Dark pattern e personalizzazione manipolativa: *fit check* del panorama legislativo europeo*

Edoardo Gatelli

Abstract

I *dark pattern* sono tecniche di manipolazione degli utenti in ambito digitale il cui impiego si colloca in una zona grigia tra legittimi tentativi di persuasione a fini commerciali e influenze indebite nel processo decisionale dei consumatori. Negli ultimi anni, il progresso tecnologico in ambiti quali la raccolta dati, la profilazione e l'intelligenza artificiale, ha portato le più recenti forme di manipolazione degli utenti ad un livello di persuasione molto più allarmante rispetto a quelli che ormai è possibile considerare come *dark pattern* tradizionali. Il quadro normativo europeo, se paragonato alla risposta pressoché soddisfacente del legislatore alle sfide poste dalla prima generazione di *dark pattern*, non appare altrettanto al passo coi tempi in relazione a questa nuova frontiera della manipolazione digitale; il principale punto di riferimento resta, infatti, il Regolamento generale sulla protezione dei dati (GDPR).

The employment of dark patterns – *i.e.* digital deceptive techniques aimed at manipulating users in the digital environment – falls in a blurred area between legitimate persuasion attempts for commercial purposes and undue influences in the decision-making process of consumers. In recent years, the technological advancement in such fields as data collection, profiling and artificial intelligence have brought the latest forms of user manipulation to another level with respect to what can by now be considered as traditional dark patterns. The European regulatory framework, if compared to the regulatory response to the challenges posed by first generation dark patterns, appears outdated towards this new frontier of digital manipulation and, therefore, the key to assess these phenomena from a legal perspective remains within the General Data Protection Regulation (GDPR).

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Edoardo Gatelli

Sommario

Keywords

dark pattern, manipolazione, personalizzazione, profilazione, GDPR.

1. Definizioni

I *dark pattern* possono essere definiti tecniche ingannevoli basate su tecnologie informatiche, più o meno complesse, strumentali alla manipolazione dei consumatori in ambito digitale. L'impiego di queste tecniche si colloca in una zona grigia tra legittimi tentativi di persuasione a fini commerciali e influenze indebite nel processo decisionale degli utenti. Il termine *dark pattern* venne coniato nel 2010 da Harry Brignull sul sito "*darkpatterns.org*"[1] in un pionieristico tentativo di catalogare le pratiche sleali rilevate con maggiore frequenza sulle piattaforme digitali di uso comune. L'espressione deriva dalla nozione di *design pattern* in ingegneria del software, ossia una soluzione generale e ripetibile ad un problema ricorrente nella progettazione software[2]. Pertanto, se l'idea di design pattern è quella di indentificare un problema e la relativa soluzione, astrarla dal caso specifico e modellarla in maniera più generica per poterla riutilizzare applicandola in diversi scenari, i *dark pattern* possono essere considerati come una particolare tipologia di *design pattern* intrinsecamente maligna e specificamente concepita per ingannare e manipolare gli utenti. Ad oggi, rinunciando al *pathos* del vocabolo "*dark*" in favore del più evocativo e chiaro "*deceptive*", il neologismo si è evoluto in "*deceptive patterns*", per quanto i due termini possano comunque essere utilizzati come sinonimi. Nel 2022, la Direzione generale della Giustizia e dei consumatori della Commissione europea ha pubblicato un report che fornisce una definizione generale del fenomeno, enucleando sommariamente le diverse caratteristiche catalogate dalla letteratura esistente sui *dark pattern*. In particolare, il report propone la seguente nozione di *dark pattern*: «*practices in digital interfaces that steer, deceive, coerce, or manipulate consumers into making choices that often are not in their best interests*»[3]. Rientrano in questa definizione, dunque, tutte le tecniche implementate in ambito digitale finalizzate a indurre, ingannare, costringere o manipolare gli utenti a prendere decisioni che, nella maggior parte dei casi, si rivelano contro il loro stesso interesse. Tuttavia, il report sottolinea anche l'esigenza di superare le singole definizioni specifiche, poiché, dal punto di vista del diritto dei consumatori dell'UE, esiste un concetto generale capace di comprendere tutte le pra-

[1] Vedi H. Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, in *A list apart: interaction design, usability,* 338, 1 novembre 2011.

[2] Vedi E. Gamma-J. Vlissides-R. Helm-R. Johnson, *Design Patterns: Elements of Reusable Object-Oriented Software*, in *Addison-Wesley Professional*, 31 ottobre 1994, 2.

[3] F. Lupiáñez-Villanueva-A. Boluda-F. Bogliacino-G. Liva-L. Lechardoy-T. Rodríguez De Las Heras Ballell, *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report*, in *Publications Office of the European Union*, aprile 2022, 20.

tiche commerciali manipolative a danno dei consumatori, indipendentemente dalle modalità utilizzate, ossia 'pratica commerciale sleale' ai sensi della direttiva 2005/29/CE[4] ("UCPD").

2. I *dark pattern* "tradizionali" e la tutela dei consumatori

È infatti possibile considerare la quasi totalità dei *dark pattern* catalogati dalla letteratura esistente[5] come pratiche commerciali scorrette alla luce della direttiva sulle pratiche commerciali sleali e, nonostante la sua entrata in vigore risalga a quasi vent'anni fa, l'UCPD grazie alla sua versatilità ancora oggi rappresenta la principale risposta del legislatore europeo alle pratiche commerciali scorrette in ambito digitale. Il che è stato reso possibile anche dalla ventata d'aria fresca portata dalla direttiva 2019/2161/UE (Direttiva *Omnibus*)[6] che ha esteso la normativa vigente adattandola a contenuti e servizi digitali, introducendo nell'UCPD disposizioni inedite come la disciplina dei motori di ricerca e delle recensioni online, rinforzando gli obblighi di informazione, introducendo la nozione di *ranking* e includendo servizi e contenuti digitali nella definizione di prodotto. Di contro, il regolamento 2022/2065/UE[7], c.d. *Digital Services Act* (DSA), non risulta applicabile ai *dark pattern*, nonostante il suo obiettivo fosse proprio quello di rivedere il quadro legislativo delineato dalla Direttiva sul commercio elettronico al fine di modernizzare l'approccio del legislatore europeo nell'affrontare le nuove sfide poste dai servizi online. Infatti, è possibile relegare il campo di applicazione del DSA alle pratiche commerciali sleali tra imprese (B2B), quantomeno per il momento. In particolare, nonostante il primo comma dell'articolo 25 del DSA introduca il primo divieto esplicito ai *dark pattern*, il secondo comma della medesima disposizione ne esclude l'applicabilità a quelle pratiche già disciplinate dal GDPR o dall'UCPD, ridimensionandone notevolmente la portata applicativa.

[4] 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 o Unfair Commercial Practices Directive).

[5] Secondo la tassonomia proposta nel report pubblicato dalla commissione europea, le uniche due tipologie di *dark pattern* identificate che non risultano a tutti gli effetti riconducibili alle previsioni della direttiva 2005/29/CE sono i cd. *infinite scroll* e *autoplay*, vedi ivi, 67.

[6] 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.

[7] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali o *Digital Services Act*).

3. Le nuove frontiere della personalizzazione manipolativa

Tuttavia, è fondamentale operare una distinzione tra i *dark pattern* "tradizionali", ossia quelli al centro dalla letteratura del primo decennio di tentativi di inquadramento del fenomeno in categorizzazioni sistematiche[8], e i *dark pattern* di seconda generazione. Infatti, negli ultimi anni, grazie al progresso tecnologico in ambiti come la raccolta dati, la profilazione e l'intelligenza artificiale, la progenie delle tattiche di manipolazione degli utenti nell'ecosistema digitale è diventata di gran lunga più subdola e allarmante rispetto a quelli che ormai è possibile considerare come *dark pattern* tradizionali. In particolare, di pari passo alla crescita esponenziale e disponibilità senza precedenti di vasti insiemi di dati (*big data*), le tecniche di raccolta dati, profilazione e targhettizzazione vengono sempre più implementate nel marketing digitale e abbinate alle sofisticate tecnologie di sviluppo degli algoritmi che governano le piattaforme digitali, fornendo terreno fertile per la proliferazione delle tecniche di manipolazione degli utenti incentrate sulla personalizzazione 'guidata dai dati' (*data-driven*). La genesi dei *dark pattern* di seconda generazione risiede proprio nell'integrazione di queste tecniche ai dark pattern tradizionali, aumentandone considerevolmente l'efficacia grazie alla possibilità di modellare la manipolazione alle specifiche caratteristiche di determinati gruppi di utenti, personalizzando dunque la manipolazione. Con riguardo a questa nuova forma di *deceptive pattern*, la risposta del legislatore europeo risulta anacronistica se paragonata agli avanzamenti tecnologici in questi campi, ma l'*Artificial Intelligence Act* e l'*Artificial Intelligence Liability Directive* promettono di riportare il quadro normativo comunitario al passo coi tempi. Tuttavia, un'analisi dell'impatto di questi nuovi interventi sull'impianto normativo europeo risulterebbe precoce – non essendo ancora applicabili – e, per questa ragione, l'attuale punto di riferimento nel panorama legislativo comunitario resta dunque il Regolamento generale sulla protezione dei dati[9] (GDPR).

4. Il GDPR e i *dark pattern* di seconda generazione

Al sesto considerando, il regolamento (UE) 2016/679 esordisce sottolineando la ne-

[8] Vedi G. Conti-E. Sobiesk, *Malicious interface design: exploiting the user*, in *Proceedings of the 19th international conference on World wide web (WWW '10),* 2010, 272; vedi anche C. Bösch-B. Erb-F. Kargl-H. Kopp-S. Pfattheicher, *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, in *Proceedings on Privacy Enhancing Technologies*, 2016; vedi anche C. M. Gray-Y. Kou-B. Battles-J. Hoggatt-A. L. Toombs, *The Dark (Patterns) Side of UX Design* in, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 2018; vedi anche A. Mathur-G. Acar-M. J. Friedman-E. Lucherini-J. Mayer-M. Chetty-A. Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites* in *Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 81*, 7 novembre 2019; vedi anche M. Leiser, *Illuminating Manipulative Design: from 'Dark Patterns' to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive*, in *Loyola Consumer Law Review,* 14 aprile 2022.

[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 o *General Data Protection Regulation*).

cessità di far fronte alle dinamiche di mercato in costante evoluzione:

> «La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano»[10].

Il principale riferimento alla personalizzazione *data-driven* all'interno del GDPR è rinvenibile all'articolo 22, rubricato «Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione»[11]. La norma garantisce all'interessato (ossia la persona fisica alla quale il dato personale si riferisce)[12] «il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[13]. Tuttavia, il seguente punto della medesima disposizione elenca le seguenti eccezioni, al ricorrere delle quali il primo comma non trova applicazione:

- «sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento»[14];
- «sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato»[15];
- «si basi sul consenso esplicito dell'interessato»[16].

Inoltre, è rilevante sottolineare come al terzo comma la norma impone al titolare del trattamento[17] l'obbligo, nell'eventualità in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra le parti o si basi sul consenso esplicito dell'interessato, di adottare «misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[18]. Essenzialmente, salvo le suddette eccezioni, al fine di accertare la riconducibilità di una determinata tecnica di personalizzazione alla fattispecie delineata dal primo comma dell'articolo 22 del GDPR, è fondamentale stabilire se la decisione sia stata presa

[10] Considerando 6, GDPR.

[11] Art. 22, GDPR.

[12] Vedi art. 4, n. 1, GDPR.

[13] Art. 22, par. 1, GDPR.

[14] Art. 22, par. 2, lett. a), GDPR.

[15] Ivi, lett. b).

[16] Ivi, lett. c)

[17] Vedi art. 4, n. 7), GDPR.

[18] Art. 22, par. 3, GDPR.

esclusivamente sulla base di un trattamento automatizzato dei dati e se la stessa sia tale da produrre un effetto giuridicamente rilevante per l'interessato o qualsiasi altra conseguenza ad esso paragonabile sulla sua persona. Il testo del GDPR non contiene però alcuna specifica menzione alla personalizzazione manipolativa e pertanto è alle nozioni di profilazione e di processo decisionale automatizzato che bisogna fare riferimento. Il regolamento definisce la profilazione come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[19]. Alla luce di questa nozione è quindi possibile evidenziare alcuni aspetti caratterizzanti della profilazione: il trattamento dei dati dev'essere automatizzato, deve riguardare dati personali e tale trattamento dev'essere strumentale alla valutazione di certi aspetti personali dell'interessato. Per quanto concerne invece il processo decisionale automatizzato, il GDPR si limita a menzionarlo senza fornirne una specifica definizione, la quale dev'essere ricavata invece dalle "Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679"[20]: «*the ability to make decisions by technological means without human involvement*»[21], ossia la capacità di elaborare una decisione tramite strumenti tecnologici senza il coinvolgimento dell'essere umano. Le Linee guida precisano poi come – per quanto il trattamento dei dati relativo ad un processo decisionale automatizzato possa portare alla profilazione – i processi decisionali automatizzati prescindono dalla profilazione, e viceversa, sottolineando dunque come le due tecniche non siano in rapporto di interdipendenza. Infine, le Linee guida includono anche il seguente catalogo dei riferimenti normativi di profilazione e processo decisionale automatizzato nel testo del GDPR, il che risulta particolarmente utile nel sintetizzare efficacemente in una panoramica il modo in cui il regolamento disciplina la personalizzazione guidata dai dati.

«Principali disposizioni del Regolamento che fanno riferimento alla profilazione e al processo decisionale automatizzato in generale»[22]

[19] Art. 4, n. 4, GDPR.

[20] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 3 ottobre 2017, disponibile su ec.europa.eu

[21] Ivi, 8.

[22] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, allegato 2, 37, 3 ottobre 2017, disponibile su ec.europa.eu

Articolo	Considerando	Osservazioni
3, paragrafo 2, lettera b)	**24**	Il monitoraggio del comportamento [degli interessati] nella misura in cui tale comportamento ha luogo all'interno dell'Unione. **Considerando 24:** " (...) tracciate su internet (...) ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, *in particolare per adottare decisioni* che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".
4, paragrafo 4	**30**	**Articolo 4, paragrafo 4** definizione di profilazione **Considerando 30:** "identificativi online (...), quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza (...) possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, *possono essere utilizzate per creare profili delle persone fisiche e identificarle*".
5 e 6	**72**	**Considerando 72**: "la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento **(articolo 6)** o i principi di protezione dei dati **(articolo 5)**".
8	**38**	Utilizzo dei dati personali dei minori per la profilazione. **Considerando 38:** "I minori meritano una specifica protezione (...) in particolare [in merito al]l'utilizzo dei dati personali dei minori a fini di (...) creazione di profili di personalità o di utente".
13 e 14	**60**	Diritto di essere informato. **Considerando 60**: "inoltre l'interessato [*deve] essere informato dell'esistenza di una profilazione e delle conseguenze della stessa*".
15	**63**	Diritto di accesso. **Considerando 63:** "diritto di conoscere e ottenere comunicazioni (...) in relazione alla finalità per cui i dati personali sono trattati (...) e, *almeno* quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento".
21, paragrafi 1, 2 e 3	**70**	Diritto di opposizione alla profilazione. **Considerando 70:** "(…) il diritto (...) di opporsi a tale trattamento (...), compresa la profilazione nella misura in cui sia connessa a tale marketing diretto".
23	**73**	**Considerando 73:** "il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e (...) al diritto di opporsi, alle decisioni basate sulla profilazione (...), ove ciò sia necessario e proporzionato in una società democratica (...)" per la tutela di obiettivi specifici di interesse pubblico generale.
35, paragrafo 3, lettera a)	**91**	Una valutazione d'impatto sulla protezione dei dati è necessaria nel caso di una "valutazione sistematica e globale di aspetti personali relativi a persone fisiche, *basata* su un trattamento automatizzato, che include la profilazione, e in base al quale si adottano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche". **Riguarda il processo decisionale, compresa la profilazione, che è non si basa unicamente su un trattamento automatizzato.**

5. I principi generali del GDPR

Risulta dunque lecito affermare che la personalizzazione *data-driven* non è universalmente proibita quanto, piuttosto, subordinata al rispetto delle previsioni del GDPR o più in generale della normativa vigente. A tal riguardo, è essenziale quantomeno accennare i punti cardine del regolamento ai quali è possibile ricondurre la maggior parte delle tecniche di manipolazione online. Il principio generale è quello della correttezza del trattamento dei dati personali sancito al primo comma dell'articolo 5 del GDPR, che impone un «trattamento dei dati lecito, corretto e trasparente nei confronti dell'interessato»[23]. Questo principio generale esige tuttavia di essere articolato lungo i tre pilastri del GDPR: la trasparenza, la limitazione dello scopo del trattamento e la minimizzazione dei dati. Innanzitutto, il principio di trasparenza emerge dal combinato disposto del principio di correttezza con il primo comma dell'articolo 12 del GDPR, che impone ai titolari del trattamento l'adozione di «misure appropriate per fornire all'interessato tutte le informazioni […] e le comunicazioni […] relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro». Sulla base di tale principio, nel 2022 l'Autorità garante per la protezione dei dati francese (CNIL) ha comminato una sanzione di 150 milioni di euro a Google per non aver fornito informazioni facilmente accessibili dagli utenti sul trattamento dei loro dati personali[24]. Per quanto concerne invece il principio di limitazione dello scopo del trattamento, la lettera B del primo comma dell'articolo 5 del GDPR sancisce come i dati personali debbano essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»[25]. Il terzo principio fondamentale da considerare nell'analisi del GDPR in relazione al fenomeno dei *dark pattern* è poi sancito dalla lettera C del primo comma dell'articolo 5 del GDPR, la c.d. minimizzazione dei dati, che impone che i dati personali siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati»[26]. È rilevante, tuttavia, menzionare un ulteriore concetto fondamentale per l'applicazione del GDPR, ossia quello del consenso dell'interessato, in quanto molte delle tattiche di manipolazione degli utenti in esame sono finalizzate ad indurre gli utenti a prestare il proprio consenso al trattamento dei dati senza che sussistano quei requisiti di «volontà libera, specifica, informata e inequivocabile dell'interessato»[27] che dovrebbero invece caratterizzare l'espressione del consenso secondo il GDPR.

Infine, è fondamentale anche il riferimento alle Linee guida pubblicate nel 2022 dal Comitato europeo per la protezione dei dati (EDPB) in merito all'implementazione di *deceptive pattern* nelle piattaforme di social media[28], che predispongono una classificazio-

[23] Art. 5, par. 1, lett. a), GDPR.

[24] Vedi Commission Nationale de l'Informatique et des libertés [CNIL], *Deliberation of the restricted committee No. SAN-2021-023 of 31 December 2021 concerning GOOGLE LLC and GOOGLE IRELAND LIMITED*, 31 dicembre 2021, disponibile su *cnil.fr*

[25] Art. 5, par. 1, lett. b), GDPR.

[26] Art. 5, par. 1, lett. c), GDPR.

[27] Art. 4, n. 11, GDPR.

[28] Comitato europeo per la protezione dei dati, *Guidelines 03/2022 on Deceptive design patterns in social media*

ne delle diverse tecniche riconducendole alla rispettiva previsione del GDPR potenzialmente violata. In aggiunta, le Linee guida hanno proposto anche la distinzione tra «*content-based patterns*»[29], cioè tecniche basate sul contenuto effettivo delle informazioni veicolate agli utenti, sul modo in cui vengono formulate e il contesto nel quale vengono fornite, e gli «*interface-based patterns*»[30], ossia quelle tattiche che sfruttano le modalità di visualizzazione dei contenuti e di interazione con gli stessi da parte degli utenti.

platform interfaces: how to recognise and avoid them. Version 2.0, 14 February 2023, disponible su edpb.europa.eu

[29] Ivi, 10.

[30] *Ibid.*