Revue ouverte d'ingénierie des systèmes d'information
2025, vol. 5, n° 1, 95-120 pages, DOI : 10.21494/ISTE.OP.2025.1301 ISTE OpenScience

Éthique de la gestion du consentement au traitement des données à caractère personnel : Comment les *dark patterns* permettent-ils d'orienter la prise de décision des internautes ?

Ethical management of consent to the processing of personal data: How can dark patterns be used to guide the decision-making?

Robert Viseur[1]

[1] Service TIC, Faculté Warocqué d'Économie et de Gestion, UMONS, 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 sur la 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, nous avons identifié les *dark patterns* utilisés par un ensemble de sites de presse puis avons utilisé la typologie de *dark patterns* de Gray et ses co-auteurs pour classer les designs. Nous avons ensuite discuté, d'une part, leur légalité, d'autre part, leur éthique (du point de vue des approches utilitariste et déontologique). Nous avons enfin discuté 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 collectées à caractère personnel.

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 research, we identified the dark patterns used by a set of press sites and then used the dark pattern typology of Gray and his co-authors to classify the designs. We then discussed, on the one hand, their legality and, on the other, their ethics (from the point of view of the utilitarian and deontological approaches). Finally, we discuss the best ways of combating the abuses observed. In particular, we demonstrate the existence of a grey area that allows professionals to maximise, 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

La protection de la vie privée des citoyens est une préoccupation déjà relativement ancienne. En témoigne la multiplication des recherches dans le domaine économique dès la fin des années soixante-dix [ACQ 09]. Elle résulte d'un compromis entre la divulgation et la protection, supposé satisfaire les individus, les organisations et la société dans son ensemble. Le volume d'informations a connu, avec le développement commercial d'Internet, une accélération au cours du quart de siècle écoulé [ACQ 09] [DUB 17]. La monétisation de nombreux services par la publicité, incluant notamment le secteur de la presse en ligne, et l'essor de la publicité ciblée, ont contribué à cette évolution [DUB 17] [ALL 18]

[LAG 19]. Parmi les bénéficiaires les plus visibles se retrouvent les GAFAM, progressivement devenus incontournables dans le paysage économique. Au cœur de leurs modèles d'affaires : la collecte massive de données (*big data*) 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 RGPD (Règlement général sur la protection des données), 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. Est notamment impactée la myriade d'acteurs impliqués dans les dispositifs de publicité ciblée, en particulier dans ceux, davantage fragmentés, de la publicité programmatique [ALL 18]. Cependant, 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, sont également concernées. Cela concerne par exemple les éditeurs de la presse en ligne [SEH 17] [LAG 19]. 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 [HIL 20], soit des CMP (*Consent Management Platforms*), d'autre part, à la mise en œuvre de *dark patterns* visant à forcer le consentement à l'aide d'artifices techniques et visuels à la légalité et à l'éthique discutables [NOU 20]. Cette recherche propose dès lors une analyse de ces *dark patterns* appliqués aux interfaces de recueil de consentement (CMP) et aux conditions générales d'utilisation des services (CGU) fixant les finalités de la collecte de données. Quelles formes ces *dark patterns* prennent-ils ? Comment influent-ils la prise de décision des utilisateurs ? Quels enjeux éthiques l'utilisation des *dark patterns* soulève-t-elle ? Quels risques les organisations qui y recourent prennent-elles ?

Notre article est organisé en quatre sections. Dans la première section, nous proposons une revue de littérature sur la publicité ciblée, la collecte de données, le *tracking*, le RGPD et le concept de *dark pattern*. Dans la seconde section, nous présentons succinctement notre méthodologie. Dans la 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 la quatrième section, 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. Cet article constitue une version étendue de l'article [VIS 23] présenté lors du congrès INFORSID 2023.

2. Revue de la littérature

Dans cette section nous présentons le rôle croissant des données à caractère personnel sur le Web puis les principales caractéristiques du Règlement général sur la protection des données (RGPD). Nous expliquons ensuite le concept de traceur puis celui de *dark pattern*.

2.1. *Développement du marketing des traces*

Mesguish et Thomas distinguent quatre âges du Web [MES 13]. Le premier, s'étendant de 1994 à 1996, est baptisé « *Web des pionniers* » [MES 13]. 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 stimulée 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* » évolue grâce à l'expansion des réseaux sociaux (audience) ainsi qu'à la large adoption 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* » couvrant à la fois les mondes virtuels (p. ex. moteurs de recherche) et réels (p. ex. objets connectés) [ZUB 19].

La publicité en ligne contemporaine est également le fruit de cette évolution. Elle a en effet pris des formes de plus en plus ciblées [PEY 09]. La publicité personnalisée, basée sur la collecte active de données volontairement divulguées par l'internaute, a longtemps cohabité avec la publicité contextuelle, influencée par le contenu consulté ou recherché [PEY 09] [DUB 17]. Le ciblage s'est par la suite affiné, en exploitant, d'une part, le comportement des internautes (publicité comportementale), d'autre part, les actions entreprises par ces derniers (*retargeting*) [PEY 09] [DUB 17] [VIS 21]. Ce ciblage évolué suppose un travail constant de mise à jour de profils. Si l'attention se porte beaucoup sur les grandes régies internationales liées aux GAFAM, dont Meta (Facebook, Instagram, WhatsApp...) et Google constituent deux acteurs de première importance [VIS 21], le secteur est aussi marqué par l'existence d'acteurs plus petits, notamment actifs en publicité programmatique [ALL 18]. Ces entreprises participent à une collecte passive de données alimentant un flux constant de données entre des acteurs nombreux [DUB 17] [VIS 21]. Le développement de la publicité programmatique implique par ailleurs des exigences de rapidité accrue, par exemple lors de la mise aux enchères en temps réel d'espaces publicitaires disponibles [DUB 17] [ALL 18]. L'objectif est d'optimiser les performances des espaces publicitaires (optimisation du taux de clics ou du taux de conversion selon la modalité retenue).

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. Cela passe principalement par deux textes : la directive ePrivacy, protégeant la vie privée, toujours en cours de révision (futur règlement ePrivacy), applicable depuis 2002, et le règlement général sur la protection des données (RGPD), applicable depuis 2018 [DUB 17].

2.2. *Protection des données*

La protection des données à caractère personnel est assurée, dans l'Union européenne, par le « Règlement général sur la protection des données » (RGPD), publié le 27 avril 2016. Ce dernier est d'application depuis le 25 mai 2018 [BAN 18]. 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. 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* ».

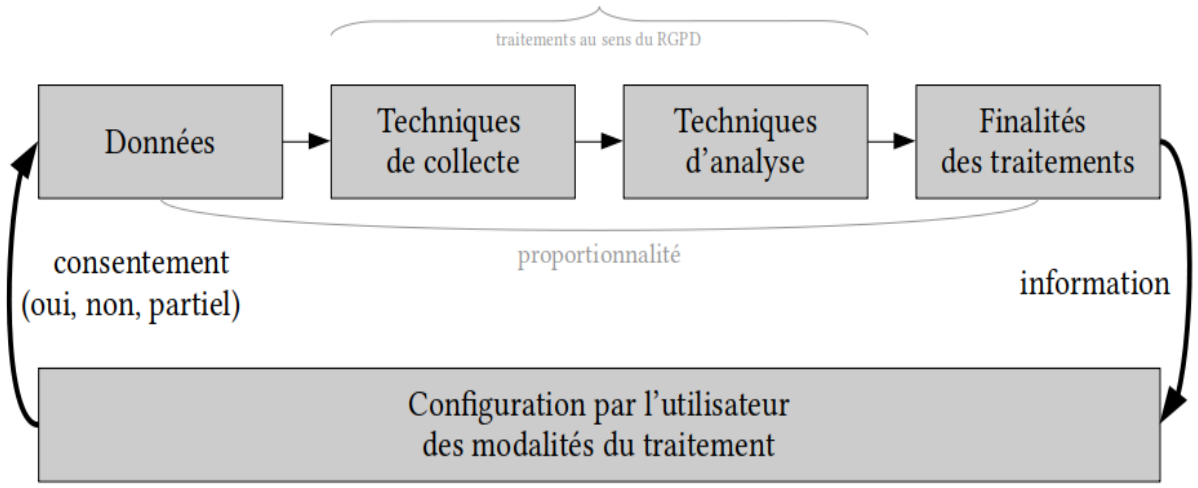

Figure 1. *Fonctionnement du RGPD dans le cadre d'activités marketing.*

Le RGPD prévoit que les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée [BAN 18]. La première condition suppose que le traitement soit fondé, les deux suivantes que la personne ait été correctement informée. La licéité du traitement de données, si elle n'est pas fondée sur le consentement, doit l'être sur un des cinq autres motifs suivants ; (1) l'intérêt légitime (p. ex. lutter contre les fraudes), (2) la mission d'intérêt public (p. ex. travail de la Police), (3) l'exécution d'un contrat (p. ex. contrat de travail), (4) la sauvegarde des intérêts vitaux d'une personne (p. ex. prise en charge suite à un accident) et (5) le respect d'une obligation légale (p. ex. recensement de population). Dans le cas des activités marketing, le consentement sera généralement nécessaire. Il doit être libre, éclairé et se manifester par un acte positif de la part de l'utilisateur (cf. Figure 1). Le consentement au traitement doit également pouvoir être retiré avec une facilité équivalente [GRA 21]. Le RGPD impose aussi que les données collectées soient cohérentes au regard des finalités annoncées (principe de proportionnalité). Le règlement stipule ainsi que soient mises en œuvre des « *mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* ». 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 (APD) telles que la CNIL (Commission Nationale de l'Informatique et des Libertés) en France ou l'APD en Belgique. La question du recueil du consentement est cruciale pour les entreprises traitant des données commerciales, en particulier celles liées à la publicité ciblée et à l'analyse de performances dès lors qu'elles recourent à des données qui ne sont pas anonymisées.

2.3. *Traceurs et collecte de données*

L'exploitation à des fins marketing des données à caractère personnel à partir du navigateur nécessite la capacité à suivre, voire à reconnaître, l'utilisateur [VIS 21]. Ainsi, l'objectif est de permettre le regroupement des données collectées et de dresser un profil. Ce suivi va s'appuyer sur différents types de traceurs incluant les *cookies* et les empreintes (« *fingerprinting* »). Ces dernières sont des codes alphanumériques calculés sur base des caractéristiques de la machine sur laquelle est installé le navigateur [VIS 21]. L'identification de l'utilisateur peut s'appuyer, soit sur des identifiants déterministes (p. ex. *login* et *cookies*), soit probabilistes (p. ex. *fingerprinting* et adresse IP). Par probabiliste nous entendons que l'identification de l'utilisateur passe par le croisement de plusieurs informations (p. ex. empreintes et adresse de connexion).

Les entreprises vont par ailleurs combiner des données internes (dites *first party data*), notamment issues de leur logiciel CRM (*Customer Relationship Management*) et des applications Web (p. ex. sites et comptes de réseaux sociaux), des données issues de partenaires (dites *second party data*) et des données achetées auprès de tiers tels que des courtiers en données (dites *third party data*). Le croisement

de ces données augmente 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 [SWE 00]. 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 [NAR 16].

Ces dispositifs de traçage, et les techniques d'identification associées, se sont progressivement révélés indispensables dans le cadre des activités marketing en ligne des entreprises. En effet, si l'on s'en tient aux seuls *cookies*, ces derniers se révèlent utiles, voire nécessaires, premièrement, pour limiter l'exposition des utilisateurs à une campagne de publicité (principe du *capping*), deuxièmement, pour cibler les publicités qui lui sont envoyées, soit par son suivi au sein d'une session, soit par le biais de son identification puis de son rattachement à un profil, troisièmement, pour dresser des statistiques de fréquentation fiables (p. ex. comptabilisation des visiteurs uniques) [VIS 21].

Dans ce contexte, le RGPD a 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. Ce dernier n'est pas sans conséquence. La multiplicité des intervenants, couplée à l'obligation de collecter le consentement lors de chaque interaction, conduit à une démultiplication des demandes de consentement, dès lors à un risque accru de refus de la part des utilisateurs. Ainsi, si l'on prend un ensemble d'acteurs issus d'une chaîne de publicité programmatique, composé d'une myriade d'acteurs plus petits, la réconciliation de leurs données à caractère personnel nécessite l'utilisation de techniques comme le *cookie syncing* [PAP 19]. Le refus, ou le blocage, partiel ou intégral, de ces *cookies* par les internautes entrave donc la création de profils clients partagés par ces acteurs partenaires. En ont résulté plusieurs réactions. 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. Deuxièmement, des acteurs spécialisés sont apparus pour gérer les interfaces de recueil de consentement en proposant des outils standards : les CMP (*Consent Management Platform*) [NOU 20]. Troisièmement, et cela pré-existait au RGPD, le recours à des interfaces trompeuses s'est multiplié dans les dispositifs de recueil de consentement.

2.4. *Interfaces trompeuses et divulgation des données*

Le traitement des données à caractère personnel, y compris leur protection, a suscité la proposition de stratégies spécifiques qualifiées par Hoepman (2014) de « *privacy design strategies* » [HOE 14] [BOS 16]. Initialement conçues dans le respect du principe de « *privacy by design* », désormais intégré au RGPD, elles ont par la suite été détournées par Bosch et al. (2016) pour donner naissance aux « *privacy dark strategies* » [BOS 16]. Les auteurs identifient huit stratégies principales : maximiser (collecter des données plus que nécessaire), publier (rendre accessibles les données à caractère personnel), centraliser (regrouper les données au sein d'une entité centralisée), préserver (maintenir les relations entre les données), obscurcir (rendre le traitement des données incompréhensible), refuser (limiter le contrôle effectif sur les données), violer (ignorer les choix des utilisateurs) et falsifier (prétendre offrir des mesures de protection inexistantes). Certaines de ces stratégies concernent le stockage des données (centraliser, falsifier), le partage des données (préserver), les opportunités d'analyses futures (préserver), l'analyse des données (maximiser, centraliser, obscurcir) ou encore, spécifiquement, les interfaces de collecte de consentement (refuser, obscurcir, violer). Ces stratégies se concrétisent ensuite en « *privacy dark patterns* » [BOS 16], visant systématiquement à maximiser la quantité de données collectées.

Le terme « *dark pattern* » a été popularisé par Brignull [BRI 11] (avant qu'il adopte le terme « *design trompeur* » ou « *deceptive design* » en anglais). Ce designer distingue ainsi les « *interfaces honnêtes* » des « *dark patterns* ». Si les premières sont conçues dans l'intérêt des utilisateurs, au risque d'entraîner une perte de revenus à court terme, les secondes, tout en restant légales, trompent l'utilisateur pour le profit de l'organisation qui en a la responsabilité. Entre les deux extrêmes de ce continuum, Brignull classe les interfaces optimisées pour accroître les taux de conversion et qui, bien que contraires aux intérêts des consommateurs, permettent cependant la survie d'une activité commerciale [BRI 11]. Sous cet angle, le *dark pattern* peut être rapproché du concept plus ancien de « *technologie persuasive* »

[AHU 22], qui désigne un système interactif conçu pour influencer l'attitude et le comportement des utilisateurs [FOG 02]. Sur le plan éthique, les *dark patterns* sont particulièrement critiqués car ils limitent l'autonomie des utilisateurs en restreignant leur liberté de choix, leur contrôle, leur indépendance d'action et leur capacité d'agir (« *agency* ») [AHU 22]. Par la suite, Brignull a créé, et enrichi, une typologie de *dark patterns* adaptés principalement aux transactions du commerce électronique [BRI 24].

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

Tableau 1. *Typologie de dark patterns (basé sur Gray et al., 2018 [GRAY 18]).*

Le terme « *dark pattern* » désigne donc la situation où un designer utilise sa connaissance du comportement humain (p. ex. psychologie) et des désirs des utilisateurs finaux pour mettre en œuvre des fonctionnalités trompeuses qui ne sont pas dans l'intérêt de l'utilisateur [GRA 18]. Gray et ses co-auteurs 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* ») [GRA 18]. Ces catégories sont ensuite détaillées en incluant des sous-catégories issues de la typologie de Brignull [BRI 24]. Les *dark patterns* permettent au designers d'extraire trois types de ressources des utilisateurs : l'argent, l'attention et les données [NAR 21]. En effet, certains designs trompeurs, comme le motel à cafards (« *roach motel* » ; rendre simples certaines actions mais en complexifier d'autres) ou le *zuckering* de la vie privée (« *privacy zuckering* »[1] ; imposer la divulgation de davantage d'informations que nécessaire) se révèlent directement applicables au traitement des données à caractère personnel. Il est d'ailleurs connu que les comportements des usagers en matière de vie privée sont influencés par le design des interfaces, parfois indépendamment de la volonté du concepteur d'influencer ou non l'utilisateur [ACQ 15]. Il en résulte un écart parfois surprenant entre l'attitude et le comportement du consommateur en matière de vie privée.

Ces *dark patterns* sont utilisés lors de la conception des CMP [NOU 20]. Cependant, le même type de technique se retrouve dans la mise en forme des conditions générales de vente. La longueur excessive des CGUs des réseaux sociaux, soit une forme d'obstruction, a d'ailleurs 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[2]. McDonald et Cranor ont pour leur part évalué le temps annuel de lecture des politiques de confidentialité à 244 heures [MCD 08]. Les *dark patterns* présentent des effets nuisibles

[1] Le "privacy zuckering" n'apparaît plus dans la liste des *deceptive patterns* de Brignull. Toutefois, il reste associé à l'action forcée (cf. https://www.deceptive.design/types/forced-action) et continue d'être mentionné par plusieurs auteurs [BOS 16] [OZD 19] [STA 21]. Nous avons donc choisi de le conserver.

[2] Voir https://creapills.com/dima-yarovinsky-longueur-conditions-generales-reseaux-sociaux-20180507.

à plusieurs niveaux. D'une part, ils compromettent le bien-être individuel [BON 21]. D'autre part, ils favorisent des comportements anticoncurrentiels [DAY 20]. En effet, les *dark patterns* permettent à une organisation d'extraire davantage d'argent ou d'attention au détriment de ses concurrents. De plus, ils érodent la confiance des consommateurs [BON 21].

Dans la pratique, l'utilisation des *dark patterns* est alimentée par trois grands ensembles de pratiques [NAR 21]. Premièrement, les pratiques commerciales peuvent être « *trompeuses et manipulatoires* », couvrant un large éventail allant de pratiques courantes à d'autres clairement illégales [NAR 21] [LAC 12]. Deuxièmement, le « *growth hacking* », qui vise à accélérer l'adoption des services en ligne, a stimulé l'émergence de méthodes d'optimisation basées sur les données (p. ex. tests A/B[3]). Ces méthodes ont contribué à la diffusion des *dark patterns* en encourageant l'utilisation de techniques efficaces, mais peu éthiques. Brignull note que les *dark patterns* ne résultent pas toujours d'une intention malveillante, mais peuvent être le simple produit d'un processus d'optimisation des taux de conversion [BRI 11]. Troisièmement, la recherche comportementale a permis de mieux comprendre les « architectures de choix » [NAR 21] [THA 18]. Ainsi, le concept de *dark pattern* peut être rapproché des notions de « *nudge* » et de « *sludge* » popularisées par Thaler et Sunstein [THA 10] [THA 18].

Thaler et Sunstein présentent le *nudge* comme un dispositif placé au sein d'une architecture de choix, aidant l'utilisateur à « *faire des choix plus judicieux sans restreindre aucune option* » [THA 18]. Le concept de *nudge* a été adapté au domaine numérique. Weinmann et ses co-auteurs (2016) introduisent le terme « *digital nudge* », désignant « *des éléments du design de l'interface utilisateur qui guident le comportement des personnes dans des environnements numériques de choix* » [WEI 16]. Les *nudges* tirent parti des limites de la psychologie humaine [BOS 16]. En effet, les choix exprimés par les individus s'inscrivent dans une rationalité limitée [KAH 03], rendant les modèles rationnels (croyances, choix) psychologiquement irréalistes [KAH 03]. La plupart des décisions sont ainsi prises de manière intuitive [STA 21]. L'être humain utilise deux systèmes cognitifs [KAH 03] [BOS 16]. Le « *Système 1* » permet de réaliser des tâches rapidement et automatiquement, guidé par des habitudes et des « *raccourcis mentaux* » [ARD 23], et est difficilement contrôlable. Le « *Système 2* », plus lent et délibéré, repose sur des règles et est plus facilement gouvernable [KAH 03]. Les *dark patterns* exploitent ces biais cognitifs, comme la tendance à privilégier une gratification immédiate (par exemple, sacrifier sa vie privée future pour un accès immédiat à un service). Dans le cas des *nudges*, ces limites sont utilisées au profit de l'utilisateur. Toutefois, cette forme de manipulation « bienveillante » (*sic*) suscite des débats éthiques. Dans la logique du paternalisme libertaire, il est donc ici question d'inciter l'utilisateur, plutôt que de le forcer, à adopter ce qui est jugé le meilleur choix pour lui. En ce sens, certaines dispositions du RGPD relèvent de cette idéologie. L'utilisateur reste en effet libre et responsable de ses choix. Cependant, le règlement prévoit certaines dispositions jugées favorables aux utilisateurs, comme l'interdiction des cases pré-cochées, soit un *dark pattern* identifié par Brignull sous le nom de « *préselection* » [BRI 24]. En pratique, le recours aux *nudges* se révèle particulièrement efficace dans le cas de la protection de la vie privée [HUM 19]. La définition du « *sludge* » présente moins de stabilité.

Thaler présente initialement le *sludge* comme un dispositif visant « *à rendre plus difficiles la prise de décisions judicieuses et l'activité prosociale* » [THA 18]. Il y associe une intention malveillante de la part du vendeur qui souhaiterait de la sorte « *maximiser ses profits plutôt que d'améliorer le bien-être des acheteurs* ». Cette définition a par la suite été revue par Sunstein [SUN 20] [SOM 20] [NEW 22]. D'une part, Sunstein précise d'abord que le *sludge* peut être déployé de manière intentionnelle ou par inadvertance [SUN 20]. En cela, un *dark pattern* (au sens de Brignull) constitue bien un *sludge*. D'autre part, il caractérise le *sludge* par deux propriétés : il nuit aux intérêt de l'utilisateur (« *bad* ») et il ajoute une « *friction importante* » dans l'accomplissement d'une activité. Ici, le *dark pattern* pourra être vu comme un *sludge* s'il complexifie intensément la prise de décision éclairée (p. ex. obstruction) tandis qu'il relèvera plutôt du « *nudge insidieusement facile* » dans le cas de légères interférences d'interface.

[3] Le test A/B permet de tester plusieurs variantes d'un design et de conserver le design le plus performant au regard du critère retenu [YOU 14].

En résumé, les *dark patterns* appliqués aux plateformes de collecte de consentement relèveront du *sludge* au sens de Thaler ou, soit du *sludge*, soit du *nudge* insidieusement facile, au sens de Sunstein [THA 18] [SUN 20]. Ce dernier recourt d'ailleurs à une logique de classification similaire à Soman qui associe le *dark pattern* à un *nudge-for-bad* synonyme de *nudge* insidieusement facile [SOM 20]. Par soucis de simplicité, nous resterons fidèles, dans la suite du document, à la définition du *sludge* fournie initialement par Thaler [THA 18].

3. Méthodologie

Cette analyse 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'accompagnait. Cette sélection a permis d'associer un ensemble de pratiques courantes à la typologie de *dark patterns* proposée par Gray et ses co-auteurs [GRAY 18].

Cette typologie est détaillée dans un article largement cité dans la littérature (866 fois au 26 septembre 2024 sur Google Scholar). Les auteurs, et notamment Colin M. Gray, continuent d'apporter leurs contributions à cette problématique [GRA 21] [GRA 23a] [GRA 23b]. Leur typologie présente l'avantage de se fonder sur celle de Brignull tout en étant fréquemment utilisée comme référence dans les études portant sur les *dark patterns* présents sur des sites web ou des applications mobiles [FAN 18] [GRA 21] [DIG 21]. Ce choix nous permet ainsi de nourrir un domaine de recherche en pleine évolution. 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.

Bösch et ses co-auteurs (2016) consacrent une section de leur analyse aux conditions d'utilisation (« *terms and conditions* ») [BOS 16]. Ils soulignent que plusieurs facteurs entravent l'exercice d'un choix rationnel. D'une part, ces documents recourent souvent à un langage complexe et difficile à comprendre pour le grand public [LUG 13]. D'autre part, leur longueur empêche parfois leur lecture systématique [MCD 08]. Aussi, dans notre analyse des *dark patterns* applicables aux interfaces de collecte de consentement, nous ferons une distinction entre l'interface proprement dite (CMP) et le texte des conditions générales d'utilisation (CGU) qui l'accompagne et précise les données collectées, les analyses réalisées, leurs finalités. En effet, CMP et CGU mettent en œuvre des techniques distinctes visant à limiter l'exercice d'un choix libre et éclairé par les utilisateurs.

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 ses co-auteurs [GRA 18], 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.

Technique	CMP	CGU
Harcèlement	Demande récurrente d'autorisation (p. ex. géolocalisation).	Validation récurrente des CGU modifiées d'un service.
Obstruction	Multiplication des étapes pour refuser. 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 motel à cafards).	Texte très long noyant l'information, ou écrit dans un langage volontairement cryptique.
Interférence d'interface	Cases de consentement pré-cochées. Appel au consentement puis à payer. Mise en évidence du bouton pour accepter. Moindre visibilité du bouton pour refuser.	Masquage des clauses les plus problématiques (p. ex. utilisation des données d'un formulaire à des fins commerciales).
Action forcée	Principe des *cookie walls* (accès au service conditionné à l'acceptation ou au paiement). Fourniture de la date de naissance pour valider une limite d'âge (principe du *zuckering* de la vie privée).	na

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

4.2. *Analyse des dark patterns*

Cette analyse distingue, d'une part, les *dark patterns* appliqués aux interfaces de collecte du consentement (CMP), d'autre part, ceux qui le sont aux conditions générales d'utilisation (CGU).

4.2.1. *Dans le cas des CMP*

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[4]) 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 interdit, par exemple dès lors qu'un accès à une version minimale du contenu est offerte (décision du Conseil d'État[5]).

[4] Voir https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

[5] Voir https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques.

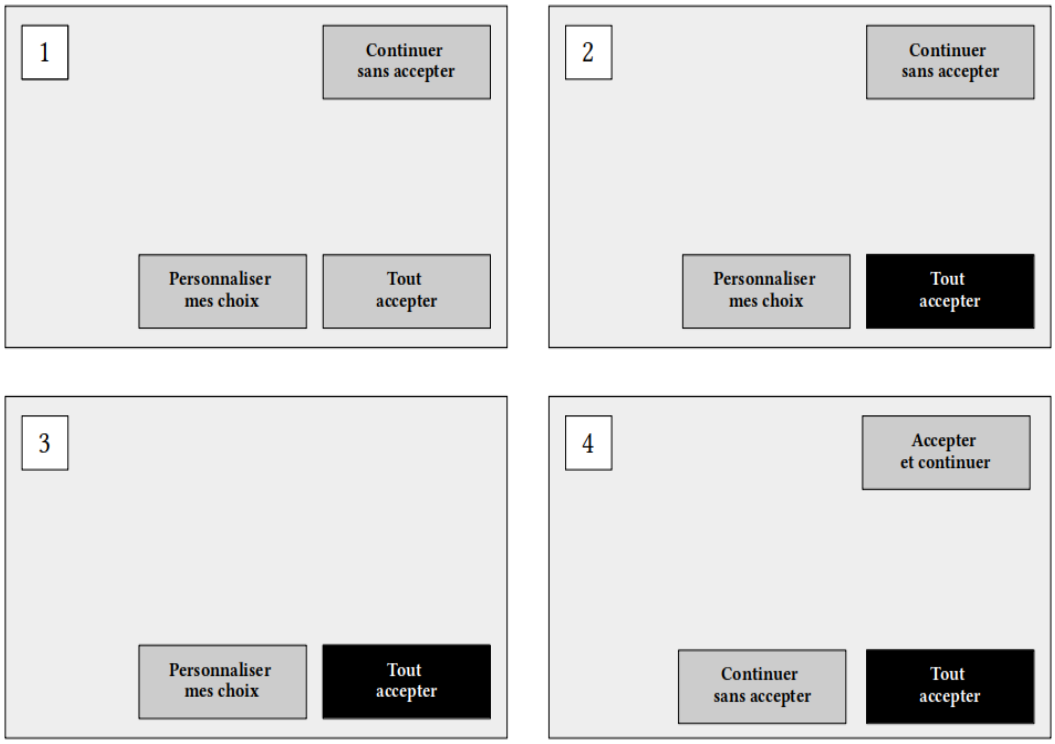

Figure 2. *Dark patterns de type interférence d'interface (2, 3, 4).*

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, a par la suite disparu, une conséquence possible de la bronca déclenchée sur les réseaux sociaux par cette découverte.

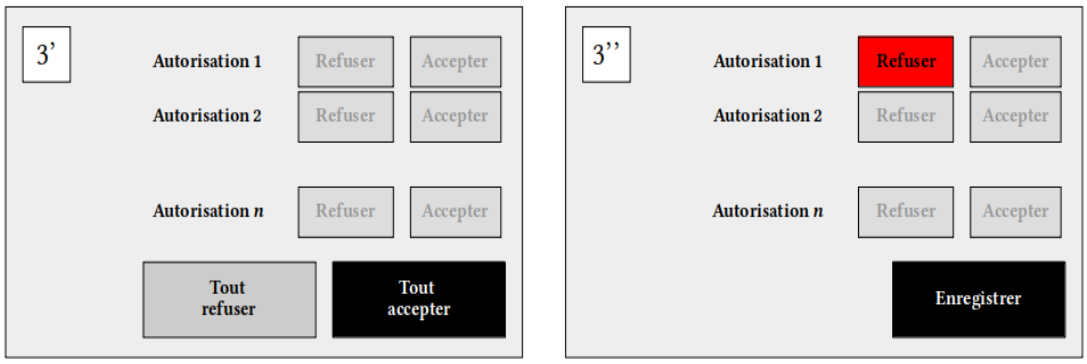

Figure 3. *Dark patterns de type interférence d'interface (3', 3'').*

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 3 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).

4.2.2. *Dans le cas des CGU*

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 discutons dans cette section de l’éthique des *dark patterns*, de l’impact sur notre analyse de la nouvelle typologie proposée par l’EDPB (*European Data Protection Board*) puis de la régulation des pratiques. Cette dernière est mise en perspective avec la dépendance aux revenus de la publicité ciblée, en particulier dans le secteur de la presse.

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[6] 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*

[6] Voir https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

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* » »[7]. 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* »[8]. 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* »[9].

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* »[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]). Cette évolution de la position de la CNIL s'explique notamment par l'arrêt rendu par la CJUE (Cours de Justice de l'Union Européenne) le 4 juillet 2023[11] associant la licéité des *cookies walls* à l'existence d'une alternative au traitement des données à caractère personnel.

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. Cette situation illustre bien la dépendance de la presse en ligne vis-à-vis de Google [LAG 19] [OUA 20]. Google est en effet un pourvoyeur de trafic, avec Google Actualités, nécessaire pour alimenter le modèle *freemium* couramment appliqué dans le secteur [SEH 17], mais aussi de revenus, avec sa régie publicitaire. Cette relation prend parfois l'allure d'un pacte faustien où, en échange d'un accès au contenu des articles, la

---

[7] Voir https://www.cnil.fr/sites/cnil/files/atoms/files/lignes_directrices_du_cepd_sur_le_consentement.pdf.

[8] Voir https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookie-walls/monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques.

[9] Voir https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf (page 61).

[10] Voir https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf (page 10).

[11] Voir https://curia.europa.eu/juris/document/document.jsf?docid=275125.

presse reçoit une assistance du moteur de recherche en matière de monétisation des contenus et d'exploitation des données. Ces collaborations s'inscrivent dans le cadre de la Google News Initiative mise en place par Google en soutien à la presse européenne [ALB 18].

La discussion de l'éthique des *dark patterns* appliqués aux CMP, directement liés à la publicité en ligne, peut s'appuyer sur des discussions pré-existantes en matière d'éthique des *nudges* [SUN 15], d'éthique des systèmes d'information [HAM 18], d'éthique de l'intelligence artificielle [DIG 19] et d'éthique en marketing [NAN 96]. Deux paradigmes éthiques, liés à l'approche cognitiviste, ressortent généralement : le conséquentialisme, incluant l'une de ses déclinations, l'utilitarisme (« *utilitarian ethics* »), et la déontologie (« *deontological ethics* ») [NAN 96] [HAM 18] [DIG 19]. Le courant conséquentialiste juge les actions à partir de leurs conséquences. Ainsi l'utilitarisme recourt au « *principe d'utilité sociale* », à savoir « *le plus grand bien pour le plus grand nombre* » [HAM 18]. Il délaisse donc l'idée de droits inaliénables pour l'individu mais privilégie un arbitrage coûts - bénéfices. L'action peut léser certains individus si elle profite au plus grand nombre. Dans le domaine du marketing, cela se traduit par une préoccupation pour la satisfaction des consommateurs [NAN 96]. Le courant déontologique valorise davantage les notions de devoir et d'intention morale [HAM 18]. Certaines actions sont dès lors proscrites au nom de règles intransgressibles [DIG 19]. Le respect de l'autonomie de l'utilisateur [AHU 22], dans ses composantes de liberté, d'indépendance, d'agentivité et de contrôle, peut ainsi être rattaché à la déontologie. Cette approche va notamment s'appuyer sur des codes d'éthique. Les codes d'éthique professionnelle (p. ex. *Association for Computing Machinery* ACM *Code of Ethics and Professional Conduct* et *Institute of Electrical and Electronics Engineers* IEEE *Code of Ethics* dans le domaine informatique), applicables aux développeurs d'applications et aux concepteurs d'interfaces [BER 99], s'inscrivent dans ce cadre. Une fois déterminé le caractère éthique ou non du résultat, et son caractère intentionnel ou non, la responsabilité du concepteur peut ainsi être engagée [BER 99]. En marketing, ces codes sectoriels insistent sur 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 [NAN 96]. L'approche socialement responsable du marketing postule ainsi l'existence d'un contrat social implicite entre la société et l'entreprise [LAC 21]. L'approche du paternaliste libertaire défendue par Sunstein (2015) développe un utilitarisme (augmenter le bien-être global) teinté de déontologie (préserver l'autonomie individuelle) [SUN 15]. En particulier, il se préoccupe de l'adhésion individuelle au dispositif « *tel que jugé par les individus eux-mêmes* » (critère AJBT) [SUN 15] [SUN 18].

Types	Éthique	Légalité
Harcèlement	Non (utilitarisme) car consentement obtenu par l'exercice d'une forme de coercition sur une large part d'utilisateurs (contraire au principe d'utilité sociale). Non (déontologie) car mépris de l'esprit du RGPD, de règles déontologiques professionnelles et de l'autonomie de l'utilisateur.	Oui mais en sursis du côté des APDs (cf. recommandations).
Obstruction	Oui (utilitarisme) dès lors que l'utilisateur est « accompagné » vers l'option jugée la plus susceptible le satisfaire (accès contre données) sans entrave forte à un choix contraire. Non (déontologie) car entrave à l'autonomie de l'utilisateur (p. ex. asymétrie de l'effort).	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 (utilitarisme) car obtention par la ruse au détriment de l'utilisateur et, sur le long terme, nuisible au commerce. Non (déontologie) car mépris de l'autonomie de l'utilisateur (p. ex. absence de contrôle par l'utilisateur).	Non pour la sournoiserie appliquée aux CMPs[12] mais oui pour de nombreuses techniques appliquées aux CGUs (p. ex. longueur et complexité) sauf si le *pattern* nuit clairement au caractère informé du consentement.
Interférence d'interface	Oui (utilitarisme) dès lors que l'utilisateur est accompagné vers l'option jugée la plus encline à le satisfaire (accès contre données) ; non dès lors que l'interférence entraîne une confusion avec d'autres designs existants et tend vers la tromperie (cf. Figure 2 /4 par exemple). Non (déontologie) car violation de l'esprit du RGPD.	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	Non (utilitarisme, déontologie) si entrave rédhibitoire à l'exercice d'un choix. Oui (utilitarisme, déontologie) si une alternative est clairement présentée (payer en données ou payer en argent) car atteinte d'un compromis et restriction moindre des libertés qu'une action forcée (consentir ou être bloqué).	Oui, mais en cours de discussion, en cas de proposition d'alternatives claires (payer en données ou payer un abonnement) selon le principe des *paywalls*.

Tableau 3. *Caractère éthique ou légal des dark patterns appliqués aux CMP ou aux CGU.*

Du point de vue de l'éthique utilitariste, certaines pratiques d'obstruction peuvent se justifier. En effet, elles assurent un compromis équilibré entre l'accès à l'information (lecteurs) et la nécessité d'un modèle de revenus (éditeurs). Cette modalité tend à préserver un accès équitable à des services en ligne, et mène à la satisfaction du client, souvent peu enclin à payer, en particulier dans le cas des sites d'actualités [KAM 15]. Du point de vue déontologique, ces pratiques ne respectent, ni l'esprit porté par le RGPD, ni certains codes éthiques professionnels. Quelle que soit l'approche éthique retenue, les *dark patterns* de harcèlement ou de sournoiserie paraissent difficilement justifiables (même sur un plan utilitariste), tout en étant de plus en plus critiqués sur un plan légal. Le premier s'accompagne en effet de dispositifs oppressants (p. ex. demandes répétées) tandis que le second se traduit par des comportements mensongers (p. ex. ignorer le refus de consentement). Ces dispositifs peuvent entraîner, d'une part, l'insatisfaction d'un client malmené ou trompé, d'autre part, une défiance généralisée (éditeurs, régies, annonceurs) nuisible au commerce. Il en va de même de certaines interférences d'interface relevant de

[12] Voir par exemple https://www.conseil-etat.fr/actualites/cookies-publicitaires-google-definitivement-condamne-a-payer-100-millions-d-euros.

la tromperie pure et simple, et s'accompagnant d'ailleurs d'un rapide retrait dès lors qu'elles sont identifiées puis accompagnées d'un « *name and shame* » sur les réseaux sociaux. Ce préjudice collectif peut surpasser les avantages économiques que les éditeurs retirent de ces pratiques. Or, si ces conséquences négatives pour les utilisateurs sont supérieures aux bénéfices pour les éditeurs, l'action ne contribue pas au « *principe d'utilité sociale* », qui vise « *le plus grand bien pour le plus grand nombre* », défendu par l'approche utilitariste.

Les *paywalls* utilisés par le secteur de la presse restent disputés sur le plan de la légalité. Cette pratique tend cependant à devenir acceptée dès lors que les dispositifs mis en œuvre offrent une véritable alternative. En présentant clairement les choix possibles (payer en données ou payer un abonnement), en proposant un compromis entre le besoin d'un accès aisé à l'information des lecteurs et la nécessité d'un modèle de revenus pour les éditeurs, le dispositif s'éloigne de la classique action forcée (payer en données ou être bloqué). Il semble apte à satisfaire tant les éthiques utilitaristes (compromis mutuellement satisfaisant) que, dans une mesure moindre cependant, déontologiques (contrôle par l'utilisateur), en particulier en cas de péage souple autorisant la lecture d'un quota d'articles gratuits. Les éditeurs sont en effet confrontés à la difficulté de faire payer pour l'accès à des contenus faciles à diffuser mais coûteux à produire [HIM 15] [KAM 15] [ARR 16]. Reste donc à voir, dans une optique davantage déontologique, l'accueil sur le long terme de ces dispositifs clarifiés par les utilisateurs eux-mêmes dont on observe, du moins sur certaines niches commerciales, une propension accrue à payer pour accéder à du contenu de qualité [HIM 15] [ARR 16] [ROB 24].

Figure 5. *Exemple de dark pattern de type obstruction (CMP).*

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). Des *dark pattern*s demeurent présents sur les sites web des journaux, comme en témoigne cette obstruction (absence de bouton de refus à côté du bouton d'acceptation) observée (capture d'écran du 29 octobre 2024) sur le site d'un grand journal belge francophone (cf. Figure 5). L'utilisation de designs trompeurs, notamment l'obstruction et les interférences visuelles, par des titres de presse flamands appartenant au groupe Mediahuis, a cependant été condamné en septembre 2024[13].

[13] Voir https://www.autoriteprotectiondonnees.be/citoyen/l-apd-prend-des-mesures-a-l-encontre-de-mediahuis-pour-l-utilisation-illicite-de-bannieres-de-cookies-sur-des-sites-de-presse.

5.2. *Comparaison à la typologie de l'EDBP*

La problématique des *dark patterns* a fait l'objet d'une analyse approfondie par l'EDPB (*European Data Protection Board*) dans un document, postérieur au démarrage de cette recherche, daté du 14 mars 2022 [EDP 22]. 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 ses co-auteurs [GRAY 18]. Le choix de cette typologie affaiblit-elle la qualité de l'analyse menée dans cette recherche ? Cette question appelle une réponse prudente et nuancée. Premièrement, la publication de cette typologie par un organisme officiel faisant autorité en Europe suppose au minimum une attention quant à la diffusion de cet outil. L'adaptation de recherches ultérieures à la typologie européenne pourrait dès lors se révéler indispensable. Deuxièmement, la typologie proposée par Gray et ses co-auteurs présente le double avantage d'être largement citée dans la littérature et de proposer un cadre général, largement inspiré de la typologie de Brignull [BRI 24], pour les activités de commerce en ligne. Troisièmement, et comme nous allons le voir à la suite, les deux typologies se recouvrent partiellement.

Types		**Modalités**	
	Origine	**CMP**	**CGU**
Harcèlement	[EDP 22]	Messages continus	Messages continus
Obstruction	[GRA 18] [EDP 22]	Labyrinthe de la vie privée	Labyrinthe de la vie privée
	[EDP 22]	Trop d'options	
			Longueur excessive
			Absence de hiérarchie
			Fausse hiérarchie
	[GRA 18]	Motel à cafards	
Sournoiserie	[GRA 18]	Continuité forcée	
	[EDP 22]		Impasse
	[EDP 22]		Informations trompeuses
	[EDP 22]		Informations contradictoires
	[EDP 22]		Décontextualisation
	[GRA 18]	Action déviée	
Interférence d'interface	[GRA 18] [EDP 22]	Présélection	
	[EDP 22]		Informations parasites
	[EDP 22]		Discontinuité de langue
	[GRA 18] [EDP 22]		Langage ambigu
	[GRA 18] [EDP 22]		Exploitation des émotions
	[EDP 22]	Détournement d'attention	
Action forcée	[GRA 18]	*Zuckering* de la vie privée	
		Paywalls	

Tableau 4. *Référentiel d'analyse des dark patterns (enrichissement de [GRAY 18]).*

La typologie de l'EDPB recouvre six catégories (les traductions en français sont de l'auteur) : la surcharge (« *overloading* »), le brouillage (« *skippping* »), la déstabilisation (« *stirring* »), l'entrave (« *hindering* »), la volatilité (« *fickle* ») et le masquage (« *left in the dark* »). La surcharge décrit les cas

où l'utilisateur est confronté à une avalanche de requêtes, d'informations, d'options ou de possibilités. Elle relève ainsi du harcèlement (demandes répétées) et de l'obstruction (quantité d'informations ou d'alternatives à analyser). Le brouillage, la déstabilisation et le masquage recouvrent pour leur part différentes formes d'interférences d'interface incluant en particulier les présélection, l'exploitation des émotion et les fausses hiérarchies. L'entrave, de par sa définition, relève plutôt de l'obstruction. La fusion de ces deux typologies offrirait dès lors un référentiel plus complet pour analyser les pratiques existantes en matière de *dark patterns*. Nous proposons dès lors un enrichissement de la typologie de Gray et ses co-auteurs à l'aide des sous-catégories proposées par l'EDBP (cf. Tableau 4).

5.3. *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 le cas, déjà évoqué, de la presse en ligne [LAG 19] mais aussi celui des nouveaux médias émergents sur des plates-formes telles que Youtube [CAU 19]. En résulte une dépendance aux GAFAM, et en particulier à Google et Meta, qui dominent le marché de la publicité en ligne (avec une part de marché cumulée sur le marché français d'environ 75 % [VIS 21]). Certes, il existe des modes de rémunération alternatifs tels que les dons récurrents [BES 17] ou les abonnements [SCH 03]. 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 [MYL 14]. Quant aux médias d'actualités issus de l'ère numérique, ils dépendent dans l'immense majorité des cas d'un modèle exclusivement publicitaire [SEH 17]. Les médias recourent en outre à des *widgets* valorisés par la collecte de données (p. ex. AddThis [VIS 21]) et incluent, sans doute par facilité, des objets également avides de données (p. ex. vidéos Youtube embarquées).

Cette dépendance aux données à caractère personnel, directe pour les régies publicitaires, indirecte pour les producteurs de contenus, eux-mêmes souvent dépendants des régies publicitaires, explique l'échec des mécanismes d'*opt-in* comme le champ d'en-tête HTTP DNT *Do Not Track*[14]. 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 ses co-auteurs [NOU 20]. Les travaux du W3C, notamment le P3P (*Platform for Privacy Preferences*), qui permettait de spécifier les préférences de confidentialité dans le navigateur, ont ainsi été suspendus. Cependant, cette approche n'a pas été entièrement abandonnée comme en témoignent les travaux récents sur les protocoles *Global Privacy Control* (GPC) [ZIM 23], inspiré par DNT, et *Advanced Data Protection Control* (ADPC) [HUM 22]. 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 par exemple en œuvre un mécanisme de filtrage de *cookies* tiers (ITP) dont le principe s'est ensuite étendu à Firefox [VIS 21].

De cette dépendance découlent donc des pratiques, parfois agressives, souvent légales mais à l'éthique discutable (*sludge*), pour obtenir le consentement au traitement de données à caractère personnel. La complexité inhérente à l'octroi d'un consentement libre et éclairé s'oppose à l'idéal de gestion individuelle [KRO 21]. Les appels répétitifs et parfois vicieux (*dark patterns*) conduisent à la résignation de nombreux utilisateurs, ce que Solove a théorisé sous l'expression « *mythe du paradoxe de la vie privée* » [SOL 20]. 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 ses co-auteurs [NOR 07]. Waldman l'explique notamment par la rationalité limitée des consommateurs, ce qu'Acquisiti et ses co-auteurs confirment et illustrent [WAL 20] [ACQ 15]. Cependant, Solove y voit plutôt un comportement rationnel [SOL 20]. 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

[14] Voir https://developer.mozilla.org/fr/docs/Web/HTTP/Reference/Headers/DNT et http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html pour plus d'informations.

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. Notre analyse, et la mise en évidence de ces techniques dans un secteur pourtant supposé être composé d'acteurs de confiance, tend à appuyer cette théorie. N'est-il pas ironique, à ce propos, et même si l'objet initial de ce devoir diffère un peu, que la Charte de Munich prévoit explicitement de « *s'obliger à respecter la vie privée des personnes* », alors que ses adhérents aident en définitive les régies dominantes à assouvir leur appétit en données à caractère personnel ? En résumé, la rationalité limitée des utilisateurs facilite l'obtention d'un consentement par la manipulation en exploitant leurs habitudes et biais cognitifs (Système 1) [ACQ 15] [WAL 20]. Cependant, les utilisateurs désireux de réguler consciemment la collecte de données à caractère personnel (Système 2) rencontrent également des interfaces qui entravent l'exercice de leurs choix. Cela se manifeste chez eux par une fatigue du consentement [GRA 21], une résignation rationnelle [SOL 20].

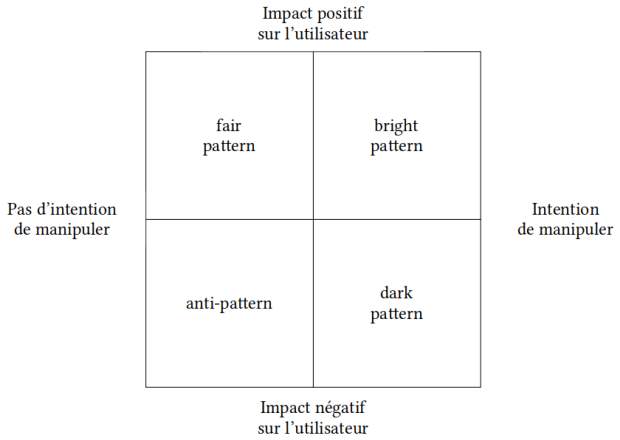

Figure 6. *Dark pattern, bright pattern, fair pattern et anti-pattern.*

Deux mesures plus globales peuvent contribuer à la lutte contre les *dark patterns*. La première mesure porte sur l'éducation à ces pratiques, visant deux publics : les citoyens et les designers d'interface utilisateur. En ce qui concerne les citoyens, Bongard-Blanchy et ses co-auteurs (2016) ont démontré que ceux qui sont les plus capables de reconnaître les *dark patterns* sont également les moins susceptibles d'y être influencés [BON 16]. Ils recommandent donc de concentrer les efforts de sensibilisation sur les générations plus âgées (plus de 40 ans) et les personnes ayant un faible niveau d'éducation, car ces groupes sont à la fois moins capables d'identifier les *dark patterns* et moins conscients des moyens d'influencer leurs choix et comportements [GRA 21]. L'objectif est ici de susciter, soit l'adoption de nouvelles heuristiques (par exemple, rechercher de manière systématique le bouton permettant de tout refuser), soit de promouvoir une pensée délibérative. En ce qui concerne les designers, l'éducation démarre par un inventaire des *dark patterns* existants, réalisé en particulier au sein de communautés actives sur des plateformes comme Reddit ou Twitter (désormais X) [BON 16] ou par des sites spécialisés [BOS 16]. Ensuite, les critères de sélection des designs doivent être intégrés dans des codes d'éthique professionnelle, tels que celui de l'ACM[15] [GRA 21] [NAR 21]. L'éducation doit aussi passer par la promotion de pratiques au sein des entreprises [NAR 21], telles que le choix de designs et d'indicateurs de performances qui favorisent la préservation de l'autonomie et de la vie privée des utilisateurs. Cela inclut par exemple l'utilisation de « *bright patterns* », des designs qui orientent les utilisateurs vers les choix les plus protecteurs, ou de « *nudges éducatifs* », comme des retours systématiques sur l'impact des choix retenus au sein des CMP [GRA 21], ou encore l'affichage du nombre de *cookies* déjà acceptés sous forme de jauge [BIE 24]. Ces deux approches se complètent, la

15 Consulter le code de déontologie sur le site de l'ACM à l'adresse suivante : https://www.acm.org/code-of-ethics. Ce document inclut des principes généraux relatifs au bien-être public, à l'honnêteté et à l'inclusivité. Par exemple, il affirme que "*les technologies et les pratiques doivent être aussi inclusives et accessibles que possible, et les professionnels de l'informatique doivent agir pour éviter de créer des systèmes ou des technologies qui privent de droits ou oppriment les personnes)*".

première tenant compte de la rationalité limitée et des biais cognitifs des utilisateurs, et la seconde visant à établir de nouvelles règles procédurales pour les individus motivés. Cependant, Graßl et ses co-auteurs mettent en garde contre les effets, encore mal connus, de ces *patterns* [GRA 21]. D'une part, les techniques d'obstruction, qui retardent l'accès aux options de configuration, créent paradoxalement l'illusion d'un plus grand contrôle chez ces utilisateurs. D'autre part, les *dark patterns* semblent induire une forme de conditionnement, amenant les utilisateurs à consentir massivement à la collecte de données, même lorsque cela va à l'encontre de leurs préférences initiales et que le dispositif de collecte n'implique pas de *nudge*. Les designers peuvent aussi contribuer à l'élaboration de bibliothèques de *patterns*. Ces collections permettraient d'inventorier les pratiques problématiques. À cet égard, il est pertinent de procéder à la distinction, comme le proposent Westin et Chiasson (2019), entre « *design pattern* », « *dark pattern* » et « *anti-pattern* » [WES 19]. Les *designs patterns* consistent en « *un ensemble de solutions flexibles pour résoudre des problèmes architecturaux récurrents* » (p. 58). Lorsqu'un *pattern* produit un effet indésirable, il devient un *anti-pattern*. L'*anti-pattern* se distingue donc du *dark pattern* en ce que l'effet négatif de ce dernier découle d'une « *intention malveillante* ». Ainsi, l'objectif de réduire les mauvaises pratiques non intentionnelles semble plus accessible. Les recueils de bonnes pratiques devraient quant à eux distinguer les concepts de « *bright patterns* » et de « *fair patterns* » [POT 24]. En effet, leurs implications éthiques diffèrent. Le premier pousse l'utilisateur à agir pour son bien supposé (dans une logique de paternalisme libertaire) tandis que le second préserve au maximum sa liberté de choix. Le choix entre l'un ou l'autre constitue donc un dilemme éthique [POT 24]. Potel-Saville et Da Rocha (2024), en s'appuyant sur les travaux de Zachrisson et ses co-auteurs [ZAC 12], présentent le contrôle offert à l'utilisateur sous la forme d'un continuum allant du *dark pattern* (manipulation nuisible à l'utilisateur, ou *sludge*), poursuivant avec le *bright pattern* (manipulation bénéfique à l'utilisateur, ou *nudge*), et terminant par le *fair pattern* (contrôle respectueux de l'utilisateur) (cf. Figure 6) [POT 24]. La réduction des pratiques problématiques repose donc sur une combinaison de pressions internes aux organisations (formation, déontologie des professionnels) et de pressions externes (dénonciations publiques [FAN 18]). En résumé, la stratégie globale consiste à faire évoluer la légitimité[16] des pratiques du secteur en combinant des pressions légales (p. ex. RGPD), normatives (p. ex. codes d'éthiques sectoriels) et individuelles (p. ex. déontologie et dénonciation).

La seconde mesure porte sur le développement de méthodologies outillées pour détecter les *dark patterns*. Comme le soulignent Marthur et ses co-auteurs (2019), l'utilisation des *dark patterns* est largement répandue [MAR 19]. Après l'exploration du concept puis l'élaboration (ou la réconciliation) de taxonomies [GRA 18] [LEI 22] [GRA 23b] [POT 24], la détection automatisée, éventuellement assistée par l'homme du fait des difficultés de repérage [GRA 20], fait partie des pistes de recherche récentes [MAR 19] [STA 21]. La détection à grande échelle de *dark patterns* représente donc un défi pour les organismes chargés de repérer les pratiques contraires aux règles établies par le RGPD. L'automatisation de cette détection pourrait servir trois cas d'utilisation principaux.

Tout d'abord, elle pourrait être intégrée aux navigateurs via des extensions pour alerter l'utilisateur lorsqu'un *dark pattern* est détecté (ou suspecté), ce qui nécessiterait une précision suffisante pour éviter les fausses alertes. Deux types d'alertes pourraient être envisagées : celles concernant le design des interfaces [OZD 20] [STA 21] et celles liées à la complexité des conditions d'utilisation [LUG 13]. Ensuite, cette détection pourrait aider les designers à accélérer l'analyse de la qualité de leurs sites (notamment pour les débarrasser des *anti-patterns*), afin de garantir une conformité maximale avec les législations sur la protection de la vie privée. Enfin, elle pourrait soutenir le travail des Autorités de Protection des Données (APD), d'une part en offrant des outils d'autodiagnostic, et d'autre part en permettant l'identification des contrevenants, ce qui pourrait mener à des avertissements ou à des sanctions.

[16] Pour plus d'informations sur les concepts de légitimité et d'illégitimité organisationnelle, consulter l'article de Roulet (2015) [ROU 15].

Dans ce cadre, les associations et les collectifs jouent un rôle essentiel qui mérite d'être valorisé. Premièrement, ils permettent de mettre en lumière et d'objectiver des comportements qu'il serait nécessaire de contrer par des logiciels ou des réglementations. Parmi les exemples, on retrouve Open Terms Archive, qui permet une traçabilité des modifications de CGU ; TOS;DR qui évalue les CGU sur une échelle normalisée, et Data Experience d'Hestia Labs, qui met en évidence les critères de profilage. Certains de ces groupes participent également à la création de contre-mesures, comme l'extension Privacy Badger éditée par la EFF, qui sert à filtrer les traceurs en ligne. Deuxièmement, ces organisations peuvent intervenir publiquement pour dénoncer les comportements éthiquement douteux, en exploitant l'intérêt des entreprises pour préserver leur réputation en ligne. La récente popularisation du concept de *dark pattern* auprès du grand public pourrait renforcer l'impact de ce type de dénonciation [NAR 21].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 [WYL 19], stables et compréhensibles, permettant dès lors l'octroi d'un consentement réellement éclairé.

	Avant	Actuellement	Futur possible
Macro	Lois nationales (*privacy*).	RGPD (EU). APD.	Cadre juridique mondial émergent (RGPD, CCPA, PIPL…). Renforcement des APD.
Meso	Modèle publicitaire dominant.	Développement d'une niche de marché *pro-privacy*.	Contrôle des GAFAM et des prestataires CMP. Relais par les associations professionnelles (p. ex. IAB). Soutien aux initiatives de standardisation (p. ex. P3P), de labellisation (p. ex. D-Seal) et de création d'outils de détection de mauvaises pratiques. Soutien aux associations *pro-privacy* jouant un rôle de contrôle par la société civile. Action de sensibilisation et de formation (utilisateurs, concepteurs).
Micro	Technologies anti-*tracking* (anonymisation, extensions…).	Technologies anti-*tracking* (anonymisation, extensions…). Consentement libre et éclairé.	Technologies anti-*tracking* (anonymisation, extensions…) et de détection des *dark patterns*. Consentement libre et éclairé.

Tableau 5. *Protection des utilisateurs contre la collecte abusive de données.*

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. En effet, le respect du RGPD s'accompagne aujourd'hui de *dark patterns* légaux à défaut d'être éthiques. Comment le régulateur pourrait-il dès lors optimiser son action ? Nous proposons une stratégie sur trois niveaux (cf. Tableau 5). Au niveau « macro » nous pouvons constater un renforcement de l'arsenal juridique, que ce soit en dehors de l'Europe (voir par exemple le *California Consumer Privacy Act* aux États-Unis et le *Personal Information Protection Law* en Chine) ou en Europe. L'Union européenne a ainsi récemment complété son RGPD par des textes visant à réguler l'action des plateformes, à savoir le DSA (*Digital Services Act*) et, applicable aux acteurs jugés structurants, le DMA (*Digital Market Act*) [NAV 21]. Le soutien à ce cadre légal, incluant le renforcement des agences compétentes (p. ex. APD), devrait stimuler

l'assainissement des pratiques. Au niveau « meso », les autorités publiques peuvent s'appuyer sur un réseau d'acteurs en vue de diffuser les bonnes pratiques. 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 APD un moyen d'action sur des acteurs ayant un impact significatif sur les pratiques auxquelles sont confrontés les utilisateurs. De plus, les APDs disposent d'un relais négocié via les associations professionnelles telles que l'IAB (*Interactive Advertising Bureau*). Cette dernière publie des recommandations à destination des professionnels, via son TCF (*Transparency & Consent Framework*), et maintient également une liste de CMP certifiés[17]. Mentionnons l'exigence de Google, depuis 2024, d'utiliser des CMP certifiés et, depuis 2020, sa collaboration avec l'IAB via l'intégration du TCF[18]. En contrepoids à ces *bigtechs*, davantage de visibilité pourrait également être accordée aux initiatives de standardisation et de labellisation (p. ex. D-Seal) [SCH 23] afin d'améliorer la qualité de l'information à l'utilisateur. Capitaliser davantage sur les collectifs et associations *pro-privacy* pourrait également être pertinent dès lors que ceux-ci se révèlent des soutiens utiles pour les APD en aidant à la construction des dossiers en violation du RGPD. Au niveau « micro », il demeure essentiel de sensibiliser les utilisateurs, notamment en documentant les *dark pattern*s (pour faciliter leur reconnaissance) et en présentant les contre-mesures disponibles (comme les extensions telles que Consent-O-Matic).

La faiblesse actuelle des moyens de contrôle public quant au respect de la vie privée se traduit par la résurgence de ce qu'Alain Supiot qualifie de « *structure juridique féodale* » [SUP 15]. Cette organisation liée au « *reflux du gouvernement par les lois* » s'accompagne d'une extension de « *réseaux d'allégeance* ». Dans le cas des données à caractère personnel, cela entraîne un renforcement progressif de Google en tant que régulateur *de facto* en matière de vie privée. Cette position avait été relevée par Gerardin et ses co-auteurs (2021) suite à la publication par Google d'un ensemble de propositions connu sous le nom de « *privacy sandbox* » [GER 21]. Google y proposait une nouvelle approche du ciblage publicitaire, permettant de dépasser la fin prochaine des *cookies* tiers, en privilégiant un traitement local des données, mais tendant à rendre incontournable le navigateur Google Chrome. Ce statut de régulateur *de facto* impacte également les CMP. En effet, Google impose l'utilisation de CMP certifiés dans le cadre de la diffusion d'annonces publicitaires ciblées et s'appuie explicitement sur les recommandations de l'IAB[19]. Cette dernière publie également une liste de CMP compatibles avec le TCF (*op. cit.*). Notre proposition d'actions sur trois niveaux, si elle s'inscrit dans une continuité européenne et répond pragmatiquement au manque de ressources des APD, présente dès lors un risque évident d'accroître l'« *inféodation* » des acteurs plus petits à des plateformes structurantes que l'Union européenne tente justement de réguler.

6. Conclusion

Dans cette recherche, nous avons présenté l'évolution du marketing en ligne vers une approche de plus en plus ciblée, occasionnant une collecte massive de données à caractère personnel. 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 inciter, de manière plus ou moins sournoise, à consentir au traitement de leurs données. Sur base d'une typologie de *dark patterns*, nous avons alors analysé, sur un ensemble de CMP et de CGU, comment ces *dark patterns* s'appliquaient concrètement au recueil de consentement. Nous avons combiné une typologie largement citée dans la littérature, également employée pour notre analyse [GRAY 18], avec celle récemment proposée par l'EDPB [EDP 22]. Cette recherche nous a permis de

[17] Voir https://iabeurope.eu/cmp-list/.

[18] Voir https://support.google.com/adsense/answer/13554116.

[19] Voir https://support.google.com/admanager/answer/13554116.

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.

Cette recherche présente deux perspectives. Premièrement, et compte tenu de la rapidité de l'évolution du design des CMP, 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. Deuxièmement, l'analyse des flux émotionnels en lien avec les biais psychologiques reconnus émerge comme un champ de recherche en économie. Cela englobe des domaines tels que la finance comportementale [FIN 21] ou la publicité en ligne [SIN 20]. Étudier le comportement des utilisateurs face aux *dark patterns* intégrés aux CMP les plus répandus pourrait tirer parti d'outils de suivi de l'attention (comme l'*eye tracking*) et des émotions (p. ex. électrocardiogramme, ECG), combinés à une modélisation des parcours utilisateur (« *dark path* ») [MIL 23] et à des entretiens semi-directifs. Cette approche permettrait de mieux comprendre l'impact de l'état émotionnel sur la prise de décision en matière de *privacy*. Ainsi, l'influence des *dark patterns*, mais aussi l'efficacité des contre-mesures, pourrait être analysée de manière plus approfondie.

Comme l'a souligné Arduin (2023) [ARD 23], et dans le cadre de notre réflexion sur l'éthique des *design patterns*, il est important de noter le caractère ambivalent de ce type de recherche. Une meilleure compréhension des mécanismes de manipulation des utilisateurs dans leurs choix de consentement peut servir à améliorer les interfaces au profit des utilisateurs (*bright patterns*, *fair patterns*), mais elle risque également de renforcer la sophistication des techniques malveillantes.

Cette recherche comporte deux principales limites. Premièrement, elle se concentre essentiellement sur l'Union européenne et sur la période post-RGPD, ce qui la rend contextuellement et géographiquement située dans l'espace et dans le temps. Or, comme l'ont souligné Laufer et Wolfe (1977), le concept de « *privacy* », bien qu'il inclue des éléments universels (tels que le rôle dans le développement de l'autonomie), reste fortement influencé par les spécificités culturelles des pays ou régions où il est étudié [LAU 77]. Une comparaison entre régions culturellement distinctes (p. ex. France, États-Unis et Chine) permettrait d'identifier à la fois des points communs et des divergences dans la mise en œuvre et la perception des dispositifs de collecte de données à caractère personnel.

Deuxièmement, notre analyse des *dark patterns* s'est limitée à un secteur précis et à un échantillon de sites web. Toutefois, ces pratiques sont également présentes dans les applications mobiles [BOS 16], où elles sont parfois encore plus fréquentes, notamment pour collecter des données à caractère personnel [GUN 21] [DIG 21]. Une analyse comparative des designs récurrents entre sites web et applications mobiles d'un même groupe de médias pourrait donc s'avérer pertinente. En outre, une comparaison des interfaces développées pour les applications mobiles sous Android et iOS apporterait une dimension supplémentaire, étant donné les approches divergentes de Google et Apple en matière de publicité ciblée [VIS 21].

7. Références

[ACQ 09] Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. IEEE security & privacy, 7(6), 82-85. https://doi.org/10.1109/MSP.2009.163.

[ACQ 15] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514. https://doi.org/10.1126/science.aaa1465.

[AHU 22] Ahuja, S., & Kumar, J. (2022). Conceptualizations of user autonomy within the normative evaluation of dark patterns. Ethics and Information Technology, 24(4), 52. https://doi.org/10.1007/s10676-022-09672-9.

[ALB 18] Albrecht, J. (2018). Introducing Subscribe with Google. Google News Initiative, 20 mars 2018. https://blog.google/outreach-initiatives/google-news-initiative/introducing-subscribe-google/.

[ALL 18] Allary J., & Balusseau V. (2018). La publicité à l'heure de la data. Adtech et programmatique expliqués par des experts, Dunod. ISBN : 9782100765751.

[ARD 23] Arduin, P. E. (2023). A cognitive approach to the decision to trust or distrust phishing emails. International Transactions in Operational Research, 30(3), 1263-1298. https://doi.org/10.1111/itor.12963.

[ARR 16] Arrese, Á. (2016). From Gratis to Paywalls: A brief history of a retro-innovation in the press's business. Journalism studies, 17(8), 1051-1067. https://doi.org/10.1080/1461670X.2015.1027788.

[BAN 18] Banck A. (2018). RGPD : la protection des données à caractère personnel, Gualino. ISBN : 9782297224437.

[BER 99] Berdichevsky, D., & Neuenschwander, E. (1999). Toward an ethics of persuasive technology. Communications of the ACM, 42(5), 51-58. https://doi.org/10.1145/301353.301410.

[BES 17] Bessière, V., & Stéphany, É. (2017). Le crowdfunding: fondements et pratiques. De Boeck Supérieur. ISBN : 9782807306783.

[BIE 24] Bielova, N., Litvine, L., Nguyen, A., Chammat, M., Toubiana, V., & Hary, E. (2024). The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 2813-2830). https://www.usenix.org/system/files/usenixsecurity24-bielova.pdf.

[BON 21] Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., & Lenzini, G. (2021)."I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"-Dark Patterns from the End-User Perspective. In Proceedings of the 2021 ACM Designing Interactive Systems Conference (pp. 763-776). https://doi.org/10.1145/3461778.3462086.

[BOS 16] Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies. https://doi.org/10.1515/popets-2016-0038.

[BRI 11] Brignull, H. (2011). Dark Patterns: Deception vs. Honesty in UI Design. DarkPatterns.Org, 01 novembre 2011. https://www.deceptive.design/articles/dark-patterns-deception-vs-honesty-in-ui-design.

[BRI 24] Brignull, H., Leiser, M., Santos, C., & Doshi, K. (2024). Types of deceptive pattern. Deceptive.Design, 30 janvier 2024. https://www.deceptive.design/types.

[HUM 19] Hummel, D., & Maedche, A. (2019). How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies. Journal of Behavioral and Experimental Economics, 80, 47-58. https://doi.org/10.1016/j.socec.2019.03.005.

[CAU 19] 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). https://doi.org/10.4000/map.3417.

[DAY 20] Day, G., & Stemler, A. (2020). Are dark patterns anticompetitive?. Ala. L. Rev., 72, 1. https://dx.doi.org/10.2139/ssrn.3468321.

[DIG 19] Dignum, V. (2019). Responsible artificial intelligence: how to develop and use AI in a responsible way (Vol. 2156). Cham: Springer. ISSN : 2365-306X.

[DIG 21] Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., & Bacchelli, A. (2020, April). UI dark patterns and where to find them: a study on mobile applications and user perception. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-14). https://doi.org/10.1145/3313831.3376600.

[DUB 17] Dubois, L., & Gaullier, F. (2017). Publicité ciblée en ligne, protection des données à caractère personnel et ePrivacy: un ménage à trois délicat. LEGICOM, (2), 69-102. https://doi.org/10.3917/legi.059.0069.

[EDP 22] 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. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

[FAN 18] Fansher, M., Chivukula, S. S., & Gray, C. M. (2018). # darkpatterns: Ux practitioner conversations about ethical design. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-6). https://doi.org/10.1145/3170427.3188553.

[FOG 02] Fogg, B. J. (2002). Persuasive technology: using computers to change what we think and do. Ubiquity, 2002(December), 2. https://doi.org/10.1145/764008.76395.

[GER 21] Geradin, D., Katsifis, D., & Karanikioti, T. (2021). Google as a de facto privacy regulator: analysing the privacy sandbox from an antitrust perspective. European Competition Journal, 17(3), 617-681.

[GRA 21] Graßl, P. A. J., Schraffenberger, H. K., Zuiderveen Borgesius, F. J., & Buijzen, M. A. (2021). Dark and Bright Patterns in Cookie Consent Requests. Journal of Digital Social Research 3, 11 (Feb 2021), 1–38. https://doi.org/10.33621/jdsr.v3i1.54.

[GRA 18] 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). https://doi.org/10.1145/3173574.3174108.

[GRA 21] Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In Proceedings of the 2021 CHI conference on human factors in computing systems (pp. 1-18). https://doi.org/10.1145/3411764.3445779.

[GRA 23a] Gray, C. M., Sanchez Chamorro, L., Obi, I., & Duane, J. N. (2023). Mapping the landscape of dark patterns scholarship: A systematic literature review. In Companion Publication of the 2023 ACM Designing Interactive Systems Conference (pp. 188-193). https://doi.org/10.1145/3563703.3596635.

[GRA 23b] Gray, C. M., Santos, C., & Bielova, N. (2023, April). Towards a preliminary ontology of dark patterns knowledge. In Extended abstracts of the 2023 CHI conference on human factors in computing systems (pp. 1-9). https://doi.org/10.1145/3544549.3585676.

[GUN 21] Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., & Wilson, C. (2021). A comparative study of dark patterns across web and mobile modalities. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 1-29. https://doi.org/10.1145/34795.

[HIL 20] 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). https://doi.org/10.1145/3419394.3423647.

[KAH 03] Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American economic review, 93(5), 1449-1475. https://doi.org/10.1257/000282803322655392.

[HAM 18] Hamet, J., & Michel, S. (2018). Les questionnements éthiques en systèmes d'information. Revue française de gestion, (2), 99-129. https://shs.cairn.info/article/RFG_271_0099/pdf.

[HIM 15] Himma-Kadakas, M., & Kõuts, R. (2015). Who is willing to pay for online journalistic content?. Media and communication, 3(4), 106-115. https://doi.org/10.17645/mac.v3i4.345.

[HUM 22] Human, S. (2022). Advanced data protection control (ADPC): An interdisciplinary overview. arXiv e-prints, arXiv-2209. https://dx.doi.org/10.48550/arXiv.2209.09724.

[KAM 15] Kammer, A., Boeck, M., Hansen, J. V., & Hauschildt, L. J. H. (2015). The free-to-fee transition: Audiences' attitudes toward paying for online news. Journal of Media Business Studies, 12(2), 107-120. https://doi.org/10.1080/16522354.2015.1053345.

[KES 12] Kessous E. (2012). L'attention au monde. Sociologie des données personnelles à l'ère numérique, Armand Colin. ISBN : 9782200280550.

[KRO 21] 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. https://dx.doi.org/10.2139/ssrn.3881776.

[LAC 21] Laczniak, G., & Shultz, C. (2021). Toward a doctrine of socially responsible marketing (SRM): A macro and normative-ethical perspective. Journal of Macromarketing, 41(2), 201-231. https://doi.org/10.1177/0276146720963682.

[LAC 12] Laczniak, G. (2012). Ethics of marketing. In SAGE Brief Guide to Business Ethics (pp. 308-322). Los Angeles : SAGE Publications. ISBN : 978-1412997218.

[LAG 19] Laguës, B. (2019). La presse peut-elle faire sans Google ? La revue des médias, INA, 26 février 2019. https://larevuedesmedias.ina.fr/la-presse-peut-elle-faire-sans-google.

[LAU 77] Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of social Issues, 33(3), 22-42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.

[LEI 22] Leiser, M. (2022). Illuminating Manipulative Design: From" Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive. Loy. Consumer L. Rev., 34, 484. https://lawecommons.luc.edu/lclr/vol34/iss3/6.

[MAT 19] 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. https://doi.org/10.1145/3359183.

[MCD 08] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. ISJLP, Vol. 4:3, 543-568. http://hdl.handle.net/1811/72839.

[MES 13] Mesguish V. & Thomas A. (2013). Net recherche 2013. De Boeck. ISBN : 978-2-8041-8228-1.

[MIL 23] Mills, S., Whittle, R., Ahmed, R., Walsh, T., & Wessel, M. (2023). Dark patterns and sludge audits: an integrated approach. Behavioural Public Policy, 1-27. https://doi.org/10.1017/bpp.2023.24.

[MYL 14] 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. https://doi.org/10.1080/21670811.2013.813214.

[NAN 96] 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. http://dx.doi.org/10.1108/03090569610118713.

[NAR 16] 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. http://dx.doi.org/10.1007/978-94-017-7376-8_13.

[NAR 20] Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. Queue, 18(2), 67-92. https://doi.org/10.1145/3400899.3400901.

[NAV 21] Navaro Auburtin, Q., & Weill, M. (2021). Régulation des plateformes numériques : le moment européen. In Annales des Mines-Realites industrielles (No. 4, pp. 37-40). https://doi.org/10.3917/rindu1.214.0037.

[NEW 22] Newall, P. W. (2022). What is sludge? Comparing Sunstein's definition to others'. Behavioural Public Policy, 7(3), 851-857. https://doi.org/10.1017/bpp.2022.12.

[NOR 07] 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. https://psycnet.apa.org/doi/10.1111/j.1745-6606.2006.00070.x.

[NOU 20] 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). https://doi.org/10.1145/3313831.3376321.

[OUA 20] Ouakrat, A. (2020). Négocier la dépendance? Google, la presse et le droit voisin. Sur le journalisme, 9(1), 44-57. https://doi.org/10.25200/SLJ.v9.n1.2020.417.

[OZD 20] Özdemir, Ş. (2020). Digital nudges and dark patterns: The angels and the archfiends of digital communication. Digital Scholarship in the Humanities, 35(2), 417-428. https://doi.org/10.1093/llc/fqz014.

[PAP 19] 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). https://doi.org/10.1145/3308558.3313542.

[PEY 09] Peyrat, B. (2009). La publicité ciblée en ligne. Rapport, CNIL (Commission Nationale de l'Information et des Libertés). https://www.huntonak.com/files/webupload/PrivacyLaw_CNIL_Report_Online_Advertising.pdf.

[POT 23] Potel-Saville, M., & Da Rocha, M. (2023). From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures. In Annual Privacy Forum (pp. 145-165). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61089-9_7.

[ROB 24] Robertson, C. T. (2024). How Much do People Pay for Online News? And What Might Encourage More People to Pay? In Reuters Institute Digital News Report 2024. https://doi.org/10.60625/risj-vy6n-4v57.

[ROU 15] Roulet, T. (2015). Qu'il est bon d'être méchant! Paradoxe de l'illégitimité organisationnelle dans le contexte des banques d'investissement. Revue française de gestion, (3), 41-55. https://doi.org/10.3166/RFG.248.41-55.

[SCH 23] Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR?. Business Ethics Quarterly, 1-29. https://doi.org/10.1017/beq.2022.30.

[SOL 21] Solove, D. J. (2021). The myth of the privacy paradox. Geo. Wash. L. Rev., 89, 1. https://dx.doi.org/10.2139/ssrn.3536265.

[SUN 20] Sunstein, C. R. (2020). Sludge audits. Behavioural Public Policy, 6(4), 654-673. https://doi.org/10.1017/bpp.2019.32.

[SUN 18] Sunstein, C. R. (2018). "Better off, as judged by themselves": a comment on evaluating nudges. International Review of Economics, 65, 1-8. https://doi.org/10.1007/s12232-017-0280-9.

[SUN 15] Sunstein, C. R. (2015). Nudging and Choice Architecture: Ethical Considerations. Yale Journal on Regulation, Forthcoming. https://ssrn.com/abstract=2551264.

[SUP 15] Supiot, A. (2015). La gouvernance par les nombres. Fayard. ISBN : 9782213681092.

[SCH 03] Schiff, F. (2003). Business models of news Web sites: A survey of empirical trends and expert opinion. First Monday. https://doi.org/10.5210/fm.v8i6.1061.

[SEH 17] Sehl, A., Cornia, A. Nielsen, R. K., Simon, F. (2017). Pay Models in European News. Reuters Institute Digital News Publication. https://www.digitalnewsreport.org/publications/2017/pay-models-european-news/.

[SIN 20] Singh, S. (2020). Impact of neuromarketing applications on consumers. Journal of Business and Management, 26(2), 33-52. https://doi.org/10.6347/JBM.202009_26(2).0002.

[SOM 20] Soman, D. (2020). Sludge: A very short introduction. White paper. BEAR (Behavioral Economics in Action at Rotman). https://www.rotman.utoronto.ca/-/media/Files/Programs-and-Areas/BEAR/White-Papers/BEARxBIOrg-Sludge-Introduction.pdf/.

[STA 21] Stavrakakis, I., Curley, A., O'Sullivan, D., Gordon, D., & Tierney, B. (2021). A framework of web-based dark patterns that can be detected manually or automatically. https://doi.org/10.21427/20g8-d176.

[SWE 00] Sweeney L. (2000). Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. https://privacytools.seas.harvard.edu/sites/projects.iq.harvard.edu/files/privacytools/files/paper1.pdf.

[THA 18] Thaler, R. H. (2018). Nudge, not sludge. Science, 361(6401), p. 431. https://doi.org/10.1126/science.aau9241.

[THA 10] Thaler, R., Sunstein, C. (2010). Nudge. Comment inspirer la bonne décision. Vuibert. ISBN : 978-2-311-00105-1.

[VIS 21] 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. https://doi.org/10.21494/ISTE.OP.2021.0603.

[VIS 23] Viseur, R. (2023). Éthique de la gestion du consentement au traitement de données personnelles : une analyse au prisme des dark patterns. Actes du congrès INFORSID 2023, 133-148. http://inforsid.fr/actes/2023/Actes_INFORSID2023.pdf.

[WAL 20] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology, 31, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025.

[WES 19] Westin, F., & Chiasson, S. (2019). Opt out of privacy or" go home" understanding reluctant privacy behaviours through the FoMO-centric design paradigm. In Proceedings of the New Security Paradigms Workshop (pp. 57-67). https://doi.org/10.1145/3368860.3368865.

[WEI 16] Weinmann, M., Schneider, C., & Brocke, J. V. (2016). Digital nudging. Business & Information Systems Engineering, 58, 433-436. https://doi.org/10.1007/s12599-016-0453-1.

[WYL 19] Wylie, C. (2019). Mindfuck: Le complot Cambridge Analytica pour s'emparer de nos cerveaux. Grasset. ISBN : 978-2246824732.

[YOU 14] Young, S. W. (2014). Improving library user experience with A/B testing: Principles and process. Weave: Journal of Library User Experience, 1(1). https://doi.org/10.3998/weave.12535642.0001.101.

[ZAC 12] Zachrisson, J., Storrø, G., & Boks, C. (2012). Using a guide to select design strategies for behaviour change; Theory vs. Practice. In Design for Innovative Value Towards a Sustainable Society: Proceedings of EcoDesign 2011: 7th International Symposium on Environmentally Conscious Design and Inverse Manufacturing (pp. 362-367). Springer Netherlands. https://link.springer.com/chapter/10.1007/978-94-007-3010-6_70.

[ZIM 23] Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and enforceability of global privacy control. Proceedings on Privacy Enhancing Technologies, 2023(2). https://doi.org/10.56553/popets-2023-0052.

[ZUB 19] Zuboff S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs. ISBN : 978-1610395694.

