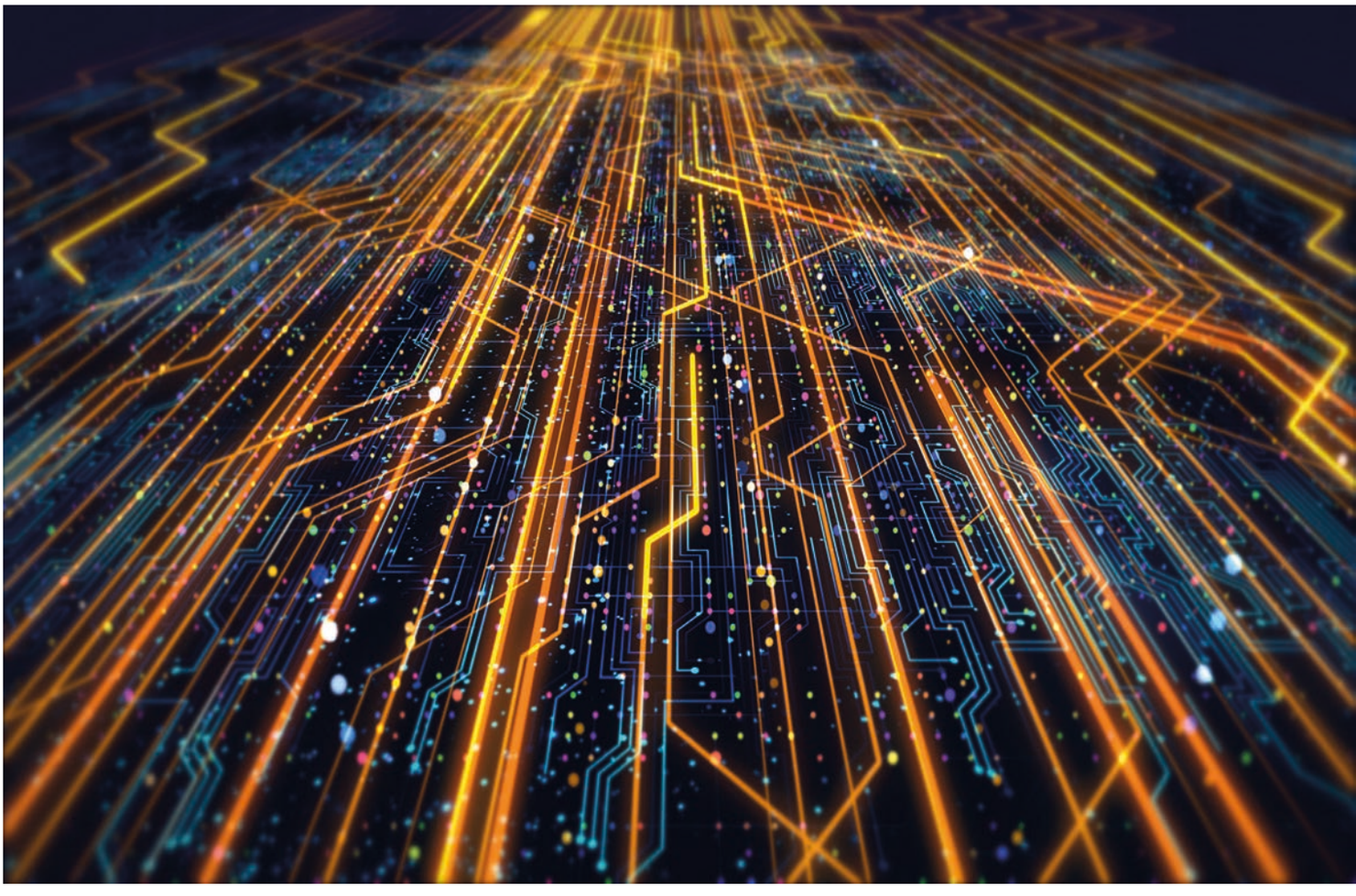
LES REVUES LEXISNEXIS

REVUE PRATIQUE DE LA PROSPECTIVE ET DE L'INNOVATION

JUSTICE - DROIT - SOCIÉTÉ

Direction :
Sophie FERRY

NOVEMBRE 2022 - **N°2**
6e ANNÉE - ISSN 2497-2703



▶ ENTRETIEN

2 > p. 4
« L'avocat doit faire preuve de créativité et d'audace, il doit aussi continuer à douter toujours »
entretien avec Richard Malka

▶ DOSSIER

11 > p. 6
Demain : l'avocat de l'an 2000 !
par Philibert Ledoux
présenté par Hervé Croze

▶ DOSSIER

12 > p. 10
Les progrès en neurosciences : quel impact sur le fonctionnement de la justice dans les années à venir ?
par Philippe Damier

LexisNexis
Lexis Kiosque
CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

Sommaire

P. 1 **Édito**

Le futur a-t-il de l'avenir ? ..... **n° 2**

La vie des idées

P. 2 **Focus**

Le Dictionnaire Juridique du Changement Climatique : savoir et justice climatique à portée de main ..... **n° 2**

P. 4 **Entretien**

« L'avocat doit faire preuve de créativité et d'audace, il doit aussi continuer à douter toujours » ..... **n° 2**

P. 6 **Dossier**

Demain : l'avocat de l'an 2000 ! ..... **n° 11**

Les progrès en neurosciences : quel impact sur le fonctionnement de la justice dans les années à venir ? ..... **n° 12**

Au Pays de Galles, le développement durable et de la protection des générations futures érigés en obligation légale ..... **n° 13**

Le genre à l'épreuve des algorithmes ..... **n° 14**

Avortement aux États-Unis, pour les droits des femmes, l'enfer est pavé de bonnes intentions ..... **n° 15**

Compliance et métavers - une éthique réelle dans un monde virtuel ..... **n° 16**

Marché européen des données : ce qu'il faut savoir ..... **n° 18**

Dark Patterns : l'étau législatif se resserre (enfin ?) sur les interfaces manipulatrices ou trompeuses ..... **n° 19**

Plaidoyer pour un cadre de droit souple applicable aux jetons non-fongibles ..... **n° 20**

P. 52 **Pratique professionnelle**

Comprendre les ressorts de la nouvelle génération d'avocats : une stratégie gagnante ..... **n° 2**

L'avocat et « sa » parole ..... **n° 3**

P. 58 **Le point sur**

Un métier féminisé et difficile. Réflexions sur l'actualité et l'avenir de la magistrature française ..... **n° 2**

Justice et blockchain : vers l'émergence d'un nouveau type de justice dite décentralisée ? ..... **n° 3**

Index

Avocat
- Exercice de la profession ..... entretien 2, prat. 3, repère 2
- Formation ..... prat. 2

Injustices
- Droit des femmes ..... étude 15
- Injustices citoyennes ..... étude 13
- Justice climatique ..... alerte 2

Justice
- Exercice de la justice ..... prat. 2
- Numérique ..... prat. 3

Nouvelles technologies
- Algorithmes ..... étude 14
- Internet ..... étude 19
- Justice ..... étude 12

Numérique
- Données ..... étude 18
- Métavers ..... étude 16
- NFT ..... étude 20

Prospective
- Droit ..... étude 11

Evoluprint - Parc Industriel Euronord, 10, rue du Parc, 31150 Bruguières - Le Directeur de la publication : Éric Bonnet-Maes.

Cette revue peut être citée de la manière suivante : RPPI 2022, édito 1 ; RPPI 2022, alerte 1 ; RPPI 2022, entretien 1 ; RPPI 2022, dossier 1 ; RPPI 2022, idée nouvelle 1 ; RPPI 2022, le point sur 1

19

Dark Patterns : l'étau législatif se resserre (enfin ?) sur les interfaces manipulatrices ou trompeuses

Marie POTEL-SAVILLE,
Fondatrice d'Amurabi, innovation juridique par le design

« *J'accepte* ». Qui n'a pas cliqué sans y penser sur le beau gros bouton bien vert, au lieu des petits liens gris en dessous ? Pire, qui aura réussi à se désabonner sans perdre son temps ni ses nerfs, alors qu'il avait suffi d'un clic pour « *essayer gratuitement* » ? Ces interfaces ne doivent rien au hasard. Elles jouent sur nos biais cognitifs pour nous influencer, voire nous manipuler. Le phénomène des « *dark patterns* » est endémique et mondial. Les régulateurs et législateurs en Europe et dans le monde ont pris la mesure du danger pour la confiance dans l'économie numérique, voire dans l'économie de marché tout court. Des interdictions spécifiques voient le jour, comme le *Digital Services Act*, en complément de l'arsenal législatif existant en droit des données personnelles, de la consommation et de la concurrence. Cela serait-il suffisant pour restaurer la souveraineté des utilisateurs ?

Introduction

1 - Le règlement européen sur les services numériques (DSA, pour *Digital Services Act* [1]), l'un des grands chantiers numériques de l'Union européenne avec le règlement sur les marchés numériques (DMA [2]), interdit pour la première fois en Europe – expressément et dans un texte contraignant [3] – les « *dark patterns* ».

2 - Si le terme est connu du monde académique, où professeurs de droit, chercheurs en interaction homme-machine, et certains designers ont développé depuis une douzaine d'année une riche littérature sur la notion de « *dark pattern* » [4] ou « *deceptive pattern* [5] », la façon dont ils manipulent nos biais congitifs, leur taxonomie [6], leurs critères d'évaluation et leur régulation [7], il est encore relativement peu connu des entreprises et des juristes.

3 - Cela nous conduit à nous pencher sur la définition des *dark patterns* (1), mais aussi à analyser les difficultés pour les êtres humains et la société créées par ces interfaces-pièges (2). Face à un phénomène d'ampleur mondiale (3), un maillage réglementaire se met en place en Europe et aux États-Unis, où des interdictions spécifiques viennent compléter l'arsenal général en droit de la consommation, droit de la protection des données personnelles, droit de la concurrence et droit sectoriel (4). Cet étau juridique sera-t-il suffisant pour endiguer un phénomène planétaire ? Quelles sont les nouvelles compétences des juristes, mais aussi des législateurs, requises pour pleinement appréhender ce phénomène et y mettre un terme ?

1. Qu'est-ce qu'un *dark pattern* ?

4 - Selon l'article 25 (1) du DSA, qui pose les obligations de transparence qui pèsent sur les fournisseurs de plateformes en ligne, il s'agit d'une interface digitale qui « *trompe, manipule, altère ou entrave substantiellement la capacité des utilisateurs à prendre des décisions libres et éclairées* », en raison de son « *design, de son organisation ou de la façon dont elle est opérée* » [8]

1. *PE et Cons. UE, règl., 19 oct. 2022, relatif à un marché intérieur des services numériques (législation sur les services numériques, dit DSA) et modifiant la directive 2000/31/CE.*
2. *PE et Cons. UE, 14 sept. 2022, règl. relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques dit DMA).*
3. Le DSA s'appliquera, dès février 2024, à tous les intermédiaires en ligne qui offrent leurs services (biens, contenus ou services) sur le marché européen : les fournisseurs d'accès à internet (FAI) ; les services d'informatique en nuage (cloud) ; les plateformes en ligne comme les places de marché *(market places)*, les boutiques d'applications, les réseaux sociaux, les plateformes de partage de contenus, les plateformes de voyage et d'hébergement ; les très grandes plateformes en ligne et les très grands moteurs de recherche, utilisés par plus de 45 millions d'Européens par mois. Cette catégorie vise en particulier les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), même s'ils ne sont pas directement nommés.
4. *Brignull, H. (2022), Types of deceptive design. Accédé le 20 août 2022 à partir de www.deceptive.design/types.*
5. Certains auteurs préfèrent le terme « *deceptive pattern* », pour éviter tout malentendu sur une quelconque connotation péjorative associée au terme « *dark* ». L'autrice adhère pleinement à cette précaution, toutefois dans la mesure où les régulateurs utilisent le terme « *dark pattern* » dans les textes de loi, cet article fait de même dans un souci de clarté.
6. *V. not. Brignull, H. préc. – Jarovsky, L. (2022). Dark Patterns in Personal Data Collection : Definition, Taxonomy and Lawfulness. Taxonomy and Lawfulness (March 1, 2022). – Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April), The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (p. 1-14). – Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019), Dark patterns at scale : Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3 (CSCW), 1-32.*
7. *V. not. King J., Adriana S. (2021), Regulating privacy dark patterns in practice – Drawing inspiration from California Privacy Act. 5 GEO. L. TECH. REV. 250 (2021), Leiser, M.R. (2020). Dark Patterns : The case for regulatory pluralism https://doi.org/10.31228/osf.io/ea5n2.*
8. *Il existe une riche littérature scientifique sur la définition des dark patterns, avec différentes taxonomies. Cet article se limite aux définitions juridiques. V. not. Mathur, A. et a. (2021). What Makes a Dark Pattern... Dark ? Design Attributes, Normative Considerations, and Measurement Methods. Human-Computer Interaction https://doi.org/10.1145/3411764.3445610. – Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April), The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (p. 1-14). – Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021, June). – « I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous ! » – Dark Patterns from the End-User Perspective. In Designing Interactive Systems Conference 2021 (p. 763-776). – Maier, M., & Harr, R. (2020), Dark design patterns : An end-user perspective. Human Technology, 16 (2), 170. – Waldman, A. E. (2020). Cognitive biases, dark patterns, and the « privacy paradox ». Current opinion in psychology, 31, 105-109.*

5 - En d'autres termes, et selon le point 67 du préambule du DSA [9], ce sont des mécanismes qui poussent les utilisateurs à agir de façon involontaire, ou à prendre des décisions non souhaitables, qui peuvent avoir des conséquences négatives sur eux-mêmes.

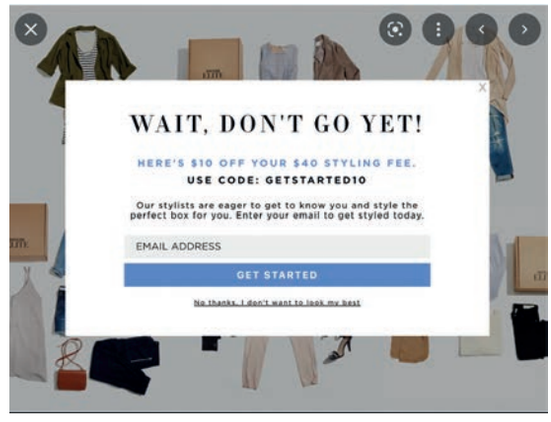
Il s'agit donc de tromperie ou de manipulation au travers d'interfaces digitales.

6 - 3 pratiques sont visées par l'article 25 (3), sans bien sûr que cette liste ne soit exhaustive :

- mettre en avant certains choix lorsqu'il est demandé à l'utilisateur de prendre une décision (ex. type : un bouton *« J'accepte »* vert, engageant, ou plus gros que le bouton *« Je refuse »* mais il existe des cas plus sournois et difficiles à repérer pour les utilisateurs) ;

Légende : Dans cet exemple [10], le bouton « Continue » est très engageant (et semble même la seule option pour poursuivre la réservation, alors qu'il dirige vers une sélection de siège payante, mais non obligatoire), alors que « Skip seat selection » n'est pas un bouton et ne ressemble même pas un lien, donc l'utilisateur pourrait penser qu'il n'est pas possible de cliquer. Dans tous les cas, il est très fortement dirigé vers l'option payante.

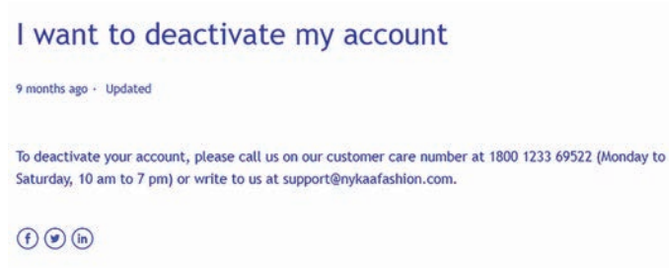
- continuer à demander à l'utilisateur de faire un choix alors qu'il l'a déjà fait, en particulier en présentant un *pop-up* qui interfère avec l'expérience utilisateur (ex. type : lorsqu'un utilisateur souhaite annuler son achat, désactiver une fonctionnalité, l'interface demande *« êtes-vous sûr de vouloir annuler ? »*, éventuellement avec une formulation dite *« confirm shaming »* où l'action que souhaite faire l'utilisateur est présentée comme le mauvais choix *« je ne souhaite pas bénéficier de la réduction de X % »*, pour dissuader l'utilisateur de cliquer sur ce bouton) ;



Légende : Dans cet exemple, l'utilisateur a déjà cliqué sur « annuler », mais l'interface lui pousse un pop-up « Wait, don't go yet », avec un bouton bleu très engageant « get started », ou un lien pour décliner, beaucoup moins visible et moins engageant, qui contient en outre une formulation dite de « confirmshaming », où le choix des mots est fait pour dissuader l'utilisateur de cliquer sur ce lien. Ici « No thanks, I don't want to look my best », manifestement rédigé pour que celui qui clique se sente idiot.

- ou encore rendre la résiliation d'un service plus difficile que la souscription (ex. type : pour mettre à un abonnement, l'utilisateur doit cliquer à de multiples endroits, voire n'arrive pas trouver comment procéder, alors qu'il a suffi d'un clic pour souscrire).

9. *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CONSIL:PE_30_2022_REV_1=1666618253097=EN , accédé le 24 oct. 2022.*
10. *Pour être parfaitement clair, aucun exemple illustré (copies d'écran ou interfaces type) ne figure dans le texte actuel du DSA. Il reviendra sans doute à la Commission d'indiquer des exemples illustrés dans ses lignes directrices à venir. Pour autant, de très nombreux exemples illustrés sont présents dans l'abondante littérature citée dans cet article, et en matière de données personnelles dans les Lignes directrices du Comité européen des données personnelles sur les dark patterns sur les réseaux sociaux : https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.*



Légende : Dans cet exemple, il a suffi d'un clic pour créer son compte, mais il faut appeler un service commercial, ou écrire un mail pour le supprimer

La Commission européenne pourra préciser, vraisemblablement sous forme de lignes directrices, comment l'article 25 (3) s'applique à des pratiques spécifiques, dont les 3 exemples ci-dessus.

La structure, le design et les fonctionnalités d'une interface pourront désormais faire l'objet d'une analyse juridique de conformité au regard du DSA (outre les autres textes déjà mobilisables tels que la directive sur les pratiques déloyales [11] ou le RGPD [12] *(V. pt IV, ci-dessous)*. Il s'agit d'assurer la « souveraineté utilisateurs ».

2. En quoi les *dark patterns* sont-ils problématiques ?

7 - *« Avez-vous déjà cliqué juste ici ? Vous le ferez ».*

8 - C'est ce qu'indiquait la bannière du site Wired dès 1994, dans une première tentative de *dark pattern*. Grossier mais sans doute efficace, ainsi que le rapporte le laboratoire d'innovation de la CNIL, le LINC, dans ses Cahiers innovation et prospective, *« La Forme des Choix »* [13].

9 - Dans l'économie de l'attention, qui vend du *« temps de cerveau disponible »* non plus seulement pour du soda mais pour collecter des données toujours plus nombreuses et granulaires, le sociologue Dominique Boullier rappelle que *« tout l'enjeu de cette lutte pour capter le temps de cerveau disponible consiste à réduire à l'extrême les hésitations et les arbitrages conscients »*. En d'autres termes, nous rendre moins conscients de nos choix en ligne, voire les manipuler, serait un business model. Mais limiter notre autonomie et liberté de choix est-il le meilleur modèle économique pour nos sociétés ?

Selon l'OCDE, la transparence de l'information est l'une des conditions pour que l'économie de marché continue à être le modèle qui produit les meilleurs bénéfices pour les consommateurs [14].

10 - La récente étude de la Commission européenne sur les *dark patterns* [15] rappelle que les conséquences néfastes pour les consommateurs ont été largement documentées ces dernières années : pertes financières, altération de l'autonomie et de la vie privée, charges cognitives, et dans certains cas altération de la santé mentale (addictions...), outre des risques d'altération de la concurrence, diminution de la transparence des prix et in fine perte de confiance dans les marchés. Cette étude démontre en outre que les *dark patterns* affectent particulièrement les consommateurs vulnérables. Or, un tiers des internautes dans le monde sont des mineurs [16], officiellement vulnérables et devant bénéficier d'une protection accrue aux termes du RGPD, notamment..

11 - Aux États-Unis, Maya MacGuineas, présidente du comité pour un budget fédéral responsable, a affirmé en 2020 que dans un marché qui fonctionne bien, les consommateurs ont la liberté d'agir dans leur propre intérêt, pour maximiser leur bien-être, *« mais les nouveaux pouvoirs de l'ère digitale ont construit leur modèle sur des stratégies qui mettent à mal les principes qui font du capitalisme un " bon deal " pour la plupart des gens »*.

La préservation de la liberté de faire des choix éclairés en ligne est bien une condition du bon fonctionnement de l'économie de marché. Se pose alors la question de savoir à quel point les *dark patterns* altèrent ce bon fonctionnement.

3. Quelle est l'ampleur du phénomène des *dark patterns ?*

12 - Le terme *« dark pattern »* a été conceptualisé par le designer et docteur en sciences cognitives Harry Brignull dès 2010 [17], qui ne listait déjà pas moins de 12 types différents de *dark patterns* [18]. Ce terme a été repris par une large communauté de chercheurs à travers le monde, avec une abondante littérature scientifique [19].

11. *PE et Cons. UE, dir. 2005/29/CE, 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales »).*
13. *CNIL, Cahiers innovation et prospective n° 2, janv. 2019, https://linc.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf*
14. *OCDE (2018), Improving online disclosures with behavioural insights, Documents de travail de l'OCDE sur l'économie numérique : Éditions OCDE, Paris, n° 269, https://doi.org/10.1787/39026ff4-en..*
15. *Commission européenne, Direction Générale Justice et Consommateurs (2022). – Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et a., Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report, Publications Office of the European Union, https://data.europa.eu/doi/10.2838/859030.*
16. *V. not. : Potel-Saville, M., Talbourdet, E. (2021), Empowering children to understand and exercise their personal data rights. Legal Design Perspectives, Ledizioni, 10.5281/zenodo.5710845.*
17. *https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/. Harry Brignull, Dark Patterns : Deception vs. Honesty in UI Design, November 01, 2011, Interaction Design Journal, Issue 338.*
18. *Aujourd'hui, son site www.deceptive.design/(accédé le 20 août 2022) fournit une classification en 12 catégories, des liste de sources académiques et un « Hall of Shame » qui recense des milliers d'exemples en ligne.*

13 - En 2018, le Conseil norvégien des consommateurs a jeté un pavé dans la marre juste avant l'entrée en vigueur du RGPD avec son rapport *« Deceived by Design »* [20]. Cet organisme de protection des consommateurs financé par le gouvernement norvégien a analysé les paramètres de création et de gestion de compte de Facebook, Google et Windows 10, et identifié des **dizaines d'interfaces « *privacy intrusive* » : conduisant les utilisateurs à partager plus de données personnelles qu'ils ne l'auraient fait consciemment**. Parmi les *dark patterns* identifiés figurent notamment des paramètres par défaut intrusifs, l'illusion de donner le contrôle aux utilisateurs sur leurs données personnelles, détourner les utilisateurs des choix protecteurs de leur vie privée, ou rendre ces choix plus difficiles.

	Facebook	Google	Windows	Chapter
No privacy intrusive default settings in popups	✗	✗	✓	4.1
Equal ease (number of clicks) for privacy friendly options in popups	✗	✗	✓	4.2
Design (colours and symbols) does not lead toward privacy intrusive option in popups	✗	✗	✗	4.2
Language does not lead toward privacy intrusive option in popups	✗	✗	✗	4.3
Privacy friendly options in popups come without "warnings"	✗	✗	✓	4.4
Users can clearly postpone the decision while accessing the service in the meantime	✗	✗	✗	4.5

Source : Extrait du rapport du Conseil Norvégien des Consommateurs, « Deceived by Design », p. 3

14 - En 2019, des chercheurs de Princeton et de l'université de Chicago ont pour leur part analysé environ **11 000 sites e-commerce les plus populaires** [21] dans le monde (en anglais), dont 53 000 pages produits et identifié **1 818 cas de *dark patterns*** [22]. Au passage, ces chercheurs ont aussi identifié 22 fournisseurs de services qui offrent des interfaces *dark patterns « clés en main »*, présents dans 1 066 des sites analysés. Ainsi, certains fournisseurs offrent des *plug-ins, pop-ups* ou autres interfaces prêtes à l'emploi qui visent ouvertement à *« jouer sur la peur des consommateurs de rater quelque chose, en montrant que certains produits créent du buzz »* (fournisseur : Fresh Relevance), *« créer un sentiment d'urgence pour booster les conversations et accélérer le cycle de vente »* (fournisseur : Insider), ou encore un *« plug-in qui va créer des faux achats »* ou des *« faux messages de réseaux sociaux »* (fournisseur : Woocommerce) [23];

15 - Dans son étude comportementale sur les *dark patterns* d'avril 2022 [24], la Commission européenne met en évidence leur caractère endémique : **97 % des sites e-commerce et applications les plus populaires auprès des consommateurs européens contiennent au moins un *dark pattern***. Les plus répandus sont les suivants :

- information cachée/fausse hiérarchie (par ex., pour choisir entre deux packages, l'information sur le 2e est partiellement cachée et ne peut être vue qu'en cliquant sur trois petits points) ;
- préselection (choix par défaut les moins favorables aux consommateurs) ;
- *« Nagging »* (réorientation de l'utilisateur qui persiste malgré plusieurs actions) ;
- résiliations/annulations difficiles (résiliation complexe, longue ou impossible alors qu'il est possible de s'abonner ou d'acheter en un clic) ;
- enregistrement forcé (obligation de créer un compte).

Cette étude comporte notamment deux expérimentations édifiantes :

- l'une en laboratoire, visant à tester les réactions neurophysiologiques et psychologiques des consommateurs, dans trois États membres (Italie, Allemagne, Espagne), avec 120 participants. Cette expérimentation a montré que le *dark pattern « action forcée »* (la conception de l'interface force l'utilisateur à effectuer une action non souhaitée), combinée à de la personnalisation a limité la capacité des participants à effectuer une tâche quotidienne banale en ligne - mais aussi a augmenté leur rythme cardiaque lors de l'apparition des pop-ups contenant les dark patterns, et pourrait être lié à une augmentation de l'anxiété et de l'état d'alerte. Sans parler de la frustration des participants, évidente ;
- l'autre en ligne, pour tester les impacts de pratiques déloyales sur la prise de décision des consommateurs dans 6 États membres (Bulgarie, Allemagne, Italie, Espagne, Pologne et Suède), avec 7 430 participants. Ce test visait à déterminer si l'exposition à des *dark patterns* conduit les consommateurs à prendre des décisions qu'ils n'auraient pas prises autrement – c'est-à-dire si les *dark patterns* génèrent une altération de la rationalité et remplissent les conditions de pratiques déloyales au sens de la directive relative aux pratiques déloyales. Les résultats montrent que les ***dark patterns « information cachée », « jouer sur les émotions » et « jouer sur les émotions avec personnalisation »* affectent la prise**

19. *V. not. Maier, M., & Harr, R. (2020). Dark design patterns : An end-user perspective. Human Technology, 16 (2), 170. – Jarovsky, L. (2022), préc. – Waldman, A. E. (2020), précité ; Chang, D., Krupka, E. L., Adar, E., & Acquisti, A. (2016, May), Engineering information disclosure : Norm shaping designs. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (p. 587-597). – Isaac Dinner, Eric Johnson, Daniel Goldstein, Kaiya Liu, Partitioning Default Effects : Why People Choose Not to Choose (2011) 17 J. Exp. Psy.-Appl. 332, 335. – Jentzsch, N., Preibusch, S., & Harasser, A. (2012), Study on monetising privacy : An economic model for pricing personal information. ENISA, Feb, 1 (1).*
20. *Frobrukerrådet, Deceived by design : How tech companies use dark patterns to discourage us from exercising our rights to privacy (2018).*
21. Selon Alexa Top Sites – API Reference. *https://docs.aws.amazon.com/AlexaTopSites/latest/ApiReferenceArticle.html.*
22. *Mathur et a., Dark Patterns at Scale : Findings from a Crawl of 11K Shopping Websites, 2019, Proc. ACM Hum.-Comput. Interact. Ces chercheurs ont automatisé une partie de la détection des dark patterns de la façon suivante : automatisation du parcours primaire d'interaction avec les sites, extraction des éléments textuels de l'interface présent dans ce parcours, regroupement et clusterisation, puis analyse de chaque cluster par un expert.*
23. *Mathur et a., Dark Patterns at Scale : Findings from a Crawl of 11K Shopping Websites, 2019, Proc. ACM Hum.-Comput. Interact. Ces chercheurs ont automatisé une partie de la détection des dark patterns de la façon suivante : automatisation du parcours primaire d'interaction avec les sites, extraction des éléments textuels de l'interface présent dans ce parcours, regroupement et clusterisation, puis analyse de chaque cluster par un expert, p. 24.*
24. *Commission européenne, Direction Générale Justice et Consommateurs (2022). – Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et a., Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report, Publications Office of the European Union, https://data.europa.eu/doi/10.2838/859030.*

de décision des consommateurs, et conduisent à des incohérences par rapport à leurs préférences. Le *dark pattern « information cachée »* est celui qui conduit au plus fort degré d'incohérence avec les préférences des consommateurs.

Enfin, les résultats de ces deux études indiquent que les *dark patterns* affectent particulièrement les plus vulnérables : ils conduisent les personnes âgées ou les personnes peu éduquées à des décisions incohérentes par rapport à leurs préférences (10 % de différence par rapport aux autres groupes).

16 - En ligne, nous sommes donc entourés de *dark patterns*. L'autrice de ces lignes, dont l'œil est désormais exercé à les repérer, en croise plusieurs tous les jours lors de sa navigation. Pourtant, de nombreux textes prohibent des interfaces trompeuses et manipulatrices.

4. Quels sont les textes qui interdisent les *dark patterns* ?

17 - De très nombreux textes au niveau européen et dans le monde sont déjà applicables aux *dark patterns*, en tant que pratiques déloyales ou contraires au droit de la protection des données personnelles, et de nouveaux textes ont vu le jour pour les interdire expressément, en tant que *« dark patterns »*.

Il est important de noter que le DSA ne sera applicable aux *dark patterns* que s'ils ne sont pas déjà interdits par la directive relative aux pratiques commerciales déloyales ou par le RGPD [25].

Légende : Visualisation des sanctions en cas de dark patterns

A. - De nombreux textes existants, déjà applicables aux *dark patterns*

18 - **Au niveau européen**, il existe un large corpus législatif déjà applicable aux *dark patterns* :

a) En droit de la consommation

- La directive relative aux pratiques commerciales déloyales [26], en particulier ses articles 5, 6, 7 et 8, et l'annexe de pratiques interdites, qui s'appliquent à tous les *dark patterns* qui créent de la confusion ;
- La directive relative aux droits des consommateurs 2011/83/EU, qui s'applique notamment aux *dark patterns « paramètres par défaut défavorables aux consommateurs »*, *« coûts cachés »* et *« rajouter dans le panier »* ;
- La directive relative aux clauses abusives 93/13/EEC qui s'applique aux *dark patterns « surcharge d'information »* (c'est-à-dire les murs de texte inintelligibles) ou *« questions piège »* (par ex., doubles négations, ou texte contraire à ce que suggère l'interface), notamment ;

b) En droit de la protection des données personnelles

- Le RGPD impose des principes de transparence, loyauté des traitements et minimisation de la collecte des données personnelles, lesquels s'opposent globalement à tous les *dark patterns* visant à ce que les utilisateurs partagent plus de données qu'ils ne l'auraient fait consciemment (par ex., *« Privacy Zuckering »*, *« Emotional Stirring »*), ceux visant à créer de la confusion chez les utilisateurs quant à l'utilisation de leurs données ou leurs droits (par ex., *« Privacy Maze »*, *« Information Overload »*, *« Trick Questions »*) ;

25. *DSA, art. 23.*
26. À noter que les Lignes directrices de la commission sur l'interprétation de cette directive publiées en décembre 2021 mentionnent expressément les *dark patterns*.

● Le projet de Lignes directrices du CEPD relatif aux *dark patterns* sur les réseaux sociaux [27], dont la version finale devrait être publiée début 2023, précise que les dispositions suivantes du RGPD interdisent les *dark patterns* :

- bien entendu l'article 5 (1), qui impose la loyauté du traitement, l'article 5 (1), a, c et 5 (2), qui impose transparence, minimisation de la collecte et responsabilité ;

- l'article 4 (11), qui impose un consentement libre, éclairé, spécifique et univoque ;

- l'article 12, qui impose que l'information sur la base de laquelle est recueilli le consentement soit *« concise, transparente, intelligible et facilement accessible, en utilisant un langage clair et simple »*. Le CEPD affirme clairement que les *« murs de texte »* c'est-à-dire les politiques de protection des données longues, jargonneuses, inintelligibles et totalement inadaptées à un usage digital constituent un *dark pattern* ;

- et fondamentalement l'article 25, qui impose la privacy by design et par défaut,

● La directive e-Privacy 2002/58/EC, dont l'article 5 (3) s'oppose en particulier aux *dark patterns* consistant à créer un bouton *« j'accepte »* bien plus engageant et accessible que le bouton *« je refuse »* ou *« je paramètre »*, ou encore aux *dark patterns* consistant à créer de la confusion entre le texte et le bouton associé.

c) En droit sectoriel

● La directive e-commerce 2000/31/EC, qui impose que l'information commerciale soit facilement accessible et présentée de façon claire et non ambiguë : elle s'oppose notamment aux *dark patterns « hidden information »* (information cachée) ;

● La directive sur les services audiovisuels et media 2010/13/EU, telle qu'amendée par la directive 2018/1808, qui impose notamment que toute publicité soit clairement reconnaissable en tant que telle et interdit l'utilisation de techniques subliminales : elle s'oppose notamment aux *dark patterns « disguised ads »* (publicité déguisée) ;

d) En droit de la concurrence

Certains *dark patterns* pourraient être qualifiés d'abus de position dominante [28]. . Par exemple, la Commission européenne a condamné Google pour abus de domination au travers de son moteur de recherche, pour avoir positionné son propre service de comparateur d'achat d'une manière qui le favorise [29]. Cette pratique constitue une combinaison des *dark patterns « Faire obstacle à la comparaison », « Favoriser »* et *« Défauts »*. Si les conditions d'abus sont par ailleurs remplies, ces pratiques pourraient donc être abusives, sanctionnables jusqu'à 10 % du chiffre d'affaires mondial des entreprises dominantes.

19 - **Aux États-Unis**, la section 5 du FTC Act interdit les *« comportements ou pratiques déloyales ou trompeuses affectant le commerce »*. En septembre 2020, la FTC a poursuivi la société Age of Learning, spécialisée dans l'éducation des enfants, pour pratiques trompeuses en matière d'abonnement [30].

B. - Les textes qui prohibent expressément les *dark patterns* : une tendance forte à travers le monde et un maillage qui se resserre

20 - Au sein de l'Union européenne, on l'a vu, l'article 25 (1) du DSA interdit désormais expressément les *dark patterns*. Le DSA doit entrer en vigueur au plus tard en 2024. La plupart des textes majeurs récents, adoptés ou en cours d'adoption interdisent également les *dark patterns*, dans leurs champs respectifs. Ainsi, le *Digital Markets Act* prévoit une disposition *« anti-contournement »* des principales interdictions imposées aux *« controleurs d'accès »* (*gatekeepers*, en pratique les GAFAM), notamment au travers du *« design d'interface »* [31].

21 - Le projet de règlement en matière d'intelligence artificielle [32] interdit aussi les dark patterns, en tant que pratiques d'intelligence artificielle contraires aux valeurs de l'Union [33]. Les pratiques en matière d'intelligence artificielle suivantes sont interdites :

● (a) La mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des **techniques subliminales** au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers ;

● (b) La mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui **exploite les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental** d'un groupe de personnes donné pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers.

22 - En France, la loi n° 2022-1158 du 16 août 2022, dite *« loi pouvoir d'achat »* [34], prévoit qu'à partir de 2023, tous les consommateurs ayant souscrit un contrat en ligne doivent pouvoir le résilier également sur internet, en *« 3 clics »*. Sans citer expressément les *dark patterns*, il s'agit bien de lutter contre les interfaces rendant plus difficiles la résiliation que la souscription.

Concrètement, un bouton *« Résiliation »* doit être prévu sur l'interface du client et la mise en place de la résiliation du contrat doit être opérationnelle immédiatement ou en 2 autres clics de souris maximum.

23 - Aux États-Unis, après avoir organisé un atelier sur les *dark patterns* en avril 2021 [35], la FTC a publié en octobre 2021 une déclaration de mise en œuvre de sa politique [36] spécifiquement sur les *dark patterns*. La FTC indique clairement qu'elle renforcera ses actions contre les *dark patterns* qui poussent les consommateurs à souscrire à un abonnement, ou les piègent lorsqu'ils tentent de résilier (*« trick or trap dark patterns »*). Les entreprises américaines s'exposent à des sanctions si elles ne fournissent pas des informations *« claires, en amont, lorsqu'elles obtiennent le consentement des consommateurs lors de la souscription »* et si elles ne rendent pas la résiliation facile.

24 - Dans cette lignée, le 15 septembre 2022, a été publié un rapport sur les *dark patterns « Bringing Dark Patterns to light »* [37], dans lequel la FTC identifie en particulier 4 catégories de dark

27. *Comité européen de protection des données, avr. 2022, Lignes directrices 3/2022 sur les dark patterns sur les réseaux sociaux, https://edpb.europa.eu/our-worktools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.*
28. *TFUE, art. 102.*
29. *Commission européenne, aff. AT 39740, Google Search (Shopping) [2017] 213 : « By positioning and displaying more favourably, in Google Inc.'s general search results pages, Google Inc.'s own comparison shopping service compared to competing comparison shopping services, the undertaking consisting of Google Inc. and also, since 2 October 2015, of Alphabet Inc. has infringed Article 102 of the Treaty and Article 54 of the Agreement on the European Economic Area ».*
30. *Le commissaire de la FTC de l'époque, Rohit Chopra, a affirmé dans un communiqué que « La tromperie en ligne ne peut pas être un business model viable aux Etas-Unis. [...] La FTC doit déployer des outils pour lutter contre les grandes entreprises qui gagnent des millions voire des milliards en piégeant les utilisateurs au travers de dark patterns. », www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.*
31. *DMA, art. 4.*
32. *Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle : Doc. COM (2021) 206 final, 21 avr. 2021.*
33. *Proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, art. 5 (a) et 5 (b).*
34. *L. n° 2022-1158, 16 août 2022, portant mesures d'urgence pour la protection du pouvoir d'achat..*
35. *Bringing Dark Patterns to Light : an FTC workshop, 29 avr. 2021, www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.*
36. *FTC, Enforcement Policy Statement Regarding Negative Option Marketing, 28 oct. 2021, www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf.*
37. *www.ftc.gov/system/files/ftc_gov/pdf/P214800 % 20Dark % 20Patterns % 20Report % 209.14.2022 % 20 – % 20FINAL. pdf.*

patterns répandus et problématiques, et annonce des actions judiciaires ciblées :

- tromperie des consommateurs et publicité déguisée ;
- rendre la résiliation difficile ;
- enterrer des termes clés (sous des couches de jargon) et des coûts cachés ;
- piéger les consommateurs pour qu'ils fournissent plus de données personnelles.

25 - Au niveau des États, la Californie [38], le Colorado [39] et le Connecticut [40] interdisent expressément les *dark patterns* pour obtenir le consentement des consommateurs au traitement de leurs données personnelles.

Conclusion

26 - Plusieurs études récentes démontrent le caractère endémique des *dark patterns* dans le monde – 97 % des sites e-commerce préférés des consommateurs en contiennent au moins un – avec des risques substantiels pour les utilisateurs : pertes financières, altération de l'autonomie et de la vie privée, charges cognitives, et dans certains cas altération de la santé mentale (addictions...), outre des risques d'altération de la concurrence, diminution de la transparence des prix et in fine perte de confiance dans les marchés.

Les *dark patterns* qui ne sont pas déjà couverts par la directive pratiques déloyales ou le RGPD, seront interdits par le DSA, qui permettra des sanctions jusqu'à 6 % du chiffre d'affaires mondial, au-delà des sanctions prévues par le RGPD. Et le droit de la concurrence demeure bien sur pleinement applicable, en particulier l'interdiction des abus de position dominante.

On le voit, la régulation des *dark patterns* suppose de conjuguer de nombreux domaines du droit pour appréhender toutes les facettes de ces interfaces-pièges. Au-delà des compétences juridiques, la nature des problèmes soulevés par les *dark patterns* suppose une réelle pluridisciplinarité dans leur résolution.

Les juristes doivent désormais être capables de collaborer avec des designers pour mieux comprendre la fabrique des interfaces en cause et surtout contribuer à leur remédiation, mais aussi avec des experts en neurosciences, pour mieux comprendre les mécanismes qui sous-tendent les *dark patterns*.

Les régulateurs et les législateurs, pour leur part, doivent mieux intégrer les limites cognitives des citoyens et finalement la dimension humaine, s'ils souhaitent que leurs lois et règlements soient réellement efficaces face à des mécanismes sournois par nature. Cela plaide pour une approche du droit centrée sur l'humain, de la fabrique de la loi à son application et à la forme donnée à la loi.■

Mots-Clés : Nouvelles technologies - Internet - Protection des consommateurs - Interfaces manipulatrices ou trompeuses ou Dark Patterns

Droit de la concurrence - Abus de position dominante - Deceptive patterns - Protection des données personnelles

38. En Californie, le California Privacy Rights Act qui entrera en vigueur en 2023 fournit la 1re définition des *dark patterns* en droit américain : *« A user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation »*. On relève d'ailleurs que cette définition ne s'intéresse pas à l'intention des concepteurs d'interfaces, mais seulement à leurs effets. Le CPRA interdit expressément d'obtenir le consentement au traitement de données personnelles au travers d'un *dark pattern* : le consentement ne peut pas être forcé, ni manipulé. Le *California Consumer Privacy Act* a de son côté été amendé pour inclure une interdiction des *dark patterns* lors de l'opt-out.
39. *https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf#page = 4*
40. *www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF#page = 2*