato da autorevole dottrina, essendo la contrattazione online materialmente diversa da quella offline, i consumatori-utenti godono di un potere contrattuale ancora minore rispetto alla contrattazione offline, e per questo – a parere della stessa dottrina – le regole destinate a disciplinare le situazioni online dovrebbero essere "aggiustate" per prevenire situazioni che comprino ulteriormente l'autonomia degli utenti [93].

Da una diversa prospettiva, poi, va osservato che, nel lungo periodo, queste situazioni di incerta o debole tutela per l'utente danneggiano l'azienda a causa della percezione che i clienti hanno della stessa, provocandone la perdita di credibilità, con inevitabili conseguenze anche sul piano economico.

In attesa delle evoluzioni della materia, si fanno strada in ogni caso le azioni che si possono porre in essere fin da ora: la prima, è di imparare a conoscere e riconoscere, il più possibile, tali pratiche. La seconda, fa appello alla responsabilità di chi opera online di controllare le pratiche suddette, anche se attuate tramite terzi. In molti casi la verifica è agevole, ad esempio se si utilizzano, per il proprio sito web, banner per l'accettazione dei cookies con box pre-flaggati di cookie non necessari, oppure se l'informativa privacy sia difficile da reperire sul sito web. Nei casi più dubbi e delicati sarebbe opportuno, invece, testare i modelli di architetture digitali per ottenere feedback dalle associazioni di rappresentanza dei consumatori, affinché indichino quali comportamenti consentano di agire correttamente (c.d. *fair patterns* o *transparent patterns*) [94].

Il presente contributo rientra nell'ambito delle attività dei gruppi di ricerca FILM 4.0 e ARrT del Progetto di Eccellenza del Dipartimento di Scienze Giuridiche Diritto, Cambiamenti e Tecnologie, *Università di Verona.*

Riferimenti bibliografici

[1] Organizzazione per la cooperazione e lo sviluppo economico (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, 12.02.2002, Paris, https://doi.org/10.1787/9789264196391-en.

[2] F.H. Cate, V. Mayer-Schonberger, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, Vol. 3, No. 2, 2013. Per un primo riferimento al concetto fondamentale "notice and choice" nell'ordinamento americano si rinvia a M. Froomkin, *Big Data: Destroyer of Informed Consent*, in 21 *Yale J. L & Tech* 27, 2019. Per approfondimenti si rinvia al § 6.

[3] Commissione europea, *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni sul piano d'azione per la democrazia europea*, Bruxelles, 3.12.2020, COM(2020) 790 final.

[4] Ci si avvale dei dati psicografici al fine di creare un modello predittivo utile a vari fini, come ad esempio le attività politiche.

[5] Per inciso è qui il caso di fare un rapido cenno all'esistenza di un particolare filone di studi che, recentemente, ha proposto e indagato una diversa prospettiva: il rapporto tra privacy e personalizzazione, o diritto personalizzato. Secondo questa lettura una conseguenza del forte interventismo del legislatore secondo la politica "Do not track" comporterebbe uno "sconveniente" incentivo verso l'utilizzo di regole di default impersonali in luogo di quelle personalizzate e «…from granular personalized default rules to crude personalized default rules, and (as we. Shall see) from personalized disclosure to impersonalized disclosure» Cfr. A. Porat, J.L. Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data* (Part I: The concept of personalized law), in C. Busch, A. De Franceschi, *Algorithmic Regulation and Personalized Law*, 2021, 45.

[6] Tra i tanti si veda M. Vayena, I. Effy, *Cambridge Analytica and Online Manipulation*, 2018, disponibile al sito:https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/.

[7] Harry Brignull è l'esperto di *User Experience Design* (o *UX design*) che ha coniato il termine, e che da oltre 10 anni documenta i dark patterns. Per la realizzazione dei *dark patterns* si utilizzano quindi studi di scienza cognitiva e di abitudini del comportamento umano allo scopo di portare benefici esclusivi all'azienda che rende il servizio, come ad

esempio un temporaneo incremento di fatturato o un aumento degli iscritti o, per quanto qui interessa, una raccolta di dati personali per i quali difficilmente l'utente avrebbe prestato un consenso consapevole.

[8] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, in *ACM SIGSAC Conference on Computer and Communications Security*, November 11-15, 2019, London, United Kingdom, ACM, New York, NY, USA, 18, disponibile al sito: https://doi.org/10.1145/3319535.3354212.

[9] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in *GUUE L*. 119/1 del 4 maggio 2016.

[10] L'introduzione del Trattato di Lisbona segna una svolta per il diritto fondamentale alla protezione dei dati. Con l'adozione del Trattato di Lisbona, la CDFUE ha acquisito forza vincolante e, come risultato, il diritto alla protezione dei dati è stato riconosciuto come diritto autonomo per la prima volta. Il GDPR come fonte derivata, è adottato sulla base dell'art. 16 TFUE che fornisce una base per l'Europa per adottare la legislazione per la protezione dei dati, ed i diritti e le libertà più in generale quando i dati sono elaborati. I dati personali sono “ogni informazione relativa ad una persona naturale identificata o identificabile (“data subject”)”.

[11] State of California Legislative Counsel, Assembly Bill No. 375, Chapter 55, 2018.

[12] La procedura è stata avviata dall'Office of the Australian Information Commissioner (OAIC). Per consultare l'*Australian Privacy Act* (1988) e tutti gli emendamenti si rinvia a: https://www.legislation.gov.au/Series/C2004A03712.

[13] European Data Protection Board, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them*, 14.03.2022.

[14] L'HCI è oggetto di studi dell'etica della tecnologia, il quale presenta importanti collegamenti con altri ambiti di studi affini quali gli *Science and Technology Studies* (STS), Privacy, Etica e diritto. Si rinvia a C.M. Gray, C. Santos, N. Bielova, M. Toth, D. Cliford, *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective*, in *CHI Conference on Human Factors in Computing Systems* (CHI '21), 2021, May 8–13, 2021, Yokohama, Japan. ACM, New York, USA, 18. Si rinvia a: https://doi.org/10.1145/3411764.3445779. Nell'affrontare i collegamenti transdisciplinari caratterizzanti il problema dell'utilizzo dei cookie banners per acquisire

il consenso gli autori esaminano l'interazione tra design della tecnologia, prospettiva giuridica ed etica. Gli stessi autori sottolineano, altresì, che in tempi più recenti gli utenti si sono dimostrati sempre più consapevoli del carattere etico implicito nel *design* e nell'impiego di molte applicazioni tecnologiche digitali. Tali questioni etiche relative alla tutela della privacy e dei valori e diritti fondamentali della persona sono già stati messi in primo piano dalle nuove normative, in particolare il Regolamento EU sulla Protezione dei Dati personali (GDPR), ed il *California Consumer Privacy* Act (CCPA) del 2018 degli Stati Uniti. Le regole e gli standards giuridici ivi contenuti definiscono i designs non conformi ai principi etici e giuridici

[15] Per una lettura sul modo in cui l'architettura può orientare il comportamento degli utenti si rinvia a K. Yeung, *"Hypernudge": Big Data as a mode of regulation by design*, in *Information, Communication & Society*, 20(1), 2017, 118-136. In pratica, alcuni commercianti utilizzano sempre più spesso pratiche commerciali basate sui dati per sviluppare sollecitazioni più efficaci per attirare l'attenzione dei consumatori e influenzarli, definite come una forma di "hypernudging": ciò comporta la compromissione della loro autonomia.

[16] Per un approfondimento sul significato di bias cognitivi, ossia quelle distorsioni automatiche in cui può incorrere ciascun consumatore, indipendentemente dal livello culturale, si rinvia a: A. Tversky, D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, in *Science*, vol. 185, n. 4157, 1974. Proprio i bias cognitivi sono utilizzati in correlazione con i *dark patterns*, per spingere gli utenti di un servizio verso scelte apparentemente logiche ed obiettive, ma, in realtà, fortemente condizionate. Un esempio, tra i più frequenti, di sfruttamento dei bias cognitivi si ha quando un prodotto o un servizio viene pubblicizzato a prezzo scontato, ma solo in quantità ridotta e/o per un periodo di tempo molto limitato. In tal modo si vuole "mettere fretta" al consumatore per spingerlo ad un acquisto non ponderato e probabilmente inutile.

[17] M. Leiser, W. Yang, *Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive*, in *Modern Law Review* (in corso di stampa, 2022).

[18] European Data Protection Board (EDPB), *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them Version 1.0*, adottate il 14 marzo 2022 https://edpb.europa.eu/var/www/httpd/giustiziacivile.com/giufral/sites/giustiziacivile.co

m/files/private/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[19] Non è ancora disponibile la versione in italiano delle Linee Guida, pertanto, in questo scritto si mantengono i termini inglesi.

[20] C. Utz, M. Degeling, S. Fahl, F. Schaub, T. Holz, *(Un)Informed Consent: Studying GDPR Consent Notices in the Field*, in *Proceedings*, ACM SIGSAC Conference on Computer and Communications Security (CCS '19), ACM, New York, USA, 2019, DOI: http://dx.doi.org/10.1145/3319535.3354212. In questo recente studio sono state analizzate circa 1.000 CMPs (*Consent management platforms*), di cui almeno il 57,4% hanno usato dark pattern per spingere gli utenti ad adottare opzioni meno privacy friendly. Il 95,8% di queste non prevede poi alcuna possibilità di scelta in merito al consenso sul trattamento dei propri dati personali, o prevede solo la possibilità di accettare il trattamento e non di "adeguarlo" alla reale volontà dell'utente. Nello studio citato si è inoltre dimostrato che il tasso di accettazione delle opzioni privacy sale dallo 0,16% all'83,55% nel caso in cui le stesse siano già preselezionate dal fornitore del servizio.

[21] In uno studio norvegese viene dimostrato come nelle impostazioni di default di alcuni siti internet, i dark pattern sono usati per "spingere" gli utenti verso opzioni maggiormente invadenti per la loro privacy. Lo studio è condotto dalla Forbrukerrädet, un'organizzazione che tutela gli interessi dei consumatori ed è stata fondata dal governo norvegese. Parte del suo lavoro consiste nel promuovere i diritti dei consumatori come il diritto alla privacy, il diritto a contratti sicuri e bilanciati nell'acquisto di prodotti o servizi digitali. Lo studio citato include tra gli elementi che manipolano gli utenti in modo da spingerli a cedere i propri dati con l'illusione del controllo, l'utilizzo di impostazioni di default, l'uso di parole fuorvianti e la scelta di "architetture" dei siti internet che richiedono all'utente uno sforzo maggiore per l'adozione di misure di protezione dei propri dati personali, scoraggiando così il compimento di tali azioni. Norway Forbrukerr?adet, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Forbrukerr?adet, Norway, 2018, disponibile su: https://fil.forbrukerradet.no/ wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[22] Si pensi anche al caso in cui l'interfaccia utilizza un "interruttore a levetta" per consentire agli utenti di dare o revocare il consenso e non si capisce in quale posizione

l'interruttore si trovi, perché la levetta non corrisponde al colore. Ad esempio: il lato destro è associato all'attivazione della funzione ("accensione") e il colore dell'interruttore è rosso, il che di solito significa che una funzione è invece disattivata. O, al contrario, quando l'interruttore si trova sul lato sinistro, a significare solitamente che la funzione è disattivata, il colore di sfondo dell'interruttore è verde, che è normalmente associato a un'opzione attiva. Questo rende le informazioni poco chiare, atte a confondere l'utente.

[23] Sull'applicazione della Direttiva sulle clausole commerciali scorrette ai *dark patterns* vedi le recenti raccomandazioni della European Consumer Organization, *"Dark Patterns" and The Eu Consumer Law Acquis. Recommendations for better enforcement and reform*, 2022, disponibile sul sito: https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf. Il documento afferma: «*The use of unfair practices to distort consumers' economic behavior is not new, but it takes a new important dimension as a result of the massive collection of data and the use of technology to build consumer profiles and anticipate consumer behavior. EU consumer law already has partial capacity to address these situations, but it is currently not sufficiently enforced. In addition, EU law must be updated to tackle these unfair practices and ensure consumers are not harmed by misleading user interfaces and data personalization techniques*» (spec. 1).

[24] Cfr. D. Susser, B. Roessler, H. Nissenbaum, *Technology, autonomy, and manipulation*, in *Internet Policy Review*, *8*(2), 2019, disponibile su: https://doi.org/10.14763/2019.2.1410. L'esperimento ha rivelato che la maggior parte dei partecipanti ha acconsentito a tutte le richieste di consenso, indipendentemente dai nudges del dark design. Inaspettatamente, nonostante i livelli generalmente bassi di controllo percepito, l'ostruzione dell'opzione favorevole alla privacy ha portato a una maggiore e non minore percezione del controllo. Nel secondo esperimento (N = 255) abbiamo invertito la direzione delle spinte progettuali verso l'opzione favorevole alla privacy, che abbiamo intitolato "bright patterns". Questa volta i nudge di ostruzione e di default hanno spinto efficacemente le persone verso l'opzione che favorisce la privacy, mentre il risultato relativo al controllo percepito è rimasto invariato rispetto all'Esperimento 1. Nel complesso, i nostri risultati suggeriscono che molte delle attuali implementazioni delle richieste di consenso per i cookie non consentono scelte significative agli utenti di Internet e non sono quindi in linea con le intenzioni dei

responsabili politici dell'UE. Esploriamo anche il modo in cui i responsabili politici potrebbero affrontare il problema. Nel nostro studio, l'interferenza dell'interfaccia è stata testata in base alle dimensioni e al colore del banner dei cookie, quindi "design equivalente" nel nostro contesto significa stesse dimensioni e stesso colore. A tal fine, era sufficiente che i colori potessero essere assegnati allo stesso gruppo di colori. Osservando i diversi raggruppamenti di pulsanti, abbiamo osservato che nella maggior parte dei siti web i pulsanti variavano effettivamente in termini di dimensioni e colori. Per quanto riguarda la combinazione "Accetta tutto" e "Rifiuta tutto", solo 21 banner cookie su 330 che utilizzano questa composizione sono stati progettati in modo uguale. Il divario è ancora maggiore tra "Accetta tutto" e "Impostazioni". Su 1091 banner di cookie che utilizzavano questa composizione, solo 11 avevano un design del pulsante equivalente, mentre 1080 non lo avevano. Risultati simili valgono anche per il raggruppamento "Accetta tutto" e "Accetta parzialmente". In particolare, le opzioni di accettazione e di rifiuto del consenso non erano ugualmente visibili. Nella maggior parte dei casi, il pulsante "Accetta tutto" era evidenziato in verde o blu, mentre il pulsante "Rifiuta tutto" era per lo più bianco. Inoltre, i "pulsanti di rifiuto" bianchi spesso corrispondevano al colore di sfondo dei banner. Al contrario, l'opzione di accettazione del consenso è stata tipicamente mantenuta in un colore contrastante. Lo stesso vale per gli sfondi neri. In conclusione, l'utente è psicologicamente tentato di cliccare sul pulsante "Accetta tutto" perché sembra essere l'opzione più dominante e conveniente. Dato che queste opzioni sono di solito le più ostili alla privacy, sembra ragionevole – almeno dal punto di vista dei gestori dei siti web – dare loro regolarmente una preferenza visiva.

[25] S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Profile Books Ltd, 2019.

[26] Oltre a Zuboff si veda, in generale, la letteratura in materia di *market surveillance regulation*. Tra i tanti si rinvia al recente contributo di C. Busch, *Rethinking Product Liability Rules for Online Marketplaces: A Comparative Perspective (Consumer Law Scholars Conference in Boston (March 4-5, 2021)*, 2021, disponibile su: SSRN: https://ssrn.com/abstract=3784466 or http://dx.doi.org/10.2139/ssrn.3784466.

[27] Cfr. K. Yeung, *"Hypernudge": Big Data as a mode of regulation by design*, in *Information Communication and Society*, 20(1), 2006, 1-19.

[28] G.U. L 281 del 23/11/1995 p. 0031 – 0050. La Direttiva 95/46/CE del Parlamento e

del Consiglio d'Europa era stata adottata il 24 ottobre 1995, con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali per garantire un "flusso libero" dei dati (*free flow of data)* e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini. L'esigenza di armonizzazione nasceva dalla frammentazione in materia tra i diversi paesi aderenti all'Unione, per cui si è reso necessario procedere ad un ravvicinamento delle normative nazionali che però non determinasse un indebolimento della tutela delle persone. La direttiva 95/46/CE ha avuto un ruolo strumentale rispetto all'esigenza di abbattere le frontiere all'interno dell'Unione europea, consentendo di rimuovere i limiti ai trasferimenti immateriali (appunto, *free flow of data*). La direttiva, però, essendo strumentale al funzionamento del mercato interno, aveva come riferimento la regolazione degli scambi commerciali, e concepiva la protezione dei dati all'interno di una relazione statica tra il titolare e l'interessato, in una visione proprietaria del dato stesso. In tal senso se ne favoriva un'applicazione formalistica (tramite le informative e il consenso). Il dato è dell'interessato e quindi non può essere usato senza consenso, snodo fondamentale per l'utilizzo ampio del dato stesso. La direttiva del 1995 presentava evidenti carenze, dovute all'evoluzione della tecnologia, e dei trattamenti automatizzati, successivi alla sua approvazione. Quindi, sia per aggiornare la normativa in materia, renderla più capace di adattarsi alle tecnologie emergenti, ma anche perché col Trattato di Lisbona il diritto alla protezione dei dati personali diventa un diritto fondamentale dei cittadini, quindi da garantire allo stesso modo in tutto il territorio dell'Unione, si reso necessario sostituirla con il Regolamento europeo (GDPR).

[29] Per una prima lettura generale sul tema della disciplina del consenso ai sensi del Regolamento UE sulla protezione dei dati si veda si rinvia, tra i tanti a: M. Schmidt-Kessel, *Consent for Processing of Personal Data and its Relationship to Contract*, in A. Franceschi, R. Schulze, M. Graziadei, P. Oreste, F. Riente, S. Sica, P. Sirena (eds), *Digital Revolution – New Challenges for Law*, Oxford, 2020, 75-83; S. Thobani, *Processing Personal Data and the Role of Consent*, in *Eur. L. Privacy L. & Tech.* 93, 2020; Basunti Carlo, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, 2020, fasc. 2, 860-895; F. Ferretti, *A European Perspective on Data Precessing Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously*, in *European Review of Private Law*, vol. 2,

2012, 473-506; M. Betkier, *What is Data Privacy and what is the Role of Consent?*, in *Privacy Online, Law and the effective Regulation of Online Services*, Intersentia, 9-40; F. Ruggeri, *Sulla nozione di consenso nella nuova disciplina privacy: alcune prime considerazioni* (nota a Cass. sez. I civ. 2 luglio 2018, n. 17278), in questa *rivista*, 2019, fasc. 3, 10.

[30] Nel 2019, l'Autorità garante della protezione dei dati francese, la *Commission nationale de l'informatique et des libertés* ha pubblicato il report "*Shaping Choices in the Digital World*" (disponibile sul sito: https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf) il quale stabilisce che l'uso e l'abuso di una strategia che distoglie l'attenzione dell'utente può portare ad un consenso invalido. Altri organi europei quali design digitali possono offuscare le scelte relative alla privacy degli utenti o quali potrebbero intromettersi con la tutela della privacy, violando l'art. 25 del GDPR che richiede la protezione dei dati by design e by default.

[31] Il Working Party (WP29) è un organismo consultivo in materia di protezione di dati e privacy indipendente europeo, stabilito in base all'art. 29 della direttiva 95/46/EC. Il WP29 ha publicato le *Guidelines on consent under Regulation* 2016/679, le quali sono state adottate il 28 novembre 2017 (e riviste da ultimo il 10 aprile 2018, 17/EN, WP259 rev.01). il Gruppo di lavoro sottolinea che, sebbene il consenso sia fondamentale per far valere i diritti degli interessati garantiti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (CFEU), l'ottenimento del consenso non "annullerà o diminuirà in alcun modo gli obblighi del responsabile del trattamento ... per quanto riguarda l'equità, la necessità e la proporzionalità, nonché la qualità dei dati". I responsabili del trattamento non devono considerare il consenso, anche se ottenuto in piena conformità al GDPR, come un "lasciapassare" quando si considerano gli altri obblighi imposti dal regolamento. Come regola generale, il consenso è una base legittima per il trattamento solo "se all'interessato viene offerto il controllo e ... una scelta effettiva per quanto riguarda l'accettazione o il rifiuto delle condizioni offerte o il rifiuto senza pregiudizio". Il Gruppo di lavoro avverte inoltre i responsabili del trattamento che il concetto di consenso ai sensi del GDPR rimane legato al consenso ai sensi della bozza di regolamento ePrivacy, e che la maggior parte dei responsabili del trattamento "probabilmente avrà bisogno del consenso ai sensi dello strumento ePrivacy per la maggior parte dei messaggi di marketing online o delle chiamate di marketing, e

dei metodi di tracciamento online, compreso l'uso di cookie o di app o di altri software". Il consenso specifico è concepito per "garantire un certo grado di controllo da parte dell'utente e di trasparenza per l'interessato". La specificità è strettamente legata al requisito del consenso informato. Il Gruppo di lavoro individua tre componenti della specificità che i responsabili del trattamento devono applicare: (*i*) la specificazione delle finalità come salvaguardia contro l'estensione delle funzioni; (*ii*) "granularità" nelle richieste di consenso; (*iii*) chiara separazione delle informazioni relative all'ottenimento del consenso per le attività di trattamento dei dati da quelle relative ad altre questioni. I responsabili del trattamento che desiderano utilizzare i dati raccolti per nuove finalità sono avvertiti che prima di farlo devono ottenere un nuovo consenso dagli interessati. Le diverse finalità di trattamento richiedono diversi opt-in nella fase del consenso. Ogni consenso deve essere accompagnato da informazioni specifiche per quella richiesta "al fine di rendere gli interessati consapevoli dell'impatto delle diverse scelte che hanno a disposizione".

[32] EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 4 maggio 2020, disponibili sul sito: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf. Le Linee Guida 5/2020 dello European Board sul consenso sono solo un aggiornamento di quelle già adottate e successivamente emendate dal Gruppo articolo 29 – Sotto la lente del Board sono finite, in particolare, le pratiche dei 'cookie walls' e dello 'scrolling'.

[33] Cfr. Corte giust. UE, 1 ottobre 2019, C-673/17, *Verbraucherzentrale Bundesverband e v. Planet 49 GmbH*, para. 62-63.

[34] In materia di revoca si rinvia a G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, 299 ss.

[35] Ulteriori principi vengono in esame in tale valutazione, come la minimizzazione dei dati e l'accountability di cui all'art. 5 (1) (a), (c) e 2 GDPR, così come in alcuni casi la limitazione degli obiettivi di cui all'art. 5 (1) (b) GDPR.

[36] Gli aspetti qui elencati sono stati oggetto di chiarimenti più specifici da parte del Gruppo dell'Articolo 29 per la tutela dei dati (Article 29 Working Party o WP29) nelle Linee Guida sulla Trasparenza, adottate il 29 novembre 2017. A pagina 8 del documento si legge: «Positioning or colour schemes that make a text or link less

noticeable, or hard to find on a webpage, are not considered easily accessible». Secondo il WP29 il requisito del linguaggio «in forma concisa, trasparente, intellegibile e facilmente accessibile» è rispettato se i titolari presentano le informazioni e le comunicazioni in modo efficiente e succinto, con informative relative alla privacy chiaramente differenziate rispetto alle altre informative di tipo commerciale. Le informative dovrebbero poi essere "intellegibili", ossia facilmente comprensibili dall'utente medio, e, quindi, utilizzare un linguaggio chiaro e semplice ed evitare frasi e strutture linguistiche complesse o astratte o rese con termini ambivalenti. Il soggetto interessato dovrebbe, infine, essere in grado di determinare in anticipo la portata e le conseguenze del trattamento dei dati e non essere "colto di sorpresa". Le informazioni devono poi essere "facilmente accessibili" e all'interessato non dovrebbe essere richiesto uno sforzo eccessivo per ricercarle. L'accesso, soprattutto online, alla sezione privacy dovrebbe essere immediatamente attuabile e non prevedere lo scorrimento di una grande quantità di testi o di pagine. Dovrebbe quindi essere immediatamente evidente agli interessati dove e come queste informazioni possono essere recuperate.

[37] 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 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. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento…».

[38] I sette princìpi su cui si basa la *privacy by design*, elaborati da Ann Cavoukian, Privacy Commissioner dell'Ontario (Canada), sono: 1) prevenire e non correggere: i problemi vanno cioè valutati nella fase di progettazione al fine di prevenire il verificarsi dei rischi legati alla privacy; 2) privacy come impostazione di default: il che significa offrire il massimo grado di privacy automaticamente, quindi, anche in assenza di un'azione da parte dell'individuo interessato; 3) incorporazione della privacy nel progetto: la progettazione e l'architettura dei progetti IT e delle pratiche aziendali devono comprendere anche la privacy quale elemento essenziale e come parte integrante del sistema; 4) garanzia di massima funzionalità; 5) garanzia di sicurezza durante tutto il ciclo del prodotto o del servizio offerto;

6) visibilità e trasparenza del trattamento in tutte le fasi operative in modo che sia sempre verificabile la tutela dei dati; 7) centralità dell'utente, il che significa rispetto dei diritti ad esso riconosciuti e garanzia di tempestive e chiare risposte alle sue richieste di accesso (Cfr: Association of Privacy Professionals: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/).

[39] Garante per la protezione dei dati personali, *Linee guida cookie e altri strumenti di tracciamento*, del 10 giugno 2021, in *GU* n. 163 del 9 luglio 2021.

[40] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) modificata dalla direttiva 2006/24/CE e dalla direttiva 2009/136/CE.

[41] In sintesi, il Garante Privacy ha esplicitamente affermato che i cookie e gli altri strumenti di tracciamento non possono essere installati senza aver raccolto il consenso degli utenti (eccetto condizioni eccezionali, ad esempio se i cookie hanno esclusivamente lo scopo di fornire un servizio richiesto dall'utente). Di conseguenza, le nuove linee guida sui cookie chiariscono che non è più consentito ricorrere al legittimo interesse per la profilazione degli utenti.

[42] Cfr. Commissione europea, Comunicazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale Europeo, *Un "New Deal" per i consumatori*, Bruxelles, 11.4.2018 COM(2018) 183 final. Vedi, inoltre tutti i relativi documenti aggiornati presenti sul sito: https://ec.europa.eu/info/law/law-topic/consumer-protection-law/review-eu-consumer-law_it. Per una lettura sul rapporto fra consenso al trattamento e contratto si rinvia tra i tanti: E. Kaiser, *The concept of "Freetly Given, Specific and Informed Consent" under the Scrutinity of the European Court of Justice (case Notes – comment to Case C-61/19 Orange Romania SA c. Autoritates Nationale ANSPDCP*, decisione dell'11 novembre 2020), in 6 *Eur. Data Prot. L. Rev*. 607, 2020; L. Valle, *Cookie e Tutela dei Dati Personali tra Protezione dei Diritti della Persona e tutela del consumatore*, in *Eur. J. Privacy L & Tech* 16, 2020; C. Angiolini, *A proposito del Caso "Orange Romania" deciso dalla Corte di Giustizia dell'UE: il rapporto fra contratto e consenso al trattamento dei dati personali (Nota a sentenza Corte di Giustizia dell'Unione europea sezione II 11 novembre 2020 (causa C-61/19)*, in *Le nuove leggi civili commentate*, fasc. 1, 2021, 247-265.

[43] Cfr. G. Dworkin, *The theory and practice of autonomy*, Cambridge University

Press, 1988.

[44] Così nota M.R. Leiser, *'Dark Patterns': The Case for Regulatory Pluralism* (June 12, 2020), disponibile sul sito: https://ssrn.com/abstract=3625637; o http://dx.doi.org/10.2139/ssrn.3625637.

[45] Così l'Autorità garante della concorrenza e del mercato nel caso *Cv154 - Whatsapp-Clausole Vessatorie,* provvedimento n. 26596 Testo del provvedimento: https://www.agcm.it/dotcmsDOC/allegati-news/CV154_vessestratto_omi.pdf

[46] Cfr. Chamber Court judgement, *VZBV vs WhatsApp*, 20 dicembre 2019, AZ 5 U 9/18, Urteil des KG Berlin vom 08.04.2016, Az. 5 U 156/14.

[47] Cfr. Council and SMEs Executive Agency (EISMEA), *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization,* Luxembourg: Publications Office of the European Union, 2022.

[48] Il BEUC è un'organizzazione europea che raggruppa varie associazioni di tutela dei consumatori e dunque che rappresenta una platea considerevole di stakeholder. Il Bureau monitora costantemente le evoluzioni normative e giurisprudenziali.

[49] Bureau Européen des Unions de Consommateurs (ASBL), *"Dark Patterns" and the EU Consumer Law Aquis. Recommendations for better enforcement and reform*, 2022, disponibile al sito: https://www.beuc.eu/publications/dark-patterns-and-eu-consumer-law-acquis/html. In un interessante e articolato studio intitolato *EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets* e curato dal BEUC (Bureau Européen des Unions De Consommateurs) si considera la vulnerabilità digitale degli utenti, la gestione dei consensi, le asimmetrie informative e lo sfruttamento dei dati nelle pratiche commerciali (in particolare nella personalizzazione dei prezzi online): tra queste ultime, è analizzato anche il fenomeno qui in esame, che alimenta la visione della persona come "commodity", come prodotto. Nel documento, in particolare, si offre un'attenta e profonda analisi delle prassi penalizzanti dei consumatori/interessati, oltre che delle normative che attualmente possono essere impiegate a loro tutela.

[50] Direttiva 2005/29/Ce del Parlamento Europeo e del Consiglio dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali»).

[51] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio *GU L 304* del 22.11.2011, 64–88.

[52] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, in *GU L* 304 del 22.11.2011, 64–88.

[53] Direttiva (Ue) 2019/2161 del Parlamento Europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, in *GUUE L* 328/7 del 18 dicembre 2019.

[54] Tra le tante vedi: Corte giust. UE, 16 luglio 1998, C-210/96, *Gut Springenheide*, 1998, ERC I-04657, in ECLI:EU:C:1998:369.

[55] Corsivo aggiunto.

[56] L'art. 7 (2) del GDPR recita: «Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante».

[57] L'art. 12 (1) del GDPR recita: «Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato».

[58] L'art. 5 (2) della Direttiva 2005/29/CE del Parlamento europeo e del Consiglio

dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») recita: «Una pratica commerciale è sleale se: a) è contraria alle norme di diligenza professionale; e b) falsa o è idonea a falsare in misura rilevante il comportamento economico, in relazione al prodotto, del consumatore medio che raggiunge o al quale è diretta o del membro medio di un gruppo qualora la pratica commerciale sia diretta a un determinato gruppo di consumatori».

[59] Il quadro interpretativo offerto dalle Corti è ben ricostruito nella Relazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale Europeo, Prima relazione sull'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio ("direttiva sulle pratiche commerciali sleali"), Bruxelles, 14 marzo 2013, COM(2013) 139 final.

[60] Commissione europea, *Proposta di Regolamento del Parlamento Europeo e del consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*, Bruxelles, 15.12.2020 COM(2020) 825 final 2020/0361 (COD).

[61] Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Emendamenti del Parlamento europeo, approvati il 20 gennaio 2022, alla proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD). Il DSA procederà ora alla negoziazione con gli Stati membri dell'UE e, se trasformato in legge, avrà un profondo impatto sulla fornitura dei servizi digitali nell'Unione europea.

[62] La pubblicità comportamentale online è la presentazione di annunci pubblicitari a

un utente di Internet i quali vengono adattati agli interessi dell'utente in base a un "profilo" dell'utente che è stato costruito nel tempo attraverso il monitoraggio della sua attività online. Questo "profilo" degli interessi dell'utente e della sua attività online può essere compilato da una varietà di fonti, come i social media (ai quali gli utenti spesso rivelano pubblicamente la loro età, la data di nascita, l'ubicazione, gli hobby e gli interessi), i motori di ricerca (che tracciano la cronologia delle ricerche su Internet degli utenti) e i servizi di messaggistica (attraverso i quali gli utenti si scambiano informazioni, anche su hobby, interessi, famiglia, amici e prodotti). Un'altra fonte comune attraverso la quale si ottengono informazioni comportamentali online è rappresentata dai "cookie"; prevalentemente "cookie di terze parti".

[63] L.N. Jayakumar, *Cookies "n" Consent: an Empirical Study on the Factors Influencing Website Users' Attitudes towards Cookie Consent in the EU,* in *DBS Business Review*, vol. 4, 2021.

[64] Durante il processo di iscrizione ai social media, agli utenti vengono fornite molte informazioni e diverse impostazioni relative alla protezione dei dati. Per assicurarsi che gli utenti possano trovare le impostazioni e modificarle in qualsiasi momento durante l'utilizzo della piattaforma, le impostazioni devono essere facilmente accessibili e associate a informazioni pertinenti che consentano agli utenti di prendere una decisione informata. L'elemento "facilmente accessibile" significa che gli interessati non devono cercare le informazioni. Per quanto riguarda le politiche sulla privacy, il Gruppo di lavoro Articolo 29 ha già affermato che un posizionamento o uno schema di colori che rende un testo o un link meno evidente o difficile da trovare su una pagina web non sono considerati facilmente accessibili. Per una visione di più ampio respiro sul tema si veda lo Studio richiesto dalla Juri Commitee (European Parliament's Committee on Legal Affairs) redatto da G. Sartor, F. Lagioia, F. Galli, *Regulating targeted and behavioural advertising in digital services: How to ensure users' informed consent*, 2021.

[65] Una questione sempre controversa è la validità dei cosiddetti 'cookie walls', in base ai quali il consenso è un prerequisito per accedere a un sito web.

[66] Per una recente lettura in materia cfr. P. Vogiatzoglou, P. Valcke, *Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law*, in R. Leenes, E. Kosta, I. Kamara (eds), *Research Handbook on EU Data Protection Law*, Elgar, 2022, 11-50.

[67] Per una sintesi dei momenti cruciali di tale iter giurisprudenziale nell'ambito italiano ci si permette di rinviare a G. Guerra, *Lo «spazio risarcitorio» per violazione del solo diritto all'autodeterminazione del paziente. Note a margine di un percorso giurisprudenziale*, in *Nuova giur. civ. comm.*, parte II, fasc. 12, 2010, 617-632.

[68] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679 (WP259 rev.01)*, 2018. Si veda anche Commission nationale de l'informatique et des libertés (CNIL), *Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)*, 2019; e Information Commissioner's Office, *Guidance on the Use of Cookies and Similar Technologies*, Cheshire, 2019.

[69] Tra i tanti si rinvia a O. Pollicino, M. Bassini, *Commento all'art. 8 CdfUE*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, 2017, 132.

[70] *Ex* art. 23 d.lgs. n. 196/03 (articolo successivamente abrogato dal d.lgs. n. 101/2018), già richiedeva un consenso libero che, in base anche alle indicazioni fornite dal Garante per la protezione dei dati personali, si declinava nell'assenza di condizionamenti da parte del titolare del trattamento.

[71] La prima Sezione civile della Suprema Corte, con la sentenza n. 17278 del 2 luglio 2018, è intervenuta in una vicenda che vedeva una società offrire un servizio di newsletter su argomenti attinenti alla finanza, al fisco, al diritto e al lavoro, a condizione che l'utente acconsentisse al trattamento dei dati per l'invio alla propria casella di posta di comunicazioni promozionali e informazioni commerciali indesiderate, anche da parte di terzi. La sentenza è un importante intervento in tema di natura e caratteristiche del consenso ex art. 23 del Codice Privacy e art. 4(11) GDPR, poiché nell'accogliere il ricorso del Garante ha sottolineato che: «la nozione di consenso valida all'interno del contesto del trattamento di dati personali non può essere accostata a quella del consenso genericamente necessario a fini negoziali; si tratta invece di un consenso "rafforzato", analogo al consenso "informato" necessario a fini sanitari, e "dettato dall'esigenza di rimediare alla intrinseca situazione di debolezza dell'interessato, sia sotto il profilo della evidente «asimmetria informativa», sia dal versante della tutela contro possibili tecniche commerciali aggressive o suggestive"; il ruolo ricoperto dal consenso nel campo dei dati personali è dunque "tale da non ammettere compressioni di alcun genere e non

sopporta di essere sia pure marginalmente perturbato non solo per effetto di errore, violenza o dolo, ma anche per effetto dell'intero ventaglio di possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare"; con riferimento al requisito della libertà del consenso, la Corte ricorda che l'art. 7(4) del GDPR richiede di tenere "nella massima considerazione l'eventualità […] che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto"; tuttavia, secondo la Cassazione, il fatto che l'offerta di un determinato servizio da parte del gestore di un sito sia condizionata al consenso all'utilizzo dei dati personali per l'invio di messaggi pubblicitari da parte di terzi non comporta sempre una tale compressione della libertà dell'interessato da rendere il consenso, per ciò solo, non libero; infatti, vi sarà tanto più un condizionamento tale da rendere il consenso non conforme all'art. 23 "quanto più la prestazione offerta […] sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso». Per un commento alla sentenza si rinvia a: S. El Sabi Sabrina, *La Corte di Giustizia vieta le caselle di spunta preselezionate per il consenso all'uso dei "cookie" (nota a sentenza Corte di Giustizia dell'Unione europea grande sezione 1 ottobre 2019 (causa C-673/2017)*, in *giustiziacivile.com*, 2020, fasc. 2, 9; I. Gabriele, *Dai "Dark Patterns" al "Legal Design": problemi e soluzioni all'utilizzo degli elementi grafici per alterare la volontà degli utenti*, in *Ciberspazio e Diritto*, 2020, fasc. 1, 185-204; L. Falciai, *Il consenso dell'interessato come condizione per l'offerta di un servizio: la sentenza della Corte di Cassazione 17278/2018* (nota a Cass. sez. I civ. 2 luglio 2018, n. 17278), in *Ciberspazio e Diritto*, 2018, fasc. 3, 421-430; F. Zanovello, Consenso libero e specifico alle e-mail promozionali (nota a Cass. sez. I civ. 2 luglio 2018, n. 17278), in *La Nuova giurisprudenza civile commentata*, 2018, fasc. 12, 1778-1785.

[72] Corte giust. (Grande Sezione), 1° ottobre 2019, causa C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:246.

[73] Tra le tante si rinvia a Cass. Civ., 2 luglio-11 novembre 2019, n. 28985, in *Responsabilità civile e previdenza*, 2020, fasc. 4, 1364-1384, con nota di P. Frati, A. Campolongo, R. La Russa, M. Scopetti, *Violazione del consenso informato:*

codifichiamo nozioni, significati e risarcibilità dei danni alla luce della pronuncia n. 28985/2019 della Suprema Corte di Cassazione. Il consolidato orientamento secondo cui l'omessa informativa al paziente assume diversa rilevanza causale, a seconda che sia dedotta la violazione del diritto all'autodeterminazione oppure la lesione del diritto alla salute. In ogni caso tra le condizioni per ottenere il risarcimento dei danni causati dalla mancanza del consenso all'intervento, nel caso di condotta non colposa del medico, il paziente deve dimostrare che, ove compiutamente informato, egli avrebbe verosimilmente rifiutato l'intervento, ovvero avrebbe ottenuto la necessaria preparazione per affrontare il periodo post-operatorio (accettandone le eventuali conseguenze e sofferenze). Così recentemente chiarito dall'ordinanza della Cass., sez. III, n. 11112/2020.

[74] Si rinvia all'UK Information Commissioner's Office: https://ico.org.uk/.

[75] Per un esame del significa di "consent-fatigue" si rinvia a European Consumer Organization (BEUC), *Report on EU CONSUMER PROTECTION 2.0 Structural asymmetries in digital consumer markets*, scritto da N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, M. Sax, J. Strycharz, Brussels, 2021.

[76] Tar Lazio, sez. I, 10 gennaio 2020, n. 260 è pubblicata in *Diritto & Giustizia*, 2020 (13 gennaio), per un commento si rinvia a: A.L. Tarasco, M. Giaccaglia, *Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo*, in *Il diritto dell'economia*, 66, n. 102, 2020, 263-301. Mentre, invece, Tar Lazio 10 gennaio 2020, n. 261 in *Dir. Industriale*, 2021, 6, 511, con nota di G.L. Pastuglia, *Prime note in materia di coordinamento tra disciplina delle pratiche commerciali scorrette e regole privacy*.

[77] Diversamente, la seconda sanzione dell'Antitrust è stata annullata dal T.A.R. Lazio. Questa riguardava l'"indebito condizionamento" degli utenti i cui dati vengono trasmessi a terze parti senza il loro consenso. Il T.A.R. ha infatti ritenuto che agli utenti è data la possibilità di scegliere se consentire o meno l'integrazione tra diverse piattaforme. Su questo secondo aspetto restano tuttavia molte perplessità.

[78] Cfr. Cass. civ., Sez. I, 24 marzo 2021-25 marzo 2021, n. 14381, in *Danno e Resp.*, 2022, 2, 141 ss., con nota di G. Comandé, *Leggibilità algoritmica e consenso al trattamento dei dati personali, Note a margine di recenti provvedimenti sui dati personali*. In base alla decisione il consenso richiesto, secondo il Garante, non è informato nel caso di specie perché non sono indicate le logiche usate dall'algoritmo

mentre il sistema è suscettibile di incidere pesantemente sulla rappresentazione economica e sociale di un'ampia categoria di soggetti con ripercussioni di *rating* sulla vita privata dei soggetti elencati.

[79] Per un approfondimento si rinvia a K. E. Davis, F. Marotta-Wurgler, *Contracting for Personal Data*, in *NYU L. Rev.*, vol. 94(4), n. 19-37, 2019.

[80] Codificato dal 18 U.S. Code § 1030 (Fraud and related activity in connection with computers).

[81] United States District Court, N.D. California, San Jose Division, *Facebook v. Power.com*, C 08-5780 JF (RS), Oct. 22, 2009.

[82] Cfr. *California Privacy Rights and Enforcement Act* of 2020, Version 3, No. 19-0021, disponibile sul sito: https://www.oag.ca.gov/var/www/httpd/giustiziacivile.com/giufral/sites/giustiziacivile.com/files/private/initiatives/pdfs/19-0021A1 %28Consumer Privacy - Version 3%29_1.pdf.

[83] Il 12 ottobre 2020, il procuratore generale della California ha annunciato una nuova serie di modifiche al CCPA. La proposta di regolamento include una nuova disposizione (sezione 999.315(h) che limita il numero di passaggi necessari a un consumatore per rinunciare alla vendita di informazioni personali. Inoltre, le modifiche vietano alle aziende di utilizzare un linguaggio confuso quando il consumatore vuole rinunciare all'offerta (999.315(h)(2). I regolamenti impediscono, inoltre, all'azienda di far leggere al consumatore un elenco di motivi per non rinunciare alla vendita (999.315(h)(3). Oltre ai regolamenti proposti, l'iniziativa elettorale del California Privacy Rights Act, recentemente approvata, affronta specificamente l'uso di "dark pattern". Il CPRA definisce il termine come “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice”. Section 1798.140(h) del CPRA dichiara che il consenso ottenuto attraverso l'uso dei dark pattern non può essere considerate valido, mentre la section 1798.185(a)(20) indica che l'avvocato generale della California deve assicurcarsi che il link utilizzato dai providers per consentire l'opzione di “opt-out” all'utente non impieghi strategia di dark patterns.

[84] La nuova definizione di consenso del CPRA, che. Include il riferimento ai dark patterns stabilisce che: «agreement obtained through use of dark patterns does not constitute consent.” The law defines “dark patterns” as «a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy,

decisionmaking, or choice, as further defined by regulation» (Cal. Civ. Code § 1798.140(h).

[85] United States Court of Appeals for the Ninth Circuit, *Hiq Labs, Inc. v LinkedInd Corporation*, San Francisco, California, 18 April 2022, No. 17-16783, D.C.

[86] *HiQ Labs, Inc. v. LinkedIn Corp*, 938 F.3d 985 (9th Cir. 2019).

[87] Supreme Court of the United States, *Van Buren v. United States*, 593 U.S., June 3, 2021.

[88] I giudici del nono circuito nella sentenza *LinkedId v. Hiq Labs, Inc*, riprendono il precedente Van Buren, spiegando: «l'indagine "*gates-up-or-down*" di Van Buren è coerente con la nostra interpretazione del CFAA che contempla tre categorie di sistemi informatici [...]. La distinzione di Van Buren tra utenti di computer che "possono o non possono accedere a un sistema informatico" suggerisce una distinzione di base in cui esistono "limitazioni all'accesso" che impediscono ad alcuni utenti di accedere al sistema (cioè, esiste un "cancello", che può essere alzato o abbassato). L'indagine della Corte sui "cancelli aperti o chiusi" si applica quindi alle ultime due categorie di computer che abbiamo identificato: se l'autorizzazione è richiesta ed è stata data, i cancelli sono aperti; se l'autorizzazione è richiesta e non è stata data, i cancelli sono chiusi. Come abbiamo notato, tuttavia, una caratteristica distintiva dei siti Web pubblici è che le loro sezioni disponibili al pubblico non hanno limitazioni di accesso; al contrario, tali sezioni sono aperte a chiunque abbia un browser Web. In altre parole, applicando l'analogia dei "cancelli" a un computer che ospita pagine web pubblicamente disponibili, tale computer non ha eretto alcun cancello da alzare o abbassare. Van Buren rafforza quindi la nostra conclusione che il concetto di "senza autorizzazione" non si applica ai siti web pubblici» (traduzione mia).

[89] La possibilità che il CFAA possa essere usato per “punire” un inadempimento contrattuale – come si deduce dalla Parte III dell'opinione di maggioranza in *Van Buren v. United States*, 141 S. Ct. 1648 – è motivo per interpretare la disposizione in modo restrittivo. Al contrario, l'opinione dissenziente in Van Buren sostiene (verso la fine della Parte I) che l'uso non autorizzato di un sistema informatico è analogo a una violazione dei diritti di proprietà e quindi l'estensione della punibilità risulterebbe appropriata. Il dibattito sulla natura del dato personale e sulla relativa tipologia di rimedi applicabili nel caso di violazione è viva anche alle nostre latitudini: cfr. C. Langhanke, M. Schmidt-Kessel, *Consumer Data as Consideration*, in *4 Journal of*

European Consumer and Market Law, 2015, 218 ss., i quali propongono di risolvere il problema del valore di scambio delle prestazioni sul piano del *contract law* e non già del *data protection law*; G. Alpa, *La "proprietà" dei dati personali*, in N. Zorzi, F. Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, 17, secondo il quale il dato personale è una parte della persona, una sua proiezione (in linea con quest'ultima posizione si veda precedentemente: S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, 30, il quale ipotizza una sovrapposizione tra noi ed i nostri dati). In materia si rinvia anche a G. Resta, *Identità personale e identità digitale*, in *Dir. inform.*, 2007, 3, 511 ss., in part. 514-515; e G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi di rete*, in *Riv. trim. dir. proc. civ.*, 2018, 2, 416.

[90] Cfr. L. Edwards, *Law, Policy and the internet*, Oxford, 2019.

[91] Per un esempio di consenso semplificato, vedi B. Custers, F. Dechesne, W. Pieters, B.W. Schermer, S. Van der Hof, *Consent and privacy*, in A. Müller, P. Schaber, *The Routledge Handbook of the Ethics of Consent*, London, 2018, 247-258.

[92] Recital 24, European Parliament and Council, Directive (EU) 2019/770 del 20 maggio 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ* L 136/1, 2019. Sul Prezzo di mercato dei dati si rinvia tra i tanti a V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e* la n*uova epistemologia del giurista*, in *MediaLaws - Rivista di diritto dei media*, 2, 2018.

[93] Cfr. R. Brownsword, *The e-commerce directive, consumer transactions, and the digital Single Market – Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection*, in S. Grundmann (ed), *European Contract Law in Digital Age*, Intersentia, 2018, 165-204. Si veda anche dello stesso autore: *Automated transactions and the law of contract. When codes are not congruent*, in M. Furmston (ed), *The Future of the Law of Contract*, London, 2020.

[94] Ad esempio, proprio sul sito dedicato ai privacy patterns curato da accademici dell'Università di Berkeley, è possibile trovare soluzioni, implementazioni, fonti ed esempi di correttezza, abbinati ai dark pattern ivi censiti nell'ambito privacy.