Éthique de la gestion du consentement au traitement de données personnelles : une analyse au prisme des *dark patterns*

Robert Viseur[1]

1. Service TIC, FWEG, UMONS
17 place Warocqué, B-7000 Mons, Belgique
robert.viseur@umons.ac.be

RÉSUMÉ. Face au développement du big data et à son application aux données à caractère personnel, le législateur européen a conçu un cadre juridique protecteur : le « Règlement général de protection des données » (RGPD). Son entrée en application le 25 mai 2018 a ramené au cœur des préoccupations des acteurs de la publicité ciblée et de l'analyse de performances la question du recueil du consentement préalable à tout traitement de données à caractère personnel. En a découlé l'apparition de prestataires spécialisés dans la création d'interfaces de recueil de consentement, les Consent Management Platforms (CMP), mais aussi la multiplication des dark patterns visant à forcer l'obtention dudit consentement. Dans cette recherche exploratoire, nous utilisons une typologie de dark patterns pour classer les pratiques identifiées puis discuter, d'une part, leur légalité, d'autre part, leur éthique (du point de vue des approches utilitariste et déontologique), enfin les meilleures manières de lutter contre les dérives observées. Nous montrons en particulier l'existence d'une zone grise permettant aux professionnels de maximiser, parfois provisoirement, la quantité de données à caractère personnel collectées.

ABSTRACT. Faced with the development of big data and its application to personal data, the European legislator has provided a protective legal framework: the "General Data Protection Regulation" (GDPR). When it came into force on May 25, 2018, the issue of obtaining consent prior to any processing of personal data was at the heart of the concerns of targeted advertising, particularly programmatic advertising, and of performance analysis. This has led to the emergence of service providers specialized in the creation of consent collection interfaces, the Consent Management Platforms (CMP), but also to the multiplication of dark patterns aiming at forcing the obtaining of such consent. In this exploratory research, we use a typology of dark patterns to classify the identified practices and then discuss, on the one hand, their legality, on the other hand, their ethics (from the point of view of utilitarian and deontological approaches), and finally, the best ways to fight against the observed drifts. In particular, we show the existence of a grey area allowing professionals to maximize, sometimes temporarily, the amount of personal data collected.

Mots-clés : vie privée, éthique, cookie, dark pattern, RGPD, CMP.

KEYWORDS: privacy, ethics, cookie, dark pattern, DGPR, CMP

1. Introduction

Avec une capitalisation boursière cumulée de l'ordre de dix mille milliards de dollars, les GAFAM sont en vingt cinq ans devenus incontournables dans le paysage économique. Au cœur de leurs modèles d'affaires : la collecte massive (*big data*) de données à caractère personnel permettant le ciblage de la publicité (Facebook, Google, Microsoft), le classement personnalisé d'informations (Facebook, Google, Microsoft) et la suggestion de recommandations d'achats (Amazon). Cette évolution a amené le législateur européen à proposer, avec le « *Règlement général de protection des données* » (RGPD), un cadre harmonisé de protection des données à caractère personnel pour le citoyen européen.

Le RGPD impacte les GAFAM mais d'une manière générale toute entreprise ou association recueillant des données à caractère personnel, et ce quel qu'en soit le volume. Sont notamment impactés la myriade d'acteurs impliqués dans les dispositifs de publicité ciblée, en particulier dans celui, fragmenté, de la publicité programmatique (Allary & Balusseau, 2018), mais aussi les entreprises ayant mis en œuvre des modèles d'affaires basés sur l'accès gratuit à des contenus en ligne, dès lors valorisés par la publicité en ligne et la revente de données. Face à la complexité d'obtention du consentement et au risque accru de refus de la part des utilisateurs, les éditeurs de sites web recourent, d'une part, aux services d'acteurs spécialisés dans la création d'interfaces de recueil du consentement (Hils et al., 2020), soit des CMP (*Consent Management Platforms*), d'autre part, à la mise en œuvre de *dark patterns* visant à « extorquer » le consentement à l'aide d'artifices techniques et visuels à la légalité et à l'éthique discutables (Nouwens et al., 2020). Cette recherche exploratoire propose dès lors une analyse de ces *dark patterns* appliqués aux interfaces de recueil de consentement (CMP) et aux conditions d'utilisation des services (CGU) fixant les finalités de la collecte de données.

Notre article est organisé en quatre sections. Dans une première section, nous proposons un état de l'art sur la publicité ciblée, la collecte de données, le *tracking*, le RGPD et le concept de *dark pattern*. Dans une seconde section, nous présentons succinctement notre méthodologie. Dans une troisième section, nous analysons les techniques trompeuses appliquées au recueil de consentement, les classons en utilisant une typologie de *dark patterns* puis évaluons leurs caractères légal et éthique. Dans une quatrième section, et avant de conclure, nous discutons l'impact de ces *dark patterns* sur le caractère libre et éclairé du consentement fourni et proposons plusieurs pistes d'action en matière de régulation permettant de davantage respecter la vie privée des utilisateurs de services en ligne.

2. État de l'art

Mesguish et Thomas (2013) distinguent quatre âges du Web. Le premier, s'étendant de 1994 à 1996, est baptisé « *Web des pionniers* ». Cette expression désigne le développement d'un Web encore réduit en taille alimenté par des pionniers technophiles. De 1996 à 2004, le « *Web des documents* » s'accompagne d'une explosion du nombre de sites permise par la facilité des nouveaux outils d'édition de contenu et alimentée par les débuts du commerce électronique. Le « *Web social* », parfois appelé Web 2.0, s'étend de 2004 à 2010. Il voit une implication plus importante des utilisateurs dans la création et l'enrichissement des

contenus. Dès 2010, le « *Web temps réel* » se développe avec la part croissante des réseaux sociaux (audience) ainsi que le développement des *smartphones* et des tablettes. Enfin, l'essor des objets connectés annonce un cinquième âge du web, que nous baptiserons « *Web ubiquitaire* » permettant la création d'un double numérique sous la forme d'un profil et ouvrant de nouvelles perspectives en termes de services individualisés. Cette extraction continue de données personnelles conduit à la mise en place d'un « *capitalisme de surveillance* » (Zuboff, 2019) couvrant à la fois les mondes virtuels (p. ex. moteurs de recherche) et réels (p. ex. objets connectés).

Cette évolution s'est accompagnée d'une mutation de la publicité en ligne sous des formes de plus en plus ciblées (Peyrat, 2009), jusqu'à la publicité comportementale cherchant à coller au plus près des centres d'intérêt immédiats des consommateurs tels que révélés par leur historique de navigation. Cette personnalisation avancée suppose un travail permanent de *tracking* (p. ex. *cookies*) et d'analyse de données (profilage) par les régies publicitaires. Les plus connues sont Google et Facebook mais d'autres acteurs plus petits sont notamment actifs en publicité programmatique (Allary & Balusseau, 2018). Cette dernière organise, au travers de plates-formes dédiées, la rencontre en quasi temps réel des offres d'espaces publicitaires mis aux enchères par des éditeurs de sites web, et les demandes émises par les annonceurs à la recherche d'une clientèle spécifique. L'objectif est dès lors de coller aux plus près des préoccupations (commerciales) des internautes de manière à maximiser les conversions (p. ex. achat d'un produit) et la rentabilité des campagnes publicitaires.

La collecte de données personnelles à partir du navigateur va s'appuyer sur des traceurs variés incluant les *cookies* mais aussi des empreintes (*fingerprinting*) calculées sur base des caractéristiques du navigateur et de la machine sur laquelle il est installé (Viseur, 2021). Ces identifiants peuvent donc être déterministes (p. ex. *login* et *cookies*) ou probabilistes (p. ex. *fingerprinting* et adresse IP) c'est-à-dire utilisables par croisement de plusieurs données. Les entreprises vont par ailleurs combiner des données propres (*first party data*), notamment issues de leur logiciel CRM (*Customer Relationship Management*) et du Web (p. ex. site web et réseaux sociaux), des données issues de partenaires (*second party data*) et des données achetées auprès de tiers tels que les courtiers en données (*third party data*). Le croisement de ces données accroît les possibilités d'association à un profil. Aux États-Unis, le triplet composé du genre, de la date de naissance et du code postal permet ainsi la ré-identification dans 87 % des cas (Sweeney, 2000). D'autres données, telles que l'historique des requêtes dans les moteurs de recherche ou les données de géolocalisation, se prêtent également à la ré-identification (Narayanan et al., 2016).

Dans un monde où le coût de l'accès à l'information tend vers zéro, l'objet rare n'est plus l'information mais bien l'attention. Le concept d'économie de l'attention a fait l'objet d'un effort de théorisation de la part d'Emmanuel Kessous (2012). Ce dernier décrit la transition d'un marketing de segmentation vers un marketing des traces renforçant l'emprise des offreurs sur les consommateurs en l'absence d'un contrôle fort des données à caractère personnel par les individus. Ce constat d'asymétrie des forces entre les entreprises du numérique, en particulier les GAFAM, et les utilisateurs de services numériques a motivé l'Union européenne à accroître la protection des citoyens européens grâce au « *Règlement général de protection des données* » (RGPD), publié le 27 avril 2016, d'application depuis le 25 mai 2018 (Banck, 2018). Le RGPD définit le concept de « *donnée à caractère*

personnel » comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale », ce qui recouvre à la fois les identifiants déterministes et les identifiants probabilistes. Le RGPD est « *neutre sur le plan technologique* », ce qui signifie notamment qu'il s'applique à tout type de traceur.

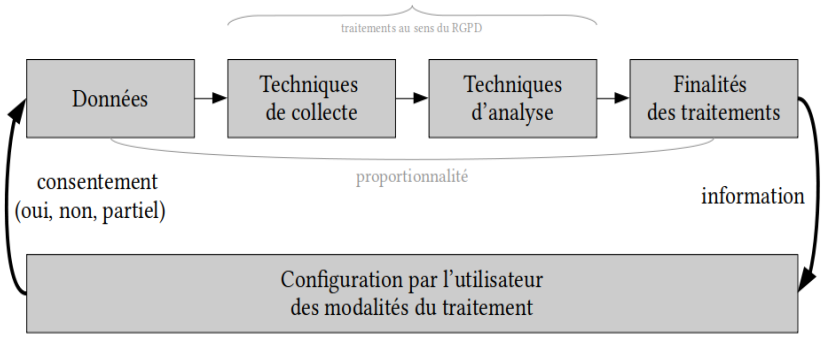

Figure 1. Fonctionnement du RGPD.

Le RGPD définit le concept de « *traitement* » de manière large comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* » (cf. Figure 1). Le RGPD exige que le consentement, libre et éclairé, se manifeste par un acte positif de la part de l'utilisateur. Il impose par ailleurs que les données collectées soient cohérentes au regard des finalités annoncées (principe de proportionnalité). Sur cette base, l'utilisateur peut refuser ou accepter, en tout ou partie, les collectes sollicitées. Les violations à ce règlement sont instruites par des agences nationales de protection de données telles que la CNIL en France.

La question du recueil du consentement est cruciale pour les entreprises actives dans la publicité ciblée et dans l'analyse de performances dès lors qu'elles recourent à des données qui ne sont pas anonymisées. En effet, si l'on s'en tient aux *cookies*, ces derniers se révèlent utiles, voire nécessaires, pour identifier un utilisateur (au travers de son navigateur), ce qui permet, premièrement, de limiter son exposition à une campagne de publicité (principe du *capping*), deuxièmement, de cibler les publicités qui lui sont envoyées, soit par le suivi d'une session, soit par le biais de son identification puis de son rattachement à un profil, troisièmement, de dresser des statistiques de fréquentation fiables (p. ex. comptabilisation des visiteurs uniques) (Viseur, 2021). Le RGPD a donc deux conséquences pour ces entreprises. D'une

part, elles doivent se mettre en conformité avec les dispositions du règlement, d'autre part, elles sont exposées au refus de consentir au traitement des données par les utilisateurs. En ont résulté plusieurs conséquences. Premièrement, les entreprises ont dû veiller à centraliser les demandes de consentement de manière à éviter leur multiplication, dès lors réduire le risque de refus. En particulier, le secteur de la publicité programmatique est composé d'une myriade d'acteurs réconciliant leurs données par le biais de techniques comme le *cookie syncing* (Papadopoulos et al., 2019). Deuxièmement, des acteurs spécialisés sont apparus pour gérer les interfaces de recueil de consentement en proposant des outils standards : les CMP (*Consent Management Platform*) (Nouwens et al., 2020). Troisièmement, et cela pré-existait au RGPD, le recours aux *dark patterns* s'est multiplié dans les interfaces de recueil de consentement.

Tableau 1. Typologie de dark patterns (basé sur Gray et al., 2018).

Nom	**Description**
Harcèlement	Appliquer une redirection des fonctionnalités attendues qui persiste au-delà d'une ou plusieurs interactions.
Obstruction	Rendre un processus plus compliqué que nécessaire de sorte à dissuader certaines actions.
Sournoiserie	Tenter de cacher, travestir ou retarder la divulgation d'une information importante pour l'utilisateur.
Interférence d'interface	Manipuler l'interface utilisateur de manière à favoriser certaines actions au détriment d'autres actions.
Action forcée	Contraindre l'utilisateur à réaliser certaines actions pour accéder (ou continuer à accéder) à certaines fonctionnalités.

Le terme « *dark pattern* » désigne la situation où un designer utilise sa connaissance du comportement humain (p. ex. psychologie) et les désirs des utilisateurs finaux pour mettre en œuvre des fonctionnalités trompeuses qui ne sont pas dans l'intérêt de l'utilisateur (Gray et al., 2018). En ce sens, il s'inscrit dans la logique des *sludges* définis par Thaler (2018) par opposition aux *nudges* (Thaler et Sunstein, 2010) supposés, dans la logique du paternalisme libertaire, aider les citoyens à faire les meilleurs choix pour eux-mêmes sans les priver de pouvoir faire s'ils le souhaitent un choix alternatif. Gray et al. (2018) proposent une typologie de *dark patterns* (cf. Tableau 1) incluant le harcèlement (*nagging*), l'obstruction (*obstruction*), la sournoiserie (*sneaking*), l'interférence d'interface (*interface interference*) et l'action forcée (*forced action*). Les exemples fournis couvrent notamment le partage de données à l'image du *privacy zuckering* par lequel l'utilisateur est amené à partager plus d'informations que nécessaire.

3. Méthodologie

Cette analyse préliminaire des caractères légal et éthique des interfaces de recueil de consentement et des conditions générales d'utilisation précisant les données collectées ainsi que les finalités s'appuie, d'une part, sur une première sélection de cas identifiés par l'auteur, d'autre part, sur des exemples documentés par le site Pixel de tracking et le compte Twitter Pixel de Tracking qui l'accompagne. Cette

sélection a permis d'associer un ensemble de pratiques courantes à la typologie de *dark patterns* proposée par Gray et al. (2018). Au total, 34 *dark patterns* ont été identifiés et repris dans une grille d'analyse (sous LibreOffice.org Calc).

Différents outils ont été exploités pour approfondir cette analyse. D'une part, l'outil « *Outils de développement web* » de Firefox a été utilisé pour valider le *dark pattern* de sournoiserie (*sneaking*) consistant à collecter des données avant le recueil du consentement. D'autre part, un script Python, permettant d'obtenir automatiquement une capture d'écran de la page d'accueil d'une liste de sites avec l'affichage du CMP, a été développé, et testé, offrant des perspectives d'automatisation des analyses par pays ou par secteur. Ce programme a notamment été utilisé sur les sites des principaux journaux belges (dont le CMP est généralement fourni par Didomi) et français, soit un total de 32 sites web.

4. Résultats

Nous proposons dans cette section, d'une part, de catégoriser les *dark patterns* appliqués au CMP (*Consent Management Platform*) et aux CGU (Conditions Générales d'Utilisation), d'autre part, d'approfondir leur mise en œuvre par les sites Web.

4.1. Catégorisation des dark patterns

Sur base de la typologie de *dark patterns* proposée par Gray et al. (2018), nous proposons de catégoriser les *dark patterns* observés, d'une part sur les CMP, d'autre part sur les CGU. Nous utiliserons les noms francophones pour désigner ces techniques.

Tableau 2. Application de dark patterns, par type, aux CMP et CGU.

Technique	**CMP**	**CGU**
Harcèlement	Demande récurrente d'autorisation (p. ex. géolocalisation).	Validation récurrente des CGU modifiées d'un service.
Obstruction	Principe des *cookie walls* allégés (p. ex. multiplication des *sliders* sans refus global).	Page interminable centralisant les CGU de tous les services proposés par une même firme.
Sournoiserie	Collecte de données même en cas de refus. Difficulté de retrait du consentement (principe du *roach hotel*).	Texte très long[1] noyant l'information, ou écrit dans un langage volontairement cryptique.
Interférence d'interface	Cases de consentement pré-cochées. Mise en évidence du bouton pour accepter.	Masquage des clauses les plus problématiques (p. ex. utilisation des données d'un formulaire à des fins

[1] La longueur excessive des CGUs des réseaux sociaux a été mise à l'honneur par l'artiste Dima Yarovinski dans l'exposition « I agree ». La durée de lecture des CGUs d'Instagram y était ainsi évaluée à 1 heure 30 environ (cf. [url]). McDonald et Cranor (2008) ont pour leur part évalué le temps annuel de lecture des politiques de confidentialité à 244 heures.

Technique	CMP	CGU
	Moindre visibilité du bouton pour refuser. Multiplication des étapes pour refuser.	commerciales).
Action forcée	Principe des *cookie walls* (accès conditionné à l'acceptation ou au paiement). Fourniture de la date de naissance pour valider une limite d'âge (principe du *privacy zuckering*).	*na*

4.2. Analyse des dark patterns

4.2.3. Dans le cas des CMPs

Le harcèlement paraît légal puisque l'utilisateur garde la possibilité de donner ou non son consentement. Il n'est par contre pas éthique dès lors qu'il tente de l'obtenir « à l'usure » et est par ailleurs contraire aux recommandations de la CNIL (délibération n°2020-092) qui prévoient de conserver les choix « *pendant un certain laps de temps* » (recommandation : 6 mois) en fonction de la nature du site ou de l'application. L'obstruction, la sournoiserie et l'action forcée débouchent généralement sur des dispositifs à la fois contraires à l'éthique et, souvent, à la loi, par exemple au titre de l'absence de consentement (p. ex. collecte avant acceptation) ou de la non-proportionnalité des données collectées au regard des finalités (p. ex. *privacy zuckering*), si l'on s'en tient aux exemples fournis dans le Tableau 2.

Le principe, largement répandu, des *cookie walls* (p. ex. refus du site d'accéder aux contenus sans acceptation de la collecte ni paiement d'une contrepartie financière), soit un cas d'obstruction ou d'action forcée (suivant le degré de blocage), se révèle contraire à la liberté du consentement (avis du Comité européen de la protection des données) mais ne doit pas être systématiquement interdite, par exemple dès lors qu'un accès à une version minimale du contenu est offerte (décision du Conseil d'État ; cf. [url]).

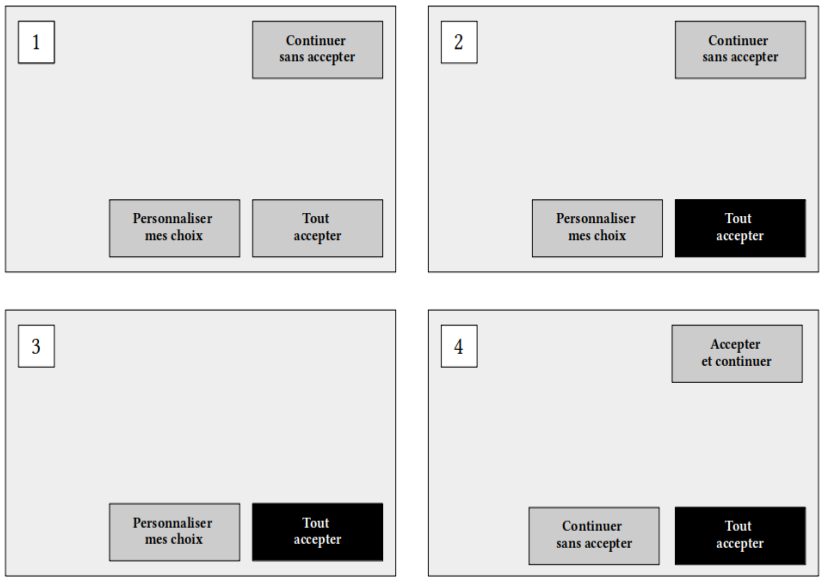

Figure 2. Dark patterns de type interférence d'interface (2, 3, 4).

Les interférences d'interface donnent lieu à une mise en œuvre plus diversifiée (cf. Figure 2). L'affichage de cases pré-cochées est clairement considéré comme illégal (cf. [url]). L'illustration n°1 représente un exemple d'interface de CMP conforme aux recommandations de la CNIL. Les illustrations n°2, 3 et 4 représentent des variations couramment observées. L'illustration n°2 consiste à mettre en évidence un choix qui arrange l'éditeur du site web car conduisant à l'acceptation de tous les traceurs. La facilité pour accepter ou refuser les traceurs est cependant équivalente. Elle s'éloigne par contre de la recommandation de la CNIL de ne pas mettre visuellement un choix davantage en évidence qu'un autre. L'illustration n°4 se révèle particulièrement vicieuse, à défaut d'être illégale, puisqu'elle inverse la position couramment utilisée pour les boutons d'acceptation totale et de refus afin d'induire en erreur l'utilisateur. Ce *dark pattern*, observé notamment sur le site du magazine Marianne, en a par la suite disparu, une conséquence possible de la bronca déclenchée sur les réseaux sociaux par cette découverte.

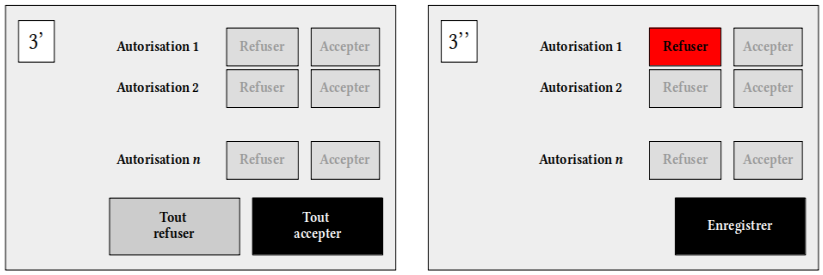

Figure 3. Dark patterns de type interférence d'interface (3', 3'').

L'illustration n°3 (cf. Figure 2) viole clairement les recommandations de la CNIL en ce sens qu'elle débouche typiquement sur l'enchaînement d'écrans illustré à la Figure 2 consistant à ne pas proposer de refus global et à multiplier les étapes pour personnaliser les choix par finalité. De plus, le consentement tend à être forcé en usant d'artifices visuels en proposant une seconde fois un bouton d'acceptation globale (cf. Figure 3 ; illustration n°3') ne disparaissant qu'à la configuration des finalités (cf. Figure 3 ; illustration n°3''). En février 2023, ce type d'interface restait par exemple majoritaire sur les sites de la presse belge (à l'exception du site de Roularta Media Group).

4.2.3. Dans le cas des CGUs

À défaut d'être clairement illégal, le harcèlement pose un problème éthique, puisqu'il tente d'obtenir un consentement « à l'usure ». Cette pratique se traduit par une modification fréquente des termes du contrat, avec une demande de validation à la clef. L'obstruction (p. ex. longueur d'un contrat) et la sournoiserie (p. ex. complexité excessive d'un contrat et morcellement entre plusieurs documents) posent ici un problème de conformité au règlement puisqu'ils touchent directement au caractère éclairé du consentement.

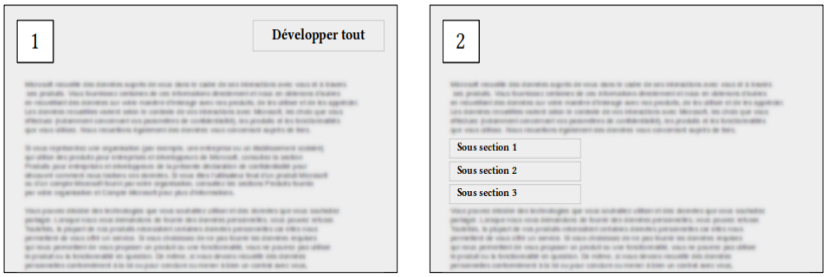

Figure 4. Dark patterns de type interférence d'interface (CGU).

Les interférences d'interface dans les CGU donnent lieu à une mise en œuvre particulièrement insidieuse (cf. Figure 4). Si la fermeture de sections spécifiques peut se justifier par des raisons de lisibilité (illustration n°2), le masquage pur et simple sans moyen simple d'identifier les sections rendues visibles dans un second temps (illustration n°1) pose clairement un problème éthique à défaut d'être une pratique illégale (car le lecteur garde la possibilité de déplier ces sections avant sa lecture… ce qu'il ne fera généralement pas dans la mesure où le lien d'affichage se révèle discret). Reste que, dans les deux cas, ces artifices sont généralement un moyen de masquer des clauses problématiques (p. ex. réutilisation des données encodées à des fins marketing dans un outil de formulaires en ligne).

5. Discussion

Nous discuterons dans cette section de l'éthique des *dark patterns*, de la dépendance à la publicité ciblée, de la régulation des pratiques ainsi que des limitations et des perspectives.

5.1. Éthique des dark patterns

Trois types de pratiques pourraient être distinguées : des pratiques clairement légales, des pratiques clairement illégales (p. ex. sournoiserie) et des pratiques légales mais peu ou prou éthiques, dont certaines en sursis (p. ex. harcèlement) du fait des évolutions de la jurisprudence et des publications des APDs (Autorités de Protection des Données), soit des lignes directrices, soit des recommandations.

Certaines pratiques comme le harcèlement (p. ex. demande répétée de consentement) et l'obstruction (p. ex. *cookie walls*) se révèlent menacées, en particulier suite à la publication de recommandations par la CNIL (cf. délibération n°2020-092 du 17 septembre 2020). Ainsi le harcèlement est explicitement ciblé par la CNIL : « *De manière générale, la Commission recommande que le choix exprimé par les utilisateurs, qu'il s'agisse d'un consentement ou d'un refus, soit enregistré de manière à ne pas les solliciter à nouveau pendant un certain laps de temps* » (Délibération n° 2020-092 du 17 septembre 2020). Idem pour la sournoiserie sous la forme d'une entrave au retrait de consentement : « *Les utilisateurs ayant donné leur consentement à l'utilisation de traceurs doivent être en mesure de le retirer à tout moment. La Commission rappelle qu'il doit être aussi simple de retirer son consentement que de le donner* » (Délibération n° 2020-092 du 17 septembre 2020).

La légalité du principe des *cookie walls* au sens strict semble également en sursis et, dans l'attente d'une clarification (p. ex. futur règlement *eprivacy*) et d'une homogénéisation des décisions, se juge au cas pas cas. Au niveau européen : « *L'EDPB a constaté la nécessité de nouvelles précisions, en particulier en ce qui concerne la validité du consentement fourni par la personne concernée lorsqu'elle interagit avec un « accès subordonné à l'acceptation de cookies» ou « cookie walls »* » (cf. [url]. Au niveau français : « *Par la décision du 19 juin 2020, le Conseil d'État a jugé que l'exigence d'un consentement « libre » ne pouvait toutefois pas justifier une interdiction générale de la pratique des « murs de traceurs » : la liberté du consentement des personnes doit être appréciée au cas par cas, en tenant compte notamment de l'existence d'alternative réelle et satisfaisante proposée en cas de refus des cookies* » (cf. [url]). Au niveau belge : « *Ne conditionnez pas la fourniture de vos produits ou services (même gratuits) à l'acceptation du traitement de données à caractère personnel non-nécessaires à la prestation du service ou à la fourniture du produit. N'essayez pas de forcer ou d'inciter, de quelque manière que ce soit, les personnes concernées, à vous fournir leur consentement à ces traitements* » (cf. [url], page 61).

Les pratiques observées évoluent parfois rapidement au gré des recadrages des autorités ou des dénonciations sur les réseaux sociaux. Certains médias (p. ex. Le Monde, Le Figaro et L'Équipe) ont ainsi persévéré dans l'utilisation du *cookie wall*. D'autres se sont adaptés (p. ex. Libération et 20 Minutes) : après avoir sollicité le paiement d'un abonnement, ces sites de journaux français permettent ensuite de consulter leur site avec un bandeau de rappel en bas de page, soit une succession de deux *dark patterns* (obstruction puis harcèlement). Cette modalité est (peut-être) elle-même en sursis : « *De plus, la Commission recommande que, lorsque le refus peut être manifesté par la poursuite de la navigation, le message sollicitant le consentement (par exemple, la fenêtre ou le bandeau) disparaisse au bout d'un laps de temps court, de manière à ne pas gêner l'utilisation du site ou de l'application et à ne pas, ainsi, conditionner le confort de navigation de l'utilisateur à l'expression de son consentement au traceur* » (cf. [url], page 10). Reste que la CNIL a très

récemment adouci sa position en prenant en compte, d'une part, la nécessité d'« *une juste rémunération* », par exemple via la publicité ou via un abonnement, et, d'autre part, l'acceptabilité du « *cookie wall* » dès lors qu'il existe « *une alternative réelle et équitable* » et qu'il est limité aux finalités permettant cette juste rémunération (cf. [url]). Signalons également, par exemple chez L'Équipe et Le Monde, la présence d'un *sludge* sous la forme d'une réduction sur le prix de l'abonnement en cas de connexion via un compte Google.

L'éthique dans le contexte du marketing se réfère à un ensemble de principes et de normes morales qui régissent les pratiques commerciales et publicitaires. Nantel et Weeks (1996) distinguent deux approches de l'éthique en marketing. La première, la plus ancienne, est utilitariste et se concentre sur la satisfaction du client. La seconde, plus récente, privilégie la déontologie. Sont dès lors mis en avant, par exemple, au sein de codes d'éthiques, le respect de l'esprit et de la lettre des législations, une présentation honnête des caractéristiques des produits vendus ainsi que le bannissement de toute pratique de vente et de publicité tendancieuse ou trompeuse. Si l'on se place sur un plan purement utilitariste, certaines pratiques d'obstruction ou d'action forcée peuvent se justifier dès lors qu'elles tendent à préserver un accès équitable à des services en ligne (satisfaction du client) ; sur un plan déontologique, par contre, ces pratiques ne respectent pas l'esprit porté par le RGPD. Quelle que soit l'approche éthique retenue, les *dark patterns* de harcèlement ou de sournoiserie paraissent difficilement justifiables tout en étant de plus en plus critiqués sur un plan légal. Quant aux interférences d'interface, leur éthique est contestable mais leur condamnation paraît parfois difficile même si certaines d'entre elles s'apparentent à la sournoiserie (p. ex. dissimulation de texte au sein des CGUs).

Tableau 3. Caractère éthique ou légal des dark patterns appliqués aux CMPs ou aux CGUs.

Technique	**Éthique**	**Légalité**
Harcèlement	Non car tentative de forcer le consentement « à l'usure ».	Oui mais en sursis du côté des APDs (cf. recommandations).
Obstruction	Non (déontologie) car volonté d'épuiser l'utilisateur mais discutable (utilitarisme) dès lors qu'elle concerne l'obtention d'une juste rémunération.	Non car condamné (p. ex. absence de bouton pour tout refuser) sauf pour les *cookies walls* (en discussion) ; oui pour les CGUs (p. ex. longueur).
Sournoiserie	Non car volonté d'obtenir le consentement en trompant l'utilisateur.	Non pour la sournoiserie appliquée aux CMPs mais oui pour de nombreuses techniques appliquées aux CGUs (p. ex. longueur et complexité).
Interférence d'interface	Non car généralement révélatrice d'une volonté de piéger l'utilisateur, en particulier quand le *dark pattern* tend vers la sournoiserie (cf. Figure 3 /4 par exemple).	Non pour un large ensemble de techniques (p. ex. cases pré-cochées et multiplication des étapes pour refuser) mais oui pour certaines techniques plus insidieuses (p. ex. déplacement de boutons standards).
Action forcée	Idem que l'obstruction.	Non observé.

Cette zone grise, composée de dispositifs en pratique tolérés (cf. Tableau 3), permet aux entreprises (p. ex. régies publicitaires) de « jouer la montre » sur base d'un calcul bénéfice-risque (probabilité et gravité d'une sanction). Si l'on assiste à un assainissement des pratiques, des dispositifs illégaux persistent cependant (p. ex. sournoiserie : collecter des données à caractère personnel sans avoir le consentement explicite des usagers). Par ailleurs, des dispositifs peu ou prou éthiques existent. Ils sont, soit en sursis (p. ex. harcèlement : demandes répétées de consentement), soit difficiles à réguler sauf à imposer des modèles d'interfaces (p. ex. interférences visuelles), soit tolérés par les APDs (sous conditions) (p. ex. obstruction : consentir ou payer).

5.2. Régulation des pratiques

Les producteurs de contenus en ligne sont aujourd'hui largement dépendants des revenus issus de la publicité, en particulier de la publicité ciblée. C'est par exemple le cas des nouveaux médias émergents sur des plates-formes telles que Youtube (Cauche, 2019). En résulte une dépendance aux GAFAM, et en particulier à Google, qui dominent le marché de la publicité en ligne (avec une part de marché cumulée sur le marché français d'environ 75 % ; Viseur, 2021). Certes, il existe des modes de rémunération alternatifs : les abonnements ou les dons récurrents (Bessière et al., 2017) par exemple. Cependant, ils semblent rester insuffisants pour remplacer totalement les revenus issus de la publicité. Les systèmes de *paywalls* se révèlent ainsi incapables de stimuler significativement les revenus de la presse (Myllylahti, 2014). Les médias recourent en outre à des *widgets* valorisés par la collecte de données (p. ex. AddThis ; Viseur, 2021) et incluent, sans doute par facilité, des objets également avides de données (p. ex. vidéos Youtube).

Cette dépendance aux données à caractère personnel, directe pour les régies publicitaires, indirecte pour les producteurs de contenus, eux-mêmes dépendants des régies publicitaires, explique l'échec des mécanismes d'*opt-in* comme le champs d'en-tête HTTP DNT *Do Not Track* (cf. [url1] et [url2] pour plus d'informations). Sont dès lors difficiles à mettre en œuvre en l'état des mécanismes de traitement automatisé des demandes de consentement (sur base d'un format structuré et de profils utilisateurs standards) par les navigateurs comme évoqué par Nouwens et al. (2020). Face à cette situation, des entreprises comme Apple se sont positionnées, avec une certaine crédibilité, comme défenseurs de la vie privée de leurs clients, en mettant en œuvre un mécanisme de filtrage de *cookies tiers* (ITP) dont le principe s'est ensuite étendu à Firefox (Viseur, 2021).

Découlent donc de cette dépendance des pratiques, parfois agressives, souvent légales mais à l'éthique discutable (*sludge*), pour obtenir le consentement au traitement de données personnelles. La complexité inhérente à l'octroi d'un consentement libre et éclairé s'oppose à l'idéal de gestion individuelle (Kröger et al., 2021). Les appels répétitifs et parfois vicieux (*dark patterns*) conduisent à la résignation de nombreux utilisateurs, ce que Solove (2020) a théorisé sous l'expression « *mythe du paradoxe de la vie privée* ». Le concept de « *privacy paradox* », c'est-à-dire le décalage entre l'intention et le comportement de divulgation de données à caractère personnel, a été introduit par Norberg et al. (2007). Si Waldman (2020) l'explique notamment par la rationalité limitée des consommateurs, Solove (2020) y voit au contraire un comportement rationnel. Si les utilisateurs valorisent leur vie privée mais agissent au contraire de leurs intérêts, ce

n'est pas la démonstration d'une faible valeur accordée, en réalité, à la vie privée mais bien un comportement rationnel de résignation face à l'arsenal de techniques insidieuses mises en œuvres pour extorquer leur consentement, soit un constat de faible contrôlabilité de ces dispositifs malgré le mécanisme légal de consentement.

Dans ce contexte, les associations et les collectifs ont un rôle qui devrait être mis en valeur. Premièrement, ils permettent la mise en évidence et l'objectivisation de comportements contre lesquels des logiciels ou des réglementations devraient pouvoir lutter. Ce sont par exemple Open Terms Archive, pour la traçabilité des modifications de CGU, TOS;DR pour leur évaluation sur une échelle standardisée, Data Experience d'Hestia Labs, pour la mise en évidence des critères de profilage, ou encore l'extension Privacy Badger, de l'EFF, pour le filtrage des traceurs. Deuxièmement, ils peuvent agir publiquement en dénonçant les comportements contraires à l'éthique, en exploitant la volonté des entreprises de conserver leur réputation en ligne. Troisièmement, ils agissent comme des intermédiaires entre les utilisateurs et les APD nationales pour construire les dossiers visant à lutter contre les infractions au RGPD (p. ex. La Quadrature du Net en France et la coupole européenne EDRi). Quatrièmement, ils pourraient, à la manière de la FSF pour les licences logicielles ou de la Creative Commons pour la culture libre, contribuer à la construction de contrats standardisés (Wylie, 2019), stables et compréhensibles, permettant dès lors l'octroi d'un consentement réellement éclairé.

Enfin, la complexité supplémentaire amenée par le RGPD a conduit à l'émergence de prestataires spécialisés dans la mise en œuvre de *Consent Management Platforms* (CMP). Ces entreprises sont par exemple : Axeptio, ConsentManager, Cookiebot, Didomi, SFBX et Sirdata. Cette concentration accrue des interfaces de recueil de consentement entre les mains de quelques prestataires offre donc aux APDs un moyen d'action sur des acteurs ayant un impact significatif sur les pratiques auxquelles sont confrontés les utilisateurs.

Tableau 4. Protection des utilisateurs contre la collecte abusive de données.

	Avant	**Actuellement**	**Futur possible**
Macro	Lois nationales (*privacy*).	RGPD (EU). APDs.	Cadre juridique mondial émergent (RGPD, CCPA…). APDs (renforcement).
Meso	Modèle publicitaire dominant.	Développement d'une niche *pro-privacy*.	Régulation des GAFAM et des prestataires CMP. Soutien aux initiatives de standardisation et de labellisation (p. ex. D-Seal). Relais via des associations professionnelles (p. ex. IAB) . Soutien aux associations *pro-privacy*.
Micro	Technologies anti-*tracking* (anonymisation, extensions…).	Technologies anti-*tracking* (anonymisation, extensions…). Consentement libre et éclairé.	Technologies anti-*tracking* (anonymisation, extensions…). Consentement libre et éclairé.

En pratique, s'appuyer sur le consentement libre et éclairé ne permet pas une protection optimale des utilisateurs face à la collecte abusive de données (cf. Tableau 4). En effet, le respect du RGPD s'accompagne de *dark patterns* légaux à défaut d'être éthiques. La recherche d'un impact maximal sur les pratiques de terrain peut dès lors passer par la régulation des acteurs conditionnant les pratiques d'un grand nombre d'acteurs (p. ex. GAFAM et CMP) ainsi que par le relais négocié via les associations professionnelles (p. ex. IAB ; car recommandations aux professionnels via le TCF : *Transparency & Consent Framework*). Davantage de visibilité pourrait également être accordée aux initiatives de standardisation et de labellisation (p. ex. D-Seal) (Schade, 2023). De plus, les collectifs et associations *pro-privacy* se révèlent des soutiens utiles pour les APD en aidant à la construction des dossiers en violation du RGPD.

5.3. Limitations et perspectives

Cette recherche exploratoire présente trois perspectives principales. Premièrement, la problématique des *dark patterns* a fait l'objet d'une analyse approfondie par l'EDPB (*European Data Protection Board*) dans un document, postérieur à cette recherche, daté du 14 mars 2022 (EDPB, 2022). Les *dark patterns* y sont assimilés à « *des interfaces et des expériences utilisateurs qui amènent les utilisateurs à prendre des décisions, involontaires et potentiellement préjudiciables, concernant le traitement de leurs données personnelles* » (page 2). Les catégories proposées diffèrent de Gray et al. (2018) et se concentrent davantage sur les interférences graphiques. Les catégories proposées sont la surcharge (comparable au harcèlement) ; l'omission, la confusion et la dissimulation (assimilables à des formes d'interférence d'interface) ; et enfin l'entrave (recouvrant la sournoiserie et l'action forcée). Cette classification devra probablement être prise comme référence et être suivie de clarifications de la part de l'EDPB ainsi que des autorités nationales. L'adaptation de cette recherche à la typologie européenne se révélera dès lors sans doute indispensable. Deuxièmement, et compte tenu de la rapidité de l'évolution du design des CMPs, notamment suite à leurs adaptations au contexte réglementaire, il serait intéressant de sauvegarder ces interfaces sur une base périodique à l'aide d'un robot (Python). De la sorte, il serait possible de déterminer leur positionnement (conformité plus ou moins importante à l'esprit du règlement), d'analyser leur évolution en relation avec les règlements, jurisprudences, lignes directrices et recommandations publiés au fil du temps ainsi que les actions de la société civile pour en dénoncer les pratiques. Troisièmement, l'utilisation d'outils d'*eye tracking*, couplée à des entretiens semi-directifs, permettrait de mieux comprendre la réaction des utilisateurs face à ces *dark patterns*, pour ensuite en évaluer l'efficacité et émettre des recommandations quant aux contre-mesures appropriées.

6. Conclusion

Dans cette recherche exploratoire, nous avons présenté l'évolution du marketing en ligne vers une approche plus ciblée occasionnant une collecte massive de données personnelles. Nous avons ensuite montré comment la question du recueil du consentement, cruciale pour les régies publicitaires et les courtiers en données (donc aussi pour la presse en ligne), avait motivé l'utilisation de *dark patterns* pour « extorquer » le consentement des utilisateurs. Sur base d'une typologie de *dark patterns*, nous avons alors analysé, sur un ensemble de CMPs et de CGUs, comment

ces *dark patterns* s'appliquaient concrètement au recueil de consentement. Cette analyse nous a permis de discuter les limites actuelles du RGPD, coexistant avec des dispositifs visant à forcer le recueil du consentement (*sludge*). Nous avons donc discuté leurs caractères légal et éthique (du point de vue utilitariste et déontologique). Cela nous a permis de montrer l'existence d'une zone grise exploitée lucrativement par les professionnels. Les moyens d'actions disponibles pour pallier ces limitations ont enfin été développés.

7. Références

Allary J., & Balusseau V. (2018). La publicité à l'heure de la data. Adtech et programmatique expliqués par des experts, Dunod.

Banck A. (2018). RGPD : la protection des données à caractère personnel, Gualino.

Bessière, V., & Stéphany, É. (2017). Le crowdfunding: fondements et pratiques. De Boeck Supérieur.

Cauche, R. (2019). Professionnalisation des modes de diffusion sur YouTube: pour une exploration des outils de mise en ligne. Mise au point. Cahiers de l'association française des enseignants et chercheurs en cinéma et audiovisuel, (12).

EDPB (2022). Dark patterns in social media platform interfaces: How to recognise and avoid them. Guidelines 3/2022. 14 mars 2022. European Data Protection Board.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

Hils, M., Woods, D. W., & Böhme, R. (2020). Measuring the emergence of consent management on the web. In Proceedings of the ACM Internet Measurement Conference (pp. 317-332).

Kessous E. (2012). L'attention au monde. Sociologie des données personnelles à l'ère numérique, Armand Colin.

Kröger, J. L., Lutz, O. H. M., & Ullrich, S. (2021). The myth of individual control: Mapping the limitations of privacy self-management. Available at SSRN 3881776.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. ISJLP, Vol. 4:3, 543-568.

Mesguish V. & Thomas A. (2013). Net recherche 2013. De Boeck.

Myllylahti, M. (2014). Newspaper paywalls—the hype and the reality: A study of how paid news content impacts on media corporation revenues. Digital journalism, 2(2), 179-194.

Nantel, J., & Weeks, W. A. (1996). Marketing ethics: is there more to it than the utilitarian approach?. European journal of marketing, 30(5), 9-19.

Narayanan, A., Huey, J., & Felten, E. W. (2016). A precautionary approach to big data privacy. Data protection on the move: Current developments in ICT and privacy/data protection, 357-385.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), 100-126.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-13).

Papadopoulos, P., Kourtellis, N., & Markatos, E. (2019). Cookie synchronization: Everything you always wanted to know but were afraid to ask. In The World Wide Web Conference (pp. 1432-1442).

Peyrat, B. (2009). La publicité ciblée en ligne. Rapport, CNIL (Commission Nationale de l'Information et des Libertés).

Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR?. Business Ethics Quarterly, 1-29.

Solove, D. J. (2021). The myth of the privacy paradox. Geo. Wash. L. Rev., 89, 1.

Sweeney L. (2000). Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

Thaler, R. H. (2018). Nudge, not sludge. Science, 361(6401), p. 431.

Thaler, R., Sunstein, C. (2010). Nudge. Comment inspirer la bonne décision. Vuibert.

Viseur, R. (2021). Du tracking, des contre-mesures et de leur efficacité dans la publicité ciblée. Revue ouverte d'ingénierie des systèmes d'information , vol. 2, n°1.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology, 31, 105-109.

Wylie, C. (2019). Mindfuck: Le complot Cambridge Analytica pour s'emparer de nos cerveaux. Grasset.

Zuboff S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.