SciencesPo

CHAIR DIGITAL, GOVERNANCE AND SOVEREIGNTY

Comment l'Union européenne devrait-elle réglementer les interfaces truquées ?

Thomas Akhurst, Laura Zurdo

Riccardo Rapparini & Christoph Mautner Markhof

Approche comparative de la réglementation des grandes entreprises technologiques (printemps 2023)

Professeur Florence G'sell

avril 2023

Résumé

En novembre 2022, la législation sur les services numériques de l'Union européenne (UE), ou Digital Services Act (DSA), est entrée en vigueur. Elle impose de nouvelles obligations aux intermédiaires en ligne afin de protéger les droits fondamentaux des utilisateurs en ligne. Parmi une série de règles, l'article 25 établit une interdiction des interfaces truquées, ou *dark patterns*. Cette note politique analyse l'approche de la loi sur les services numériques à l'égard des "dark patterns" (en français : interfaces truquées) à travers la question de recherche suivante :

"Comment l'interdiction des interfaces truquées prévue par la loi sur les services numériques doit-elle être mise en œuvre ?

Après avoir présenté le contexte politique dans la section 1 et fourni une analyse descriptive du DSA et de ses antécédents en ce qui concerne les interfaces truquées dans la section 2, la section 3 analysera quatre questions pertinentes pour la mise en œuvre de l'article 25. Ces conclusions visent à orienter la mise en œuvre de l'article 25 de la législation sur les services numériques par la Commission européenne (CE ou Commission), en mettant en évidence quatre domaines que la Commission doit aborder, que ce soit par le biais de lignes directrices sur l'article 25 et/ou d'actes délégués. La discussion sera structurée selon la logique des cercles concentriques, s'étendant d'une perspective étroite à une perspective large. La première question abordée, celle des "définitions juridiques", explore les incertitudes liées aux termes dans l'article. La deuxième question, celle de la "portée juridique", s'étend sur l'article 25 afin d'évaluer la manière dont il pourrait interagir avec la réglementation préexistante sur les interfaces truquées, en particulier le règlement général sur la protection des données (RGPD) et la directive sur les pratiques commerciales déloyales (DPCD). Notre troisième question dépasse la dimension juridique pour s'intéresser aux implications pratiques de la mise en œuvre, à savoir, de quelle manière l'article 25 influe sur les *personnes chargées de* faire respecter les interdictions relatives aux interfaces truquées et sur *la manière dont* elles le font. La quatrième question adopte une vision holistique du DSA, en explorant les dispositions en dehors de l'article 25 qui pourraient être utilisées pour lutter contre les interfaces truquées. Enfin, la dernière section présente une série de recommandations.

1. Clarifier les termes : (i) la personnalisation manipulatrice de l'interface serait mieux traitée en renforçant la protection des données du RGPD, (ii) un effet trompeur *potentiel* devrait être suffisant pour satisfaire à l'article 25 (iii) la norme utilisée pour évaluer si une pratique est susceptible de tromper devrait être inférieure à celle du consommateur moyen, afin de tenir compte des asymétries numériques.

2. Clarifier le champ d'application : définir l'interaction entre les champs d'application du DSA, de la DPCD et du RGPD.
3. Coordonner l'application de la législation, en particulier entre les coordinateurs du service numérique et les autorités chargées de la protection des consommateurs.
4. Exploiter toute la "boîte à outils" du DSA, car il existe d'autres dispositions du DSA qui peuvent être utilisées pour lutter contre les interfaces truquées, au-delà de l'interdiction prévue à l'article 25.

Table des matières

1.1. Contexte - les interfaces truquées en tant que question politique

Les "dark patterns" (*interfaces truquées*) constituent une menace sérieuse et omniprésente pour les principes démocratiques libéraux fondamentaux. Inventé par le designer Harry Brignull en 2010 (Sinders, 2021), ce terme désigne les conceptions d'interface en ligne qui visent à manipuler les utilisateurs pour qu'ils agissent à l'encontre de leurs propres intérêts, généralement au profit du fournisseur du site web ou de l'application en question (Luguri & Strahilevitz, 2021). Bien que le terme soit vaguement défini, l'action réglementaire contre les interfaces truquées trouve son origine dans l'intuition que les individus devraient être libres d'évaluer et de définir leurs propres intérêts dans une société démocratique. La démocratie repose sur la décentralisation du pouvoir et la protection des droits individuels, mais les interfaces truquées transforment les interfaces en ligne en architectures biaisées qui privilégient et amplifient les intérêts des plateformes en ligne. La loi sur les services numériques (LSN) reflète ces sentiments et vise à garantir un "environnement en ligne (qui protège) [...] les droits fondamentaux [...] en particulier la liberté d'expression, [...] le droit à la non-discrimination et [...] un niveau élevé de protection des consommateurs" (considérant 3). L'action contre les interfaces truquées est donc un élément constitutif important de l'effort plus large visant à construire une société numérique adaptée à la démocratie libérale.

Les interfaces truquées ont été interdites par divers instruments législatifs de l'UE, notamment la directive sur les pratiques commerciales déloyales (DPCD) et le règlement général sur la protection des données (RGPD). La principale raison d'être de la réglementation des interfaces truquées est représentée par le droit au respect de la vie familiale (article 7 de la Charte de l'UE), qui sous-tend la protection de l'autonomie individuelle (Gumbis et al., 2008) - ou la capacité d'aligner ses actions sur ses véritables préférences (Yeung, 2017). Cependant, leur présence est loin d'être évitée. La Commission européenne et le Réseau européen de protection des consommateurs ont récemment passé au crible des sites web de vente au détail, en se concentrant sur trois types de interfaces truquées, et ont constaté que 40 % des détaillants contrôlés les utilisaient (Commission européenne, 2023). Dans une autre étude, la Commission européenne a constaté que 97 % des sites web et des applications les plus populaires utilisés par les consommateurs de l'UE déployaient au moins une interface truquée (Lupiáñez-Villanueva et al., 2022).

Certains critiques affirment que les interfaces truquées persistent parce que la réglementation en la matière s'est généralement concentrée sur des caractéristiques "statiques" (c'est-à-dire des caractéristiques d'interface facilement observables qui ne sont pas personnalisées pour les utilisateurs), alors que la manipulation en ligne est de

plus en plus "dynamique" (c'est-à-dire qu'elle résulte de l'utilisation de données pour personnaliser les interfaces d'une manière qui manipule le comportement de l'utilisateur) (Yeung, 2017). Dans le même ordre d'idées, certains affirment que l'UE a besoin d'une réglementation supplémentaire mieux adaptée à l'ère numérique (BEUC, 2022). D'autres ont rétorqué que la raison pour laquelle les interfaces truquées prévalaient dans l'UE était principalement due à des déficiences dans l'application du cadre, plutôt qu'à un manque de réglementation (Ecommerce Europe, 2022). Une chose est sûre, les interfaces truquées incarnent une caractéristique permanente, importante et de plus en plus problématique de la vie en ligne.

C'est dans ce contexte qu'une nouvelle interdiction des interfaces truquées est entrée en vigueur par le biais de l'article 25 du DSA. L'étape suivante et la tâche la plus urgente dans le contexte de la réglementation numérique européenne des interfaces truquées consiste à déterminer la meilleure façon de mettre en œuvre le DSA. Cette note politique analyse cette question, en soulignant quatre domaines que la Commission européenne doit aborder pour exploiter au mieux le potentiel du DSA en ce qui concerne la restriction des interfaces truquées. La Commission est la mieux placée pour recevoir ces recommandations, étant donné sa capacité à produire des lignes directrices sur l'interdiction de l'article 25 (article 25(3) du DSA).

2.2. Cadre juridique - comment l'UE a-t-elle réglementé les interfaces truquées ?

Le DSA n'est pas le premier acte législatif de l'UE à interdire les interfaces truquées. Cette section présente les principales dispositions du droit communautaire utilisées pour les combattre, en passant en revue les instruments juridiques qui ont précédé le DSA avant d'analyser son ajout, l'article 25 du DSA.

2.1. Avant la loi sur les services numériques

Avant le DSA, la législation de l'UE abordait les interfaces truquées principalement par le biais de la législation sur la protection des données et des consommateurs. En particulier, le règlement général sur la protection des données (RGPD) et la directive sur les pratiques commerciales déloyales (DPCD) ont joué un rôle prépondérant, bien qu'aucun de ces textes ne mentionne expressément les interfaces truquées.

2.1.1. Règlement général sur la protection des données (RGPD)

Le RGPD[1] réglemente la protection des données personnelles, définies comme "toute information relative à une personne physique identifiée ou identifiable". Il

s'applique à tous les traitements de données à caractère personnel effectués par des responsables du traitement ou des sous-traitants qui proposent des biens ou des services à des personnes dans l'UE ou qui surveillent leur comportement. En ce sens, le RGPD s'applique quel que soit le lieu d'établissement du responsable du traitement, à l'intérieur ou à l'extérieur de l'UE. Le règlement confère également aux personnes concernées un ensemble de droits, en particulier le droit à l'information et le droit de contrôler la manière dont leurs données sont traitées.

Les activités de traitement des données doivent être loyales (article 5, paragraphe 1, point a), du RGPD) et fondées sur l'un des six motifs de traitement légitime prévus par le règlement (article 6, paragraphe 1). L'un des motifs de traitement légitime est le consentement de la personne concernée. En vertu de l'article 4, paragraphe 11, du RGPD, pour obtenir le consentement légitime d'une personne concernée, le consentement doit être libre, spécifique, éclairé et univoque. Toutefois, les responsables du traitement ont souvent conçu des interfaces utilisateur déroutantes qui empêchent la personne concernée de donner son consentement librement et légitimement (Sinders, 2021), ce qui va à l'encontre de l'article 4, paragraphe 1, du RGPD et du principe général d'équité énoncé à l'article 5 du RGPD (Commission européenne, 2021).

Pour empêcher ces pratiques, le RGPD *interdit les interfaces en ligne visant à induire l'utilisateur en erreur et à l'amener à accepter un traitement plus important que ce qui est dans son intérêt* (Luguri & Strahilevitz, 2021). Par exemple, la Cour de justice des Communautés européennes (CJCE) a estimé qu'une case pré-cochée ne peut constituer un consentement valable (affaire C-673/17 *Planet49 GmbH*). De même, le consentement n'est pas valable si la possibilité de s'opposer à la collecte et au stockage des données est "indûment affectée" par la nécessité de "remplir un formulaire supplémentaire exposant ce refus". En d'autres termes, les options "oui" et "non" d'un formulaire de cookie doivent être également accessibles (Cour de justice des Communautés européennes, affaire C-61/19 *Orange Romania*, paragraphe 53).

Par ailleurs, le Conseil européen de la protection des données (EDPB, 2022) a adopté des lignes directrices sur les interfaces truquées dans les interfaces des plateformes de réseaux sociaux, qui définissent les meilleures pratiques pour les concepteurs. Ces lignes directrices définissent six catégories de modèles qui enfreignent le RGPD : le fait de surcharger (submerger les utilisateurs d'informations ou de possibilités volumineuses), de sauter (inciter les utilisateurs à négliger ou à oublier des considérations pertinentes en matière de protection de la vie privée), de susciter une décision (faire appel aux émotions ou utiliser des incitations visuelles pour façonner les choix), d'entraver (rendre la gestion des données difficile ou impossible), d'être inconstant (des interfaces peu claires conçues pour semer la confusion chez l'utilisateur), et le fait de laisser dans l'obscurité (cacher des informations pertinentes ou des outils de protection des données).

2.1.2. Directive sur les pratiques commerciales déloyales

En droit communautaire, la directive DPCD[2] fournit le cadre général de la réglementation des pratiques commerciales dans les relations entre *entreprises et consommateurs* (B2C), en interdisant les pratiques jugées déloyales. La DPCD s'applique à un large éventail de pratiques mises en œuvre par tout professionnel impliqué dans la promotion, la vente ou la fourniture d'un produit ou d'un service aux consommateurs (article 2, point d), de la DPCD). D'une part, un professionnel est toute personne physique ou morale qui agit en son nom propre à des fins liées à son activité, ou toute personne agissant pour le compte d'un professionnel (article 2(b) de la DPCD). Les organisations caritatives et les autorités publiques peuvent être des professionnels lorsqu'elles exercent des activités commerciales à l'égard des consommateurs, comme une ONG qui vend des produits répondant à certaines normes éthiques (Commission européenne, 2021, p. 28). D'autre part, un consommateur est "une personne physique qui [agit] en dehors du cadre d'une activité économique (commerce, entreprise, artisanat, profession libérale)" (article 2(a) de la DPCD).

Une pratique commerciale peut aller d'une action à une omission, voire à des communications telles que le marketing. Elle peut avoir lieu avant, pendant ou après une transaction commerciale. Ainsi, la DPCD ne nécessite pas d'achat ou de relation contractuelle, dès lors que la pratique est directement liée à la promotion d'un produit ou d'un service auprès des consommateurs (Commission européenne, 2021). Pour être considérée comme déloyale, la pratique doit être *susceptible d'amener un consommateur à prendre une décision transactionnelle qu'il n'aurait pas prise autrement*. Les décisions transactionnelles comprennent, outre les achats, tout autre choix directement lié à ceux-ci, comme le choix d'entrer dans un magasin (Cour européenne de justice, affaire C-281/12, *Trento Sviluppo srl*, paragraphe 35). Les pratiques déloyales peuvent survenir si elles violent la diligence professionnelle du professionnel (article 5 de la DPCD), si elles sont trompeuses (article 6 de la DPCD) ou si elles sont agressives (articles 8 et 9). Les pratiques trompeuses cachent ou présentent des informations d'une manière qui conduit les consommateurs à prendre une décision qu'ils n'auraient pas prise autrement. À l'inverse, les pratiques agressives impliquent un harcèlement ou une coercition. Dans tous les cas, l'intention de tromperie du professionnel n'est pas requise.

Pour appliquer la DPCD, les autorités de contrôle vérifient si la pratique figure sur la liste noire de l'annexe I. Si ce n'est pas le cas, elles l'évaluent au cas par cas. Comme nous l'avons mentionné, la question clé est la probabilité que la pratique conduise les consommateurs à prendre une décision transactionnelle non souhaitée. En règle générale, les pratiques commerciales sont évaluées du point de vue du consommateur moyen, qui est "raisonnablement bien informé, attentif et avisé" (Cour de justice des Communautés européennes, affaire C-210/96, *Gut Springenheide et Tusky*,

paragraphe 31). 31). Toutefois, une pratique ciblant un consommateur vulnérable est évaluée de son point de vue spécifique. La vulnérabilité peut résulter de caractéristiques permanentes telles que l'âge, l'infirmité mentale ou physique, ou dépendre du contexte (Commission européenne, 2021, p. 35).). Par exemple, le caractère déloyal d'une pratique ciblant les enfants est évalué en tenant compte du fait que les enfants traitent l'information différemment (ACM, 2022, p. 15).

LA DPCD est technologiquement neutre et s'applique aussi bien hors ligne qu'en ligne. Les lignes directrices de la Commission pour 2021 sur la DPCD évaluent son application aux environnements numériques. Il est important de noter que les pratiques dans les *relations B2C où les clients n'effectuent pas de paiement monétaire mais qui génèrent un autre avantage pour le commerçant, comme la monétisation des données des utilisateurs, relèvent des pratiques commerciales* (ACM, 2022, p. 14). Les décisions transactionnelles des clients dans la sphère en ligne comprennent le choix d'accéder à un site web, de continuer à utiliser un service (par exemple, le défilement de flux), de cliquer sur un lien ou de voir des publicités (Commission européenne, 2021, p. 100).

Les lignes directrices consacrent une section aux pratiques déloyales, notant que les pratiques déloyales dans une relation B2C peuvent être contestées en vertu de la DPCD. L'annexe 1 dresse directement une liste noire de certaines pratiques déloyales, notamment l'appât et l'échange, les fausses déclarations de stocks limités, les fausses minuteries et le harcèlement. Pour les autres pratiques, la logique générale de la directive s'applique : une pratique *trompeuse est une* pratique obscure si elle cache des informations pertinentes ou les fournit d'une manière qui amène le consommateur à prendre une décision qu'il n'aurait pas prise en l'absence de cette pratique. À l'inverse, elle est *agressive* si elle entrave de manière significative la liberté de choix des consommateurs, en les contraignant ou en les influençant indûment, ce qui les amène à prendre une décision non souhaitée. Par exemple, l'interface en ligne d'un professionnel qui rend la résiliation d'un contrat plus difficile que sa conclusion (par exemple, cachée derrière plusieurs écrans ou des options déroutantes) constituerait une forme sombre interdite (Commission européenne, 2021, p. 102). De même, une interface truquée qui dissimule des frais de réservation supplémentaires inévitables constitue une pratique commerciale trompeuse, interdite en vertu de la DPCD (Dutch Trade and Industry Appeals Tribunal, Case 17/1179 *ACM/Corendon*).

2.1.3. Autres

Outre le RGPD et la DPCD, d'autres instruments font directement ou indirectement référence aux interfaces truquées. Tout d'abord, la *directive sur les clauses contractuelles abusives*[3] protège les consommateurs contre les clauses contractuelles abusives et non négociées individuellement. Un contrat peut être annulé

si ses clauses sont présentées de manière peu claire, en utilisant des interfaces truquées pour semer la confusion par le biais d'interférences visuelles (BEUC, 2022, p. 11). De même, la *directive sur les droits des consommateurs* exige que les consommateurs soient en mesure de comprendre les conséquences de la conclusion d'un contrat (BEUC, 2022, p. 9). En outre, en vertu de la *directive "vie privée et communications électroniques"* ([4]), les consommateurs doivent consentir à l'installation de cookies dans leur équipement terminal, et des interfaces trompeuses peuvent empêcher l'obtention d'un consentement légitime (Commission européenne, 2022, p. 75).

La législation récente et à venir peut également être pertinente. Par exemple, l'article 7 de la *loi sur les marchés numériques (DMA)* interdit aux gardiens d'utiliser des interfaces truquées pour contourner leurs obligations en matière de DMA. Par ailleurs, l'article 5, paragraphe 1, point a), de la proposition de *loi sur l'intelligence artificielle (AI)* interdit également l'utilisation de systèmes d'intelligence artificielle pour *déployer des "techniques subliminales* (...) *afin de déformer matériellement le comportement* [des utilisateurs]*",* susceptibles de leur causer un préjudice.

2.2. L'interdiction du DSA : Article 25

Le 1er novembre 2022, la loi sur les services numériques de l'UE est entrée en vigueur. La loi sur les services numériques réglemente la fourniture de services intermédiaires en ligne dans l'UE, ce qui a un impact sur la réglementation des interfaces truquées. En particulier, l'article 25 de la loi sur les services numériques interdit l'utilisation par les plateformes en ligne d'interfaces trompeuses ou manipulatrices, un terme qui - comme l'illustre le considérant 67 - englobe les interfaces truquées. Cette interdiction ne figurait pas dans la proposition initiale de la Commission. Toutefois, elle a été ajoutée par le Conseil et le Parlement au cours des négociations du trilogue (BEUC, 2022, p. 12).

Sous la rubrique "conception et organisation de l'interface en ligne", l'article 25, paragraphe 1, du DSA interdit aux plateformes en ligne de *"concevoir, organiser ou exploiter leur interface en ligne d'une manière qui trompe ou manipule les destinataires de leur service ou d'une manière qui fausse ou compromet d'une manière significative la capacité des destinataires du service à prendre des décisions libres et éclairées".* L'article 25 fournit trois exemples spécifiques :

- " Donner plus d'importance à certains choix lorsqu'on demande au destinataire [...] de prendre une décision ",
- " Demander de manière répétée à leur destinataire [...] de faire un choix alors que ce choix a déjà été fait ", et

- " Rendre la procédure de résiliation d'un service plus difficile que la souscription à ce service ".

Notamment, les mots "interfaces truquées" n'apparaissent pas dans l'article lui-même. Néanmoins, le considérant 67 qui l'accompagne précise que l'interdiction les inclut. Ce considérant définit les "dark patterns" comme les "structure(s), design(s) ou fonctionnalités" des "*interfaces en ligne des plateformes en ligne* [qui] *faussent ou altèrent matériellement, que ce soit dans leur but ou dans leur effet, la capacité des destinataires à faire des choix ou à prendre des décisions de manière autonome et informée". [*Elles *peuvent être utilisées pour persuader les destinataires du service d'adopter des comportements ou des décisions non désirés qui ont des conséquences négatives pour eux".* Le considérant 67 énumère également plusieurs exemples spécifiques de modèles interdits :

- " Donner plus d'importance à certains choix ",
- " Demander de manière répétée à un destinataire du service de faire un choix alors que ce choix a déjà été fait ",
- " Rendre la procédure de résiliation d'un service nettement plus lourde que l'inscription à ce service",
- " Rendre certains choix plus difficiles ou plus longs que d'autres ",
- " Rendre déraisonnablement difficile l'interruption des achats ou la déconnexion d'une plateforme en ligne donnée", et
- " Paramètres par défaut très difficiles à modifier".

2.2.1. Un champ d'application subjectif - à qui l'interdiction s'applique-t-elle ?

L'interdiction des interfaces truquées ne s'étend qu'aux *plateformes en ligne*, définies comme des prestataires de services intermédiaires qui hébergent des informations générées par les utilisateurs et les diffusent au public à la demande de ces derniers (article 3, point i), de l'accord sur les services de défense des intérêts des consommateurs, considérant 13). Il y a diffusion publique lorsque ces informations sont mises à la disposition d'un nombre potentiellement illimité de personnes, indépendamment du nombre de personnes qui y accèdent effectivement (considérant 14). L'interdiction s'applique quel que soit le lieu d'établissement de la plateforme, dès lors qu'elle fournit des services à des utilisateurs dans l'UE (article 2, paragraphe 1). Néanmoins, pour éviter d'imposer des obligations disproportionnées, l'interdiction ne s'applique pas aux micro ou petites entreprises (article 19), ni aux intermédiaires qui ne diffusent publiquement le contenu des utilisateurs qu'à titre accessoire (article 3, point i)). À l'autre extrémité se trouvent les *"destinataires du service"*, qui peuvent être

toutes sortes d'utilisateurs, y compris des consommateurs et des utilisateurs professionnels (article 3, point b), considérant 2).

2.2.2. Un champ d'application objectif - quel comportement interdit-il ?

DSA interdit les choix de conception ou les expériences d'interface utilisateur sur les plateformes en ligne qui manipulent ou trompent les utilisateurs d'une manière qui *porte atteinte à leur autonomie*. En faisant de l'autonomie son critère de référence, l'article 25 vise les pratiques qui *incitent un destinataire à faire un choix contraire à ses préférences* ou qui *entravent l'*exercice de l'autonomie de telle sorte que l'utilisateur n'est pas en mesure de définir ses propres préférences. Les intermédiaires peuvent entraver les choix des utilisateurs par "la structure, la conception ou les fonctionnalités d'une interface en ligne" (considérant 67), et l'article 25 interdit donc la manipulation "de la conception, de l'organisation et du fonctionnement" de ces interfaces.

Un autre élément de la conduite interdite est que son effet de tromperie ou de manipulation des destinataires doit être *"important".* DSA elle-même ne précise pas si l'effet doit être réel ou si un effet *potentiel* peut suffire. Elle ne précise pas non plus ce qu'est la matérialité. Une question connexe est de savoir quel devrait être le critère applicable au destinataire lorsqu'il s'agit d'évaluer si une pratique est trompeuse : quel doit être le degré d'intelligence du destinataire ? Faut-il utiliser le critère du "consommateur moyen" de la DPCD ? Enfin, l'article 25, paragraphe 2, précise que l'interdiction des ASD *ne s'applique pas aux pratiques couvertes par le RGPD et la DPCD*. La question se pose donc de savoir quel est le champ d'application de l'interdiction des ASD. Ces questions cruciales seront examinées à la section 3.

2.2.3. La mise en œuvre - comment sera-t-elle mise en œuvre ?

Comme le prévoit l'article 38 de la loi sur les services numériques, chaque État membre nomme son propre coordinateur des services numériques (CSN), qui est responsable de l'application des dispositions de la loi. Le CSN agit indépendamment des autres autorités ou parties privées (article 39) et exerce sa surveillance sur les plateformes établies dans l'État membre concerné (article 40).

Les CSD nationaux se voient confier trois types de pouvoirs différents, à savoir l'enquête, l'exécution et d'autres pouvoirs tels que la demande d'injonctions (Cauffman & Goanta, 2021). Leur pouvoir d'exécution se traduit par l'autorité de conclure des accords de conformité, d'imposer des amendes et d'autres mesures provisoires (*ibid.*). En outre, l'ASN prévoit la création d'un Conseil européen des services numériques qui conseille les CSD nationaux (article 47). Les compétences en matière d'enquête et d'imposition de sanctions sont également conférées à la Commission européenne dans le contexte des très grandes plateformes en ligne (VLOP) (article 51). Ainsi, tant la Commission que les coordinateurs de service numérique peuvent effectuer des

inspections sur place, demander des données aux plateformes et mener des entretiens (*ibid.)*.

L'application du DSA repose sur l'imposition d'amendes destinées à dissuader les entreprises de ne pas respecter la loi. Les sanctions doivent être déterminées par le droit national, avec un plafond maximum de 6 % des recettes annuelles totales (article 42, paragraphe 3). Dans des cas spécifiques, d'autres types d'amendes peuvent être imposés, tout en étant soumis à des limites imposables déterminées par le DSA. En outre, des amendes peuvent être imposées par la Commission européenne, à l'image de ce système (article 59).

Outre les sanctions en cas de non-respect, il existe également des mécanismes visant à renforcer la conformité des VLOP et des VLOSE. Parmi ceux-ci, il y a l'obligation de nommer un responsable de la conformité (article 41), ainsi que de réaliser des audits annuels indépendants (article 37). En outre, la Commission peut demander aux VLOP de définir et de partager un plan d'action visant à garantir le respect des règles du DSA (article 75). Les codes de conduite volontaires au niveau de l'Union font également partie de l'application du DSA, et leur création et leur définition sont soutenues à la fois par la Commission et par le Conseil européen des services numériques, conformément à l'article 45. Dans ce contexte, les codes de conduite visent à garantir une application cohérente du cadre en favorisant l'harmonisation réglementaire.

3.3. Questions phares de l'article 25 du DSA

Cette section présente quatre questions clés que la Commission européenne devrait aborder pour maximiser le potentiel du DSA, en particulier de l'article 25, dans la lutte contre les interfaces truquées. Premièrement, cette section examine les incertitudes liées à certains termes juridiques. Deuxièmement, elle met en évidence les questions non résolues du champ d'application juridique de l'article 25, à savoir les incertitudes relatives à l'interaction du DSA avec la DPCD et le RGPD. Troisièmement, nous abordons les défis liés à l'application de la loi. Enfin, l'article 25 n'étant qu'une des nombreuses dispositions du DSA, ce mémoire envisage des possibilités potentiellement négligées d'utiliser DSA dans son ensemble (comme une "boîte à outils") pour s'attaquer aux interfaces truquées. La Commission est dans une position idéale pour aborder ces questions, étant donné sa capacité à publier des lignes directrices sur l'interdiction de l'article 25 (article 25, paragraphe 3, du DSA).

La présente note d'orientation considère que la mise en œuvre est optimale si elle répond à trois objectifs connexes :

i. Garantir un *cadre juridique européen cohérent* sur les interfaces truquées et une *sécurité juridique* sur la manière dont les instruments réglementaires interagissent (*questions 1* et *2)*.

ii. Assurer l'*application effective* de ce cadre, y compris l'article 25 (*question 3)*.

iii. Maximiser l'*utilité* du DSA en ce qui concerne les interfaces truquées, en mettant en évidence d'autres articles qui peuvent être utilisés pour les combattre (*numéro 4*).

Ces objectifs doivent être considérés comme des conditions nécessaires pour assurer la durabilité et l'efficacité du cadre juridique de l'UE. DSA faisant partie de l'acquis juridique de l'UE, ses dispositions et les effets qui en découlent doivent s'inscrire dans le cadre juridique plus large de l'UE. Ce n'est qu'ainsi que les objectifs de l'UE, notamment la promotion du marché unique et la protection des droits des citoyens de l'UE (article 3 du traité sur l'Union européenne), peuvent être atteints. En outre, étant donné le rôle du DSA dans la réalisation de la vision de la Commission pour l'avenir numérique de l'Europe, sa mise en œuvre doit être alignée sur la déclaration solennelle interinstitutionnelle sur les droits numériques et les principes pour la décennie numérique. Dans ce contexte, il est essentiel de garantir la cohérence juridique et l'application effective des principes "l'être humain au centre", "la liberté de choix" et "la sûreté et la sécurité" (Commission européenne, 2022).

3.1. Définitions juridiques

Il existe trois incertitudes principales en matière de définition qui créent chacune leurs propres risques ou questions pertinentes. Premièrement, les termes "conception, fonctionnement et organisation de l'interface" - la définition des interfaces en ligne interdites de l'article 25 - sont vagues et pourraient être interprétés comme englobant des aspects de l'architecture en ligne qui n'ont pas été traditionnellement traités comme des interfaces truquées. Deuxièmement, il n'est pas clair si l'interdiction du DSA inclut la tromperie potentielle, ainsi que la tromperie réelle. Troisièmement, la norme relative au destinataire n'est pas claire ; selon quelle norme l'ASN évaluera-t-elle les interfaces comme étant manipulatrices et/ou trompeuses ?

3.1.1. Conduite interdite : couvre-t-elle la manipulation par la personnalisation de l'interface ?

Comme l'a montré la section 1, la plupart des approches des formes sombres se sont limitées, par définition, à des caractéristiques d'interface relativement observables. Il peut s'agir de la présentation égale des options "oui" et "non" sur les formulaires de consentement aux cookies, ou des comptes à rebours qui créent une fausse impression d'urgence pour encourager les achats. Toutefois, les critiques soutiennent

que cette approche ne tient pas compte des formes émergentes de manipulation de l'utilisateur qui se produisent par le biais de la personnalisation de l'interface. Elle a suscité des appels à une compréhension élargie des pratiques manipulatrices, certains estimant que la question ne devrait plus être abordée sous l'angle des "interfaces truquées" mais dans le cadre de conceptualisations plus larges telles que les architectures de choix en ligne manipulatrices (Ecommerce Europe, 2022), afin de tenir compte de pratiques plus dynamiques telles que les algorithmes comportementaux.

Les interfaces personnalisées manipulatrices s'appuient sur la science du comportement pour cibler les préjugés individuels, incitant les utilisateurs à agir contre leurs propres intérêts au profit de l'entreprise concernée. La nouveauté de la manipulation par la personnalisation de l'interface et de l'UX réside dans le fait qu'elle n'est pas observable à l'œil nu. Comme l'explique le Bureau européen des unions de consommateurs (BEUC), "l'utilisation de la technologie et de l'expérimentation comportementale sur l'architecture des choix... associée à la collecte de grandes quantités de données révélant les caractéristiques les plus personnelles des consommateurs, permet aux entreprises d'identifier quelle décision conduit à quel changement dans le comportement de l'utilisateur" (2022, p. 4). L'*étude comportementale de* la Commission européenne *sur les pratiques commerciales déloyales dans l'environnement numérique* a révélé que "la combinaison de schémas classiques et de techniques de personnalisation... (est) une nouvelle frontière... conduisant à des pratiques commerciales plus difficiles à reconnaître et à réglementer" (2022, p. 60).

Les approches existantes des interfaces truquées - qui tendent à se concentrer sur les aspects statiques ou observables de la conception de l'interface - sont mal équipées pour aborder la manipulation par le biais de la personnalisation de l'interface. Dans le cadre de la DPCD, cette limitation est incarnée par le fait qu'elle suppose une norme de consommateur moyen divergeant des réalités de "l'asymétrie numérique" (BEUC, 2022, p. 9). Cette norme ne reconnaît pas les effets intrinsèquement manipulateurs des "algorithmes (utilisés) par les entreprises pour cibler leur architecture de choix sur un consommateur (d'une manière qui façonne) la prise de décision individuelle" (BEUC, p. 4). De plus, en faisant peser la charge de la preuve sur le plaignant, la DPCD rend difficile la poursuite des pratiques de personnalisation qui ne sont connues que des entreprises ou cachées derrière l'opacité algorithmique. La Commission européenne elle-même a fait valoir que des changements législatifs étaient nécessaires "malgré l'existence d'un cadre juridique européen solide (...) pour mieux répondre aux interfaces truquées et à la personnalisation manipulatrice" (Lupiáñez-Villanueva et al., 2022, p. 7).

Dans cette optique, la formulation de l'article 25 et de son considérant associé peut être interprétée de manière à englober les pratiques dynamiques émergentes. Bien que les exemples interdits décrits explicitement à l'article 25 s'alignent sur la définition

statique traditionnelle des formes sombres, il convient de noter que l'article n'adopte pas le terme "formes sombres". Il opte plutôt pour la terminologie plus large d'"interface et conception en ligne". Par conséquent, l'intention de l'article 25 n'est pas claire lorsqu'il stipule que "...les plateformes en ligne ne *conçoivent, n'organisent ni n'exploitent* leurs interfaces en ligne de manière à tromper ou à manipuler..." (article 25, paragraphe 1, de l'accord de service de consultation en ligne). Dans le même ordre d'idées, qu'entend le considérant 67 lorsqu'il fait référence à l'interdiction de "la *structure, la conception ou les fonctionnalités* d'une interface en ligne" ? Ces termes ("conception", "organisation", "exploitation", "structure" et "fonctionnalités") peuvent être interprétés de manière large, au-delà des caractéristiques statiques de l'interface, comme des interfaces truquées dynamiques basés sur la personnalisation.

Étant donné que l'interdiction de l'article 25 a été mise en œuvre pour combler les "lacunes" dans la réglementation des pratiques commerciales déloyales, il est plausible que le DSA ait l'intention de considérer la personnalisation manipulatrice de l'interface comme une pratique commerciale déloyale. Comme indiqué ci-dessus, l'interdiction du DSA ne se réfère pas seulement à la conception et aux fonctionnalités d'une interface en ligne, mais aussi aux opérations et aux structures qui trompent et/ou manipulent. L'accent mis par le DSA sur la manipulation et l'autonomie est également instructif, car il s'agit de conséquences primordiales de la personnalisation de l'interface. Néanmoins, ces questions ne sont pas clarifiées.

3.1.2. Effet trompeur : réel ou potentiel ?

Comme indiqué, l'article 25 ne précise pas si l'effet de tromperie de l'utilisateur doit être réel ou potentiel. Dans le cadre de la réglementation des "dark patterns" antérieure à le DSA, un effet potentiel était suffisant. Comme indiqué à la section 2.1, la DPCD n'exige pas de démontrer qu'un consommateur a été effectivement trompé, mais seulement de prouver que le motif était susceptible d'avoir cet effet. Étant donné que la DPCD et le DSA ont pour objectif commun d'éliminer les formes sombres, elles pourraient être interprétées de manière complémentaire. En d'autres termes, l'ASN pourrait partager l'approche de la DPCD selon laquelle la tromperie réelle et la tromperie potentielle sont toutes deux soumises à l'interdiction. Une interprétation complémentaire permettrait également de déterminer l'intention de l'article 25 lorsqu'il stipule que la conception du système ou l'interface utilisateur doit fausser *matériellement* le choix de l'utilisateur, étant donné qu'une exigence de matérialité existe également dans la directive sur les pratiques commerciales déloyales. Dans ce cas, les lignes directrices de la CE montrent qu'en vertu de la DPCD, la pratique doit être *susceptible d'amener* le destinataire à prendre une décision qu'il n'aurait pas prise autrement (Commission européenne, 2021, p. 31).

3.1.3. Une norme relative au destinataire : consommateur moyen ou utilisateur vulnérable ?

Le texte de l'article 25 ne précise pas quel critère de réception sera utilisé pour déterminer si un modèle est susceptible de tromper les utilisateurs. Dans ce cas, une approche complémentaire avec la DPCD pourrait également être envisagée. Cela impliquerait d'utiliser le *consommateur moyen* comme norme générale, sauf lorsqu'une pratique vise un groupe vulnérable particulier (voir section 2.1).

La Commission pourrait également adopter une approche différente de celle de la DPCD en clarifiant la définition d'une norme de destinataire dans le DSA. Dans ce cas, les critiques du droit européen de la consommation évoquées plus haut sont pertinentes. Une fois de plus, le problème découle de l'utilisation d'un critère de "consommateur moyen" qui ne tient pas compte de l'asymétrie numérique entre les parties dans les interfaces truquées (Helberger et al., 2021 ; BEUC, 2022). Le BEUC a donc proposé de modifier la norme pour tenir compte de la vulnérabilité de la partie la plus faible. Le BEUC note que "le professionnel a accès au profil personnel détaillé du consommateur, y compris à ses biais décisionnels. [Simultanément, le professionnel contrôle et façonne l'ensemble de l'environnement dans lequel le consommateur opère". Dans ces conditions, "tous les consommateurs numériques sont rendus vulnérables" (BEUC, 2022, p. 10) et universellement susceptibles "d'être exploités par des déséquilibres de pouvoir" (Helberger et al., 2021, p. 1). Dans ce cas, "la vulnérabilité en tant qu'exception devient moins utile pour évaluer la distorsion comportementale qu'une interface peut provoquer" (BEUC, 2022, p. 10). Bien que les critiques du BEUC aient été formulées dans le contexte de la DPCD, elles peuvent éclairer l'analyse de la Commission sur la norme de destinataire appropriée dans le cadre de l'article 25 du DSA.

L'abaissement du critère de destinataire du DSA en dessous du critère actuel du "consommateur moyen" de la DPCD allégerait la charge de la preuve pour démontrer que le choix de conception d'une plateforme constitue un motif d'obscurité illégal. Il existe une base établie pour cela dans le DSA, étant donné que l'Acte articule expressément un objectif central de lutte contre les asymétries d'information entre les utilisateurs et les plateformes, et de renforcement de l'action des citoyens et des entreprises lorsqu'ils interagissent avec les environnements des plateformes (analyse d'impact du DSA, paragraphes 90 et 217). Le considérant 67 reconnaît lui-même que les interfaces truquées s'appuient souvent sur des biais comportementaux, ce qui pourrait rendre l'idée d'un consommateur rationnel et attentif incompatible avec les réalités des interfaces truquées. Même dans le domaine du droit de la consommation, la Commission semble s'orienter vers une reconnaissance de ces asymétries.[5] Toutefois, les observateurs ne sont pas tous d'accord. Les sceptiques ont mis en garde contre un assouplissement illimité des normes juridiques, citant la difficulté de distinguer la persuasion légitime de la manipulation illégitime. Ils avertissent que "si tout est un modèle sombre, alors rien n'est un modèle sombre" (Goanta & Santos, 2023, n.d.).

3.2. Le champ d'application juridique

Une réglementation efficace des interfaces truquées nécessite également une sécurité juridique. À ce titre, la Commission doit d'urgence clarifier le champ d'application des éléments clés du cadre juridique. Actuellement, l'interaction entre le DSA et les instruments juridiques préexistants n'est pas claire et peut entraîner une certaine confusion quant à la manière de prendre des mesures contre une forme d'abus donnée. L'ambiguïté provient de l'article 25, paragraphe 2, du DSA, qui exclut de son champ d'application tous les choix de conception manipulateurs déjà couverts par la DPCD et le RGPD (Sorensen, Sein & Rott, 2023). L'interaction de l'article 25, paragraphe 1, avec la DPCD est la plus problématique, tandis que le champ d'application du RGPD est plus facile à distinguer, même s'il peut encore y avoir des chevauchements (Hacker, 2021). La présente section examine plus en détail l'interaction entre ces instruments et met en évidence certaines zones d'ombre. D'autres réglementations couvrant des interfaces truquées, telles que la directive sur les droits des consommateurs ou la directive sur les clauses contractuelles abusives, ne sont pas examinées ici, car l'article 25, paragraphe 2, du DSA ne les mentionne pas.

3.2.1 DPCD et RGPD

En général, l'interaction entre la DPCD et le RGPD est assez claire. Premièrement, en tant que *lex specialis*, le RGPD prévaut dans les cas de interfaces truquées liés à des demandes de consentement pour le traitement de données (article 3, paragraphe 4, de la DPCD). Deuxièmement, la notion de vie privée n'est pas mentionnée dans la directive, ce qui l'empêche de traiter les violations de la vie privée des consommateurs (Hacker, 2021). Toutefois, la DPCD couvre un aspect de la protection des données. Les exigences en matière d'information du RGPD pourraient être considérées comme des informations importantes au titre de l'article 7(5) de la DPCD (Commission européenne, 2021). Par conséquent, lorsqu'une plateforme vend des données à caractère personnel à des tiers et tire une valeur économique de cette transaction, les données collectées font partie d'une pratique commerciale et relèvent du champ d'application de la DPCD. Si l'opérateur n'indique pas que les données sont vendues à des tiers, cela pourrait constituer une violation de l'article 7, paragraphe 2, de la directive, car il s'agirait d'une omission trompeuse d'une information substantielle. En outre, cela enfreindrait les exigences de transparence prévues à l'article 12 du RGPD, qui pourraient être prises en compte pour évaluer si une pratique commerciale est déloyale ou non (Commission européenne, 2021). Dans ce cas, le interface truquée pourrait être appliqué en vertu des deux textes législatifs - en vertu de la DPCD en tant qu'omission trompeuse ou en vertu du RGPD en tant que violation des exigences de transparence.

3.2.2 DSA et RGPD

La portée juridique du DSA et du RGPD en ce qui concerne les "dark patterns" est globalement claire. Les deux peuvent sembler se chevaucher lorsqu'un responsable du traitement des données au titre du RGPD est en même temps une plateforme en ligne au titre du DSA. Dans une telle situation, la question clé est de savoir à quoi sert l'interface truquée. S'il s'agit du consentement au traitement des données, lorsque les utilisateurs sont manipulés pour donner plus de données qu'ils n'en ont l'intention, c'est le RGPD qui prévaut. Dans ce cas, les lignes directrices susmentionnées de l'EDPB sur les "dark patterns" expliquent en détail quelles sont les "dark patterns" qui constituent des pratiques incitant à fournir des données et qui sont donc interdites par le RGPD.

En ce qui concerne la conception technique d'une plateforme en ligne, l'article 25 du DSA peut être considéré comme complémentaire de l'article 25 du RGPD. Les deux articles réglementent purement et simplement les aspects techniques des sites web plutôt que d'interdire des pratiques spécifiques. L'article 25 du RGPD prescrit aux responsables du traitement de mettre en œuvre la protection des données dès la conception. Ils doivent adopter des "mesures techniques et organisationnelles appropriées" pour garantir que les droits de la personne concernée (tels que l'autonomie) sont respectés (article 25, paragraphe 1, du RGPD) et que seules les données nécessaires sont traitées (article 25, paragraphe 2, du RGPD). En revanche, l'article 25 du DSA a été conçu comme une interdiction plutôt que comme un principe, mais les deux articles se complètent dans le cadre de la réglementation sur les interfaces truquées, car le RGPD couvre toutes les manipulations concernant la collecte de données, tandis que le DSA (ou DPCD) couvre tous les autres aspects de la conception d'interfaces en ligne manipulatrices.

3.2.3 DSA et DPCD

La distinction entre le DSA et la DPCD est plus difficile à établir. Ce qui suit est une exploration des limites possibles - des interfaces truquées qui ne relèvent pas du champ d'application de la DPCD mais de celui de l'article 25 du DSA.

Premièrement, le champ d'application subjectif de la DPCD couvre les relations B2C, de sorte que son champ d'application n'est pas respecté si la pratique commerciale n'a pas lieu entre un professionnel et un consommateur. À l'inverse, DSA s'applique aux relations entre les plateformes en ligne et tout type d'utilisateur, y compris les utilisateurs professionnels. Par conséquent, si l'on considère le côté "manipulation", lorsque le motif sombre est mis en œuvre par un commerçant qui n'est pas une plateforme en ligne, la légalité du motif ne peut pas être évaluée à l'aide du DSA. C'est le cas des modèles sombres mis en place par les commerçants directement sur leurs propres sites web qu'ils utilisent pour vendre aux consommateurs. Dans ce cas, la DPCD continuera à réglementer les pratiques commerciales. L'article 25 du DSA ne peut pas non plus être utilisé lorsque la partie qui met en œuvre l'interface truquée est

un intermédiaire en ligne (soumis à le DSA) mais pas une plateforme en ligne, telle que définie à l'article 3, point i). Dans ce cas, si l'intermédiaire dépasse également la définition d'un commerçant se livrant à une pratique commerciale de la DPCD, tout interface truquée potentiel pourrait échapper aux deux interdictions.

Du côté des "manipulés", s'il s'agit d'une entreprise ou d'un commerçant, cette pratique dépassera le champ d'application de la DPCD mais pourrait être interdite en vertu de l'article 25 - encore une fois, tant que l'"auteur" peut être considéré comme une plateforme en ligne. Dans la pratique, cependant, cette interaction entre le DSA et la DPCD est encore plus compliquée, étant donné que certains États membres tels que l'Autriche ont transposé la DPCD d'une manière qui étend les lois sur la protection des consommateurs pour couvrir également les pratiques commerciales interentreprises (Civic Consulting, 2011). En revanche, la loi allemande sur la protection des consommateurs a transposé la DPCD sans étendre la protection aux pratiques interentreprises (Civic Consulting, 2011), ce qui crée une application inégale de la DPCD dans les différents États membres.

Si l'on se concentre sur le champ d'application objectif de la DPCD, une pratique obscure dépasserait ce champ d'application soit lorsque la pratique commerciale n'est pas déloyale, soit si la pratique obscure n'est pas une pratique commerciale à proprement parler. Comme indiqué ci-dessus, la définition de la loyauté n'est pas claire, car elle dépend de l'évaluation de la loyauté en fonction de l'effet manipulateur potentiel ou réel. En outre, la loyauté dépend de la norme du destinataire par rapport à laquelle la tromperie est mesurée. Pour comprendre exactement le champ d'application, les questions de définition doivent être résolues. En l'absence de définition claire, il est également difficile de déterminer si une pratique spécifique serait considérée comme déloyale en vertu de la DPCD ou non.

En outre, il n'est pas simple de déterminer si une pratique est commerciale. Comme indiqué, les pratiques commerciales B2C peuvent inclure des actes, des omissions ou des communications avant, pendant ou après la vente ou la fourniture d'un produit (article 2 de la directive sur les pratiques commerciales déloyales). Il n'est pas certain que les interfaces truquées qui évitent les obligations de la plateforme en vertu du DSA puissent être considérés comme une pratique commerciale. Il s'agit d'obligations telles que les mécanismes de notification et d'action (article 16 du DSA), les mécanismes internes de traitement des plaintes (article 20 du DSA) et la disponibilité de règlements extrajudiciaires (article 21 du DSA). Par exemple, l'article 21 du DSA stipule que les plateformes doivent informer les utilisateurs "dans une interface claire et conviviale" qu'ils peuvent porter l'affaire devant un organe de règlement extrajudiciaire des litiges s'ils ne sont pas satisfaits de l'issue d'un recours. Si un schéma obscur était mis en œuvre pour rendre cette procédure confuse ou pour dissimuler les mécanismes de traitement des plaintes afin d'éviter que les utilisateurs ne les utilisent, ces pratiques

seraient-elles considérées comme des pratiques commerciales et relèveraient donc de la DPCD plutôt que du DSA ?

La difficulté de déterminer si c'est le DSA ou la DPCD qui s'applique aura des effets sur l'application de la législation. Pour pouvoir appliquer l'AVD, il faudra d'abord établir qu'une forme sombre spécifique n'enfreint pas la DPCD. Pour ce faire, il faut clarifier les définitions et le champ d'application afin de pouvoir déterminer quelles formes sombres ne relèvent pas du champ d'application objectif et subjectif de la DPCD et entrent dans le champ d'application du DSA. En raison notamment de l'absence de précédent juridique sur les interfaces truquées (BEUC, 2022), les personnes chargées de l'application de la loi pourraient être confrontées au problème de ne pas savoir quelle réglementation un motif sombre enfreint.

3.2.4. Un point positif : un fourre-tout au fur et à mesure de l'évolution des interfaces truquées

La sous-section ci-dessus a permis de conclure qu'il n'existe pas de distinction claire quant à la portée juridique des formes sombres couvertes par le DSA par rapport à celles couvertes par la DPCD. En effet, d'un point de vue juridique, les termes de la DPCD ont été interprétés de manière si large qu'ils incluent la plupart - voire la totalité - des formes sombres que l'on peut trouver sur une plateforme en ligne (Goanta & Santos, 2023). En outre, l'interdiction des "dark patterns" s'applique aux pratiques commerciales B2B dans certains États membres, mais pas dans d'autres, comme le montre l'exemple de l'Autriche et de l'Allemagne. Cela peut créer une certaine confusion sur le marché quant à ce qui s'applique. Bien que l'interaction peu claire entre la DPCD et le DSA puisse poser des problèmes et nécessite une clarification, l'article 25 du DSA pourrait avoir pour mérite de servir de fourre-tout pour toutes les formes sombres qui n'entrent pas dans le champ d'application de la DPCD ainsi que pour les formes sombres futures.

Étant donné que les conceptions d'interfaces manipulatrices évoluent continuellement, passant de statiques à plus dynamiques, de nouvelles interfaces truquées peuvent être légèrement modifiés pour contourner les interdictions existantes concernant des motifs spécifiques (OCDE, 2020, p. 8). Dans le cadre du RGPD, il a été démontré comment les responsables du traitement des données ont développé des interfaces truquées dynamiques pour contourner les exigences réglementaires et contrecarrer l'objectif du règlement (Sinders, 2021). La définition large du DSA peut réduire la possibilité que des interfaces truquées passent à travers les mailles du filet de la réglementation en s'attaquant aux interfaces truquées statiques qui ne sont pas traités efficacement par la réglementation existante et en couvrant également les manipulations dynamiques émergentes. Si la Commission clarifie le champ d'application pour y inclure les manipulations dynamiques, l'application du DSA s'en trouverait renforcée.

3.3. Application de la loi

Dans l'ensemble, les mécanismes d'application dans le paysage juridique de l'UE semblent être bien définis dans chaque cadre juridique. Toutefois, les champs d'application mal délimités du DSA, de la DPCD et du RGPD peuvent entraîner une incertitude quant à la procédure d'exécution à adopter dans le contexte des interdictions relatives aux interfaces truquées. D'un autre côté, l'Acte pourrait s'avérer efficace en augmentant les efforts de surveillance globale des autorités au niveau européen.

3.3.1. Aspects positifs

À ce jour, l'application de l'interdiction des interfaces truquées en vertu du RGPD et de la DPCD a été insuffisante. Une étude menée par la Commission européenne sur les "dark patterns" dans les sites de commerce en ligne montre que malgré l'applicabilité claire du cadre de la DPCD, les "dark patterns" prolifèrent sur le web.

Bien que l'interdiction de l'article 25 ne se traduise pas automatiquement par une mise en application, il convient de noter que, d'un point de vue politique, le fait que le DSA soit un règlement ayant un effet direct dans tous les États membres (contrairement à une directive comme la DPCD qui devait être transposée) est un élément que la Commission pourrait exploiter avec succès. Dans le nouveau cadre, la Commission sera en mesure d'influencer plus directement la manière dont les interfaces truquées sont réglementées dans l'UE, en renforçant l'harmonisation du paysage juridique de l'Union - à la fois en définissant des lignes directrices et en faisant appliquer les cas de interfaces truquées contre les VLOP.

En outre, l'ASN vise à prendre en compte les effets néfastes transnationaux du mauvais comportement des plateformes, en encourageant la coopération européenne entre les États membres par la création d'un cadre de partage d'informations "fiable et sûr" entre les coordinateurs de services numériques (article 67). De la même manière, l'article 45 permet aux États membres de communiquer avec les CSD de différentes juridictions, dans le but de promouvoir une application uniforme à l'échelle de l'UE. Ce mécanisme représente une protection contre l'application hétérogène qui pourrait autrement survenir en raison des différences d'infrastructure dans le domaine numérique caractérisant les différents États membres. À cet égard, DSA vise à éviter de perpétuer les écueils de l'application de la DPCD. Il convient de noter que les articles 58 et 60 de l'ASN visent également à promouvoir la coordination entre la Commission, le Comité européen des services numériques et le CSN, par exemple en autorisant les enquêtes conjointes des coordonnateurs ou les demandes réglementaires conjointes aux États membres émanant à la fois du Comité et des coordonnateurs.

Il y a aussi le fait que les pratiques illicites concernant les interfaces truquées seront très spécifiques au contexte et même au service. En se donnant le pouvoir d'élaborer des lignes directrices sur les interfaces truquées, la Commission européenne fait en sorte que l'évolution de ces dispositions reste sous son contrôle et qu'elle suive de plus près son point de vue sur la question. En effet, les lignes directrices de la Commission font autorité ; les entreprises les utilisent souvent comme guides de bonnes pratiques et d'autres autorités s'appuient également sur elles pour appliquer la loi (Terpan 2014).

En outre, l'inclusion d'une interdiction supplémentaire sur les interfaces truquées signifie qu'il y aura un degré plus élevé de surveillance réglementaire sur les interfaces truquées potentiels. À cet égard, il convient de noter que les dispositions d'application du DSA prévoient la création de coordinateurs nationaux des services numériques (CSN) et d'un Conseil européen des services numériques. Ces CSN ne sont pas nécessairement de nouvelles institutions. En fait, tous les pays qui, à ce jour, ont annoncé la création de leur CSN ont désigné une autorité préexistante (Ledger, 2023). Néanmoins, la création de CSD signifie qu'une autorité qui n'était pas responsable de la surveillance des interfaces truquées auparavant est désormais habilitée à le faire - c'est le cas en Irlande et en Hongrie, où les régulateurs nationaux des médias ont été nommés CSD. Dans d'autres cas, cela signifie qu'une autorité qui réglementait déjà les "dark patterns" dispose désormais d'un autre instrument juridique pour les réglementer efficacement. Ce sera par exemple le cas aux Pays-Bas, où l'autorité de protection des consommateurs, chargée de la mise en œuvre de la DPCD[6] , a également été nommée CSD. Ainsi, la même autorité est habilitée à agir contre les pratiques commerciales déloyales par le biais de deux cadres juridiques différents.

Un autre point susceptible d'améliorer l'application est l'applicabilité du DSA aux intermédiaires basés en dehors de l'Union. Dans le cadre de la DPCD, l'application des interfaces truquées aux opérateurs étrangers était soumise aux mécanismes traditionnels - et plus longs - du droit international privé (Commission européenne, 2021, p. 25). En revanche, le DSA, à l'image du RGPD, vise à réglementer les intermédiaires en ligne indépendamment de leur lieu d'établissement, pour autant que leurs services soient accessibles dans l'UE. Pour ce faire, DSA conditionne le maintien de l'accès au marché unique à la désignation d'un représentant légal dans l'UE, qui doit disposer des pouvoirs et des ressources nécessaires pour garantir le respect effectif du DSA (article 13 du DSA). En ce sens, même si la DPCD peut s'appliquer aux opérateurs établis dans des pays tiers, les conditions du DSA peuvent faciliter l'application effective d'une interdiction des interfaces truquées.

3.3.2. Aspects négatifs

La fragmentation des instruments juridiques traitant des interfaces truquées dans les plateformes en ligne peut créer une incertitude non seulement quant aux

réglementations applicables, mais aussi quant à l'autorité chargée de l'application. Dans ce contexte, l'interaction entre la DPCD et le DSA peut créer des tensions entre les ASF et les régulateurs au niveau national en termes d'application effective. Dans la pratique, les différentes autorités nationales ont une influence relative différente. Par conséquent, le même concept de l'interface truquée peut finir par être appliqué par différentes autorités utilisant une base juridique différente (DPCD ou DSA) en fonction des ressources dont elles disposent et du pouvoir relatif d'un organisme sur l'autre.

Ainsi, bien que le DSA définisse la création de mécanismes de coordination entre les coordinateurs de services numériques, elle ne tient pas compte de la coordination de ces derniers avec les organismes de protection des consommateurs qui visent à traiter les mêmes questions. Il s'agit là d'un écueil important, surtout si l'on considère le manque de clarté concernant le champ d'application de le DSA et de la DPCD. Dans ce contexte, les défaillances de communication entre les coordinateurs des services numériques et les autorités de protection des consommateurs pourraient conduire à des problèmes de double responsabilité lorsque les plateformes font l'objet d'une enquête et se voient infliger une amende à la fois au titre de la DPCD et du DSA pour la même infraction, ainsi qu'à des procédures d'application inefficaces.

À l'instar des questions relatives au champ d'application juridique, les incertitudes concernant l'application de la législation affectent non seulement l'autorité (ou les autorités) chargée(s) de l'application, mais aussi les acteurs du marché. Les incertitudes relatives à ce qui s'applique, à l'autorité chargée de l'application et à la manière de se conformer peuvent grandement entraver la capacité des acteurs du marché à organiser leurs activités et à comprendre leurs obligations.

3.4. La boîte à outils du DSA : d'autres outils pour s'attaquer aux interfaces truquées

Enfin, les autorités de contrôle et la Commission en particulier peuvent examiner comment d'autres dispositions du DSA, en dehors de l'article 25, peuvent être utilisées pour empêcher la diffusion d'interfaces trompeuses. Une lecture globale du DSA révèle les possibilités suivantes :

3.4.1. Droits des très grandes plateformes en ligne (VLOP)

L'approche par paliers du DSA considère la taille comme un indicateur de risque et impose des obligations asymétriques en fonction de la taille. Les VLOP, ou plateformes en ligne comptant plus de 45 millions d'utilisateurs mensuels moyens dans l'UE (article 33 du DSA), sont soumises à des obligations supplémentaires visant à lutter contre les risques plus importants associés à leurs plateformes. Certaines obligations spécifiques aux VLOP peuvent avoir une incidence sur l'utilisation d'interfaces au design déroutant.

La Commission aura un rôle clé à jouer à cet égard, puisqu'elle est la principale responsable de l'application du DSA *à l'égard des* VLOP et des très grands moteurs de recherche en ligne (VLOSE).

Par exemple, l'obligation des VLOP d'évaluer les risques systémiques (article 34) peut être utilisée pour les contraindre à déterminer les impacts potentiellement négatifs des choix de conception qui, bien qu'ils ne soient peut-être pas suffisamment "sombres" pour constituer des modèles illégaux en vertu de l'article 25 du DSA, peuvent néanmoins semer la confusion dans l'esprit des destinataires. En ce sens, les VLOP doivent évaluer l'impact réel ou prévisible de leur service sur l'exercice des droits fondamentaux, y compris la dignité humaine, la protection des données, les droits de l'enfant et la protection des consommateurs. Les risques pour les droits de l'enfant peuvent résulter de "la conception d'interfaces en ligne qui exploitent, intentionnellement ou non, les faiblesses et l'inexpérience des mineurs" (considérant 81). De même, les risques pour la santé publique et le bien-être des individus peuvent découler de "la conception d'interfaces en ligne qui stimulent la dépendance comportementale" (considérant 83).

Après l'identification des risques, les VLOP doivent les atténuer par des mesures qui seront évaluées par la Commission (article 35). Le considérant 87 du DSA indique explicitement que l'adaptation d'une interface peut constituer une mesure d'atténuation appropriée. Ensemble, ces articles encouragent les VLOP à mettre en œuvre des interfaces plus neutres et à atténuer les effets potentiellement négatifs des choix de conception qui, s'ils ne sont peut-être pas suffisamment trompeurs pour enfreindre l'article 25, peuvent néanmoins dérouter les destinataires, exploiter les faiblesses des enfants ou stimuler des comportements de dépendance. La Commission peut donc envisager d'utiliser cette disposition comme une incitation *positive* à choisir des interfaces neutres. Dans ce cas, l'accent est mis sur les risques et les préjudices qui peuvent être évités en optant pour des choix neutres, plutôt que sur les déterminations juridiques coûteuses visant à déterminer si un élément de conception franchit la ligne de l'illégalité.

Enfin, le rôle des chercheurs dans le cadre du DSA peut également permettre d'améliorer l'élaboration des politiques relatives aux interfaces truquées. Comme le notent Luguri et Strahilevitz (2021), il y a un vide dans la recherche publique sur l'efficacité des "dark patterns" à tromper les utilisateurs. Cette recherche s'est principalement déroulée à huis clos, au sein des entreprises, en utilisant les données auxquelles elles sont les seules à avoir accès. Pourtant, l'article 40 du DSA fournit un cadre permettant d'obliger les VLOP à donner accès aux données à des chercheurs agréés. Bien entendu, l'accès à la recherche aura des limites, car les VLOP ont le droit légitime de préserver la confidentialité des informations sensibles, telles que les secrets commerciaux. Néanmoins, leur travail pourrait apporter de nouvelles connaissances, permettant ainsi d'améliorer la réglementation et l'application de la loi.

3.4.2. Autres

Les interfaces truquées peuvent affecter d'autres obligations du DSA qui s'appliquent à toutes sortes d'intermédiaires en ligne, au-delà des plateformes en ligne. Par exemple, l'article 14 de l'AVD exige que tous les intermédiaires en ligne publient des conditions générales intelligibles et accessibles, y compris des informations sur les politiques de modération des contenus. Les modèles obscurs qui cachent ou embrouillent les termes et conditions pourraient contredire cette obligation. En outre, l'article 16 de l'AVD stipule que les fournisseurs de services d'hébergement[7] doivent disposer de mécanismes de notification et d'action permettant à tout utilisateur de signaler un contenu illégal. Ce mécanisme doit être facile d'accès et convivial. Par conséquent, si l'intermédiaire utilise des éléments de conception pour le dissimuler ou pour le rendre difficile à utiliser, un tel schéma obscur pourrait être considéré comme une violation de l'article 16 du DSA.

4.4. Conclusions et recommandations

Malgré de multiples efforts de réglementation, les interfaces truquées restent un élément prédominant de l'expérience en ligne des citoyens de l'UE, entravant leur capacité à définir leurs préférences de manière autonome et à agir en conséquence. Dans ce contexte difficile, la loi sur les services numériques ajoute une nouvelle dimension. Cette note politique a analysé l'approche de la loi sur les services numériques à l'égard des interfaces truquées, en se concentrant sur l'interdiction des interfaces truquées prévue par l'article 25. Après un résumé du cadre juridique de l'UE sur les interfaces truquées et une analyse de l'article 25, cette note a mis en évidence quatre domaines que la Commission européenne doit aborder afin de mettre en œuvre au mieux la nouvelle interdiction. La mise en œuvre est considérée comme optimale si elle contribue à la mise en place d'un cadre juridique cohérent et efficace pour lutter contre les interfaces truquées. Nous appelons donc la Commission européenne à agir dans le cadre de ses pouvoirs pour produire des lignes directrices sur l'article 25, en prenant en compte les recommandations suivantes.

4.1. Clarifier les termes

La section 3.1 a mis en évidence trois grandes incertitudes définitionnelles de l'article 25 qui pourraient nuire à son efficacité : (i) l'interdiction s'étend-elle à la personnalisation manipulatrice de l'interface, (ii) l'effet manipulateur doit-il être réel ou potentiel, et (iii) la norme utilisée pour déterminer cet effet est-elle celle du "consommateur moyen" ? La Commission devrait profiter de l'occasion pour clarifier ces points de la manière suivante.

4.1.1. La personnalisation manipulatrice de l'interface serait mieux traitée en renforçant la protection des données dans le cadre du RGPD.

Malgré leur inclusion potentielle dans l'interdiction du DSA, il n'est pas nécessairement vrai que la personnalisation manipulatrice de l'interface soit mieux traitée en tant qu'interface truquée. Le rapport 2022 de la Commission européenne sur ce sujet est instructif : il affirme que "les entreprises ont de plus en plus recours à des pratiques de personnalisation et les combinent avec des interfaces truquées", mais révèle en même temps que son enquête "n'a pas identifié de cas significatifs de personnalisation manipulatrice" (p. 6). La nature de l'asymétrie de l'information, l'opacité algorithmique et le défi général que représente l'identification d'une personnalisation problématique là où elle se produit ont empêché la DPCD de s'attaquer à cette question de manière adéquate. On peut s'attendre à ce qu'il s'agisse d'un défi équivalent dans le cadre du DSA.

C'est pour cette raison qu'il serait préférable de traiter la personnalisation manipulatrice des interfaces à sa source (c'est-à-dire la fourniture de données à caractère personnel), plutôt que dans sa matérialisation extérieure (souvent non observable). Comme le reconnaît la Commission européenne, ces types de pratiques "se situent à l'intersection de la protection des consommateurs, de la protection des données et d'autres instruments pertinents du cadre juridique de l'UE" (2022, p. 7). La personnalisation manipulatrice de l'interface repose sur la collecte et le traitement de données visant à révéler des informations sur un utilisateur individuel qui peuvent être exploitées pour promouvoir des actions favorables au responsable du traitement des données. L'interdiction de ces pratiques pourrait être envisagée dans le cadre de l'article 9 du RGPD, qui interdit le traitement de plusieurs catégories de données à caractère personnel "dans le but d'identifier une personne physique de manière unique". Toutefois, cet article est actuellement mal équipé pour réduire l'offre de données qui sous-tend la conception d'interfaces manipulatrices, car il se limite à des catégories spécifiques de données à caractère personnel particulièrement sensibles (par exemple, les données biométriques, la race et la religion) et exempte les circonstances dans lesquelles la personne concernée a donné son consentement explicite au traitement. Cela pose un problème car la personnalisation de l'interface manipulative peut être basée sur des catégories de données qui ne sont pas soumises aux restrictions de l'article 9 et le consentement, lorsqu'il est fourni, peut être corrompu par la personnalisation de l'interface manipulative en elle-même.

La Commission européenne devrait examiner si la pratique plus large de la personnalisation manipulatrice de l'interface est conforme à l'objectif général déclaré du RGPD de garantir que "les données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes" (RGPD(5)(1)(a)). Comme l'a souligné l'étude 2022 de la Commission européenne, cette discussion repose en fin de compte sur la différenciation entre la personnalisation "légitime" et la personnalisation

manipulatrice. Bien sûr, dans certaines circonstances, la personnalisation est bénéfique pour les utilisateurs ; elle peut légitimement aider les utilisateurs à naviguer dans la vaste cacophonie de la vie en ligne de manière plus efficace et plus productive. Cependant, nous pensons que la personnalisation manipulatrice des interfaces est un problème omniprésent et croissant qui ne peut être traité de manière adéquate en interdisant sa manifestation observable, étant donné qu'elle est rarement observable ou détectable de "l'extérieur", comme nous l'avons établi. L'action réglementaire doit donc se concentrer sur la réception de l'offre de données qui alimente ces pratiques, tout en veillant à permettre des pratiques de personnalisation légitimes lorsque cela est possible. Nous pensons que c'est l'objectif principal et le mandat du RGPD, et non l'article 25 du DSA, qui sont les mieux placés pour poursuivre cet agenda réglementaire.

4.1.2. Accepter un effet potentiel

L'article 25 du DSA ne précise pas si l'effet de tromperie de l'utilisateur doit être réel ou si un effet potentiel peut suffire. Pour mieux répondre aux objectifs du DSA de protéger les droits des utilisateurs et de créer un environnement digne de confiance (considérant 12), la disposition devrait englober les deux. Cette conclusion est étayée par le fait que la DPCD n'exige qu'un effet probable de tromperie. Étant donné que les interfaces truquées restent si répandues malgré le cadre juridique préexistant qui est "indulgent" à cet égard, et étant donné que l'article 25 du DSA vise à attraper les interfaces truquées qui dépassent le champ d'application de la DPCD, la fixation d'un seuil plus élevé à l'article 25 irait à l'encontre de l'objectif de la politique.

4.1.3. Abaisser la norme du destinataire

La Commission européenne devrait clarifier le critère du destinataire qui sera utilisé pour déterminer si un modèle est susceptible de tromper les utilisateurs. Ici, pour mieux protéger les droits des utilisateurs et refléter les asymétries de pouvoir décrites ci-dessus, l'article 25 du DSA devrait être mis en œuvre en utilisant un critère moins élevé que le critère du "consommateur moyen" typique de la DPCD.

Le manque de complémentarité entre les normes de la DPCD et du DSA pourrait entraîner des conséquences moins souhaitables, notamment en termes d'application pratique : le même motif sombre pourrait être jugé illégal s'il est évalué par le DSA d'un pays, et légal s'il est analysé par l'autorité chargée de la protection des consommateurs. Toutefois, d'une certaine manière, cela correspond à l'objectif de l'article 25, qui est de saisir les interfaces en ligne qui dépassent le cadre préexistant. En outre, étant donné que le droit de la consommation lui-même évolue vers une reconnaissance des vulnérabilités inhérentes aux "dark patterns" (voir note de bas de page 5), si le DSA adopte ce seuil inférieur, le désir de complémentarité entre la DPCD et le DSA (notamment en raison du besoin de certitude juridique des acteurs du

marché) pourrait donner l'impulsion finale nécessaire pour modifier complètement la norme dans le droit de la consommation, en l'alignant mieux sur l'ère numérique.

4.2. Clarifier le champ d'application

La Commission européenne devrait clarifier juridiquement les champs d'application du RGPD, de la DPCD et du DSA en ce qui concerne la réglementation des interfaces truquées. Actuellement, l'interaction entre les législations sur les interfaces truquées pourrait conduire à une réglementation inefficace. Par conséquent, la Commission devrait remédier à l'application peu claire de la DPCD en précisant le champ d'application subjectif et objectif de la directive. En particulier, l'interaction du DSA avec les différentes transpositions de la législation sur la protection des consommateurs doit être clarifiée, étant donné que certains États membres étendent les interdictions de pratiques manipulatrices aux pratiques commerciales interentreprises. En outre, la présente note d'orientation a donné des exemples spécifiques de pratiques particulières qui dépassent peut-être le champ d'application de la DPCD et pourraient donc être incluses dans le champ d'application de l'article 25 - telles que la dissimulation de mécanismes de traitement des réclamations. La Commission devrait fournir des orientations sur le champ d'application de ces pratiques.

4.3 Coordonner l'application de la législation

La Commission européenne devrait définir clairement un cadre pour la coordination entre les autorités nationales de protection des consommateurs, responsables de l'application de la DPCD, et les coordinateurs nationaux des services numériques. Cela peut se faire en établissant un mécanisme de communication procédural clair. Par exemple, il peut être complété par l'article 45 ou l'article 67 du DSA et prescrire la notification obligatoire de l'ouverture d'une enquête et de l'imposition d'une amende aux autorités respectives. Une telle solution permettrait au moins d'éviter tout risque de double responsabilité et rendrait le cadre réglementaire plus clair, y compris en ce qui concerne le champ d'application. En ce sens, la recommandation renforcerait l'alignement du DSA sur deux des trois principaux objectifs de la présente note d'orientation, à savoir garantir un *cadre juridique européen cohérent* sur les interfaces truquées et assurer son *application effective*.

4.4. Exploiter toute la boîte à outils du DSA

La Commission devrait examiner comment d'autres dispositions du DSA peuvent être utilisées pour lutter contre l'utilisation d'interfaces en ligne trompeuses, à la fois par les plateformes en ligne et par d'autres intermédiaires en ligne. Comme le souligne la section 3.4, une lecture transversale du DSA du point de vue des interfaces truquées

révèle de nombreuses possibilités, allant de l'évaluation des risques systémiques par les VLOP à l'accessibilité des mécanismes de notification et d'action par tous les fournisseurs de services d'hébergement.

L'une des possibilités les plus prometteuses consiste à donner accès aux données à des chercheurs agréés. Comme mentionné, le cadre de l'article pourrait permettre aux chercheurs de fournir de nouvelles informations sur les interfaces truquées, en particulier au fur et à mesure qu'ils continuent d'évoluer, permettant ainsi une meilleure réglementation. Cependant, la Commission doit garder à l'esprit les moyens par lesquels les intermédiaires peuvent essayer de contourner l'octroi d'un accès significatif : qu'il s'agisse d'abuser des revendications d'intérêt légitime ou de fournir aux chercheurs des vidages de données impossibles à analyser, au lieu des données structurées que l'entreprise utilise pour concevoir et tester les interfaces. Ce qui compte, ce n'est pas seulement le fait de donner l'accès, mais aussi les conditions de cet accès. En ce sens, pour canaliser le potentiel de l'article 40 vis-à-vis des interfaces truquées, la Commission doit veiller à ce que les chercheurs bénéficient d'un accès significatif dans le respect de tous les intérêts légitimes.

Au-delà de ce cas spécifique, les idées exposées à la section 3.4 peuvent rassurer ceux qui craignent que l'interdiction de l'article 25 n'ait été étendue à d'autres intermédiaires en ligne (par exemple, Lomas, 2022) - il existe des outils au sein du DSA pour étendre la surveillance des interfaces truquées au-delà du champ d'application subjectif de l'article 25 (c'est-à-dire les plates-formes en ligne). Il existe également des moyens d'encourager positivement des interfaces plus neutres, au-delà d'une interdiction stricte comme celle de l'article 25. Ce type d'élaboration créative des politiques pourrait peut-être être la pièce manquante du puzzle pour freiner avec succès la prolifération des interfaces truquées dans l'UE.

5.5. Bibliographie

Législation

Charte des droits fondamentaux de l'Union européenne [2012] JO C 326/391 ELI : http://data.europa.eu/eli/treaty/char_2012/oj

Version consolidée du traité sur l'Union européenne [2008] JO C115/13

Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement

européen et du Conseil *("directive sur les pratiques commerciales déloyales")* JO L 149/22 ELI : http://data.europa.eu/eli/dir/2005/29/oj

Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle *("Loi sur l'intelligence artificielle")* et modifiant certains actes législatifs de l'Union [2021] COM/2021/206

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE *("règlement général sur la protection des données")* [2016] JO L 119/1 ELI : http://data.europa.eu/eli/reg/2016/679/2016-05-04

Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 concernant les marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 *("loi sur les marchés numériques")* [2022] JO L 265/1 ELI : http://data.europa.eu/eli/reg/2022/1925/oj

Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 sur un marché unique des services numériques et modifiant la directive 2000/31/CE *("loi sur les services numériques")* [2022] JO L 277/1 ELI : http://data.europa.eu/eli/reg/2022/2065/oj

Jurisprudence

Cour de justice de l'Union européenne, arrêt du 1er octobre 2019, *Planet49 GmbH,* C-673/17, ECLI:EU:C:2019:801

Cour de justice de l'Union européenne, arrêt du 11 novembre 2020, *Orange Roumanie,* C-61/19, ECLI:EU:C:2020:901.

Cour européenne de justice, arrêt du 16 juillet 1998, *Gut Springenheide et Tusky*, C-210/96, ECLI:EU:C:1998:369.

Tribunal d'appel du commerce et de l'industrie des Pays-Bas, arrêt du 15 mai 2018, *ACM/Corendon*, affaire 17/1179, ECLI:NL:CBB:2018:145.

Autres

ACM (2022). *Lignes directrices sur la protection du consommateur en ligne : Les limites de la persuasion en ligne.* Autorité néerlandaise pour les consommateurs et les marchés. https://www.acm.nl/en/publications/guidelines-protection-online-consumer

BEUC (2022, 7 février). Les *"interfaces truquées" et l'acquis communautaire en matière de droit de la consommation*. Recommandations pour une meilleure application et une meilleure réforme. https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf

Cauffman, C. et Goanta, C. (2021). A new order : the digital services act and consumer protection. *European Journal of Risk Regulation*, *12*(4), 758-774.

Civic Consulting. (2011). *Étude sur l'application de la directive 2005/29/CE relative aux pratiques commerciales déloyales dans l'UE.* Commission européenne. https://op.europa.eu/en/publication-detail/-/publication/5550d564-65af-47c8-b7e4-a44020ad4a78

Ecommerce Europe. (2022, 14 juin). *Réponse d'Ecommerce Europe à l'appel à contribution sur l'*équité *numérique.* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/F3296360_en

EDPB. (2022).*Lignes directrices 3/2022 sur les interfaces truquées dans les interfaces des plateformes de réseaux sociaux : Comment les reconnaître et les éviter.* https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

Commission européenne. (2020, 15 décembre). *Document de travail des services de la Commission sur l'analyse d'impact.* Analyse d'impact de la loi sur les services numériques. https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

Commission européenne. (2021). Lignes directrices relatives à l'interprétation et à l'application de la directive 2005/29/CE du Parlement européen et du Conseil relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur. *Journal officiel de l'Union européenne.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)

Commission européenne (2023, 30 janvier). *Protection des consommateurs : pratiques manipulatrices en ligne constatées sur 148 des 399 boutiques en ligne*

examinées. https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418https:/op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

Commission européenne. (2022). *Déclaration européenne sur les droits et principes numériques pour la décennie numérique.* https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration

Goanta, C. et Santos, C. (2023). Dark Patterns Everything : An Update on a Regulatory Global Movement. *Network Law Review*.

Gumbis, J., Bacianskaite, V. et Randakeviciute, J. (2008). Les droits de l'homme garantissent-ils l'autonomie ? *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, (62), 77-93.

Hacker, P. (2021). Manipulation par les algorithmes. Exploration du triangle des pratiques commerciales déloyales, de la protection des données et du droit de la vie privée. *European Law Journal*.

Helberger, N., Sax, M., Strycharz, J. et Micklitz, H.-W. (2021). Architectures de choix dans l'économie numérique : Vers une nouvelle compréhension de la vulnérabilité numérique. *Journal of Consumer Policy,* 45, 175-200. https://doi.org/10.1007/s10603-021-09500-5

Lomas, N. (2022, 13 avril). Le redémarrage du livre de règles numériques de l'UE pourrait brouiller l'interdiction des interfaces truquées et les contrôles des traders, prévient le BEUC. TechCrunch. https://techcrunch.com/2022/04/13/dsa-beuc/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlmNvbS8&guce_referrer_sig=AQAAAG6LGvNEjYiDr3CBjmlRCRpLmLVEQDViZEH3RP05Cc3NrT7yHkCd46AVlnJhKb_M-veL0jzuZA29gKHSldIjaC8DTWxOxBIq92blcLismOcwTkmLwuxnXCyYbweyX0qHakPjbbnOQoVpUy71EESj6nTP2FXHOgH_WPaOL0Q2_.

Luguri, J. et Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43-109.

Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., Rodríguez de las Heras Ballell, T. (2022). *Étude comportementale sur les pratiques commerciales déloyales dans l'environnement numérique : interfaces truquées et personnalisation manipulatrice*. Commission européenne.

https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418

OCDE. (2020). *Table ronde sur les schémas commerciaux sombres en ligne. Résumé des discussions. https://one.*oecd.org/document/DSTI/CP(2020)23/FINAL/En/pdf

Sinders, C. (2021). *Designing against dark patterns*. *German Marshall Fund of the United States.* https://www.jstor.org/stable/pdf/resrep33487.pdf

Sorensen, M. J., Sein, K. et Rott, P. (2023). *Réponse de l'Institut de droit européen*. Institut de droit européen. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_the_European_Commission_s_Public_Consultation_on_Digital_Fairness_.pdf

Terpan, F. (2015). Les normes douces dans l'Union européenne : La nature changeante du droit de l'UE. *European Law Journal*, *21*(1), 68-96.

---

[1] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur.

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO 2016 L 119/1.

[3] Directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs, JO L 95 du 21.4.1993, p. 29-34.

[4] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37-47.

[5] Les lignes directrices de la DPCD reconnaissent que "les formes multidimensionnelles de vulnérabilité sont particulièrement aiguës dans l'environnement numérique" (Commission européenne, 2021, p. 35) et que, en ce qui concerne les interfaces truquées, "la référence d'un consommateur moyen ou vulnérable peut être modulée en fonction du groupe cible [de la pratique], même formulée du point de vue d'une seule personne qui a fait l'objet de la personnalisation spécifique" (*ibid.*, p. 100).

[6] Et, en fait, l'un des plus actifs dans l'élaboration de politiques concernant les modèles commerciaux sombres. L'Autorité néerlandaise de la consommation (ACM) a publié des orientations très complètes à l'intention des commerçants sur la manière dont elle évalue les interfaces truquées dans le cadre de la DPCD - plus précisément, dans le cadre de la loi nationale de transposition. Voir ACM, 2022.

[7] C'est-à-dire les intermédiaires qui hébergent des contenus générés par les utilisateurs (article 3(g)(iii)), qu'ils les diffusent publiquement ou non. Si c'est le cas, il s'agit d'une plateforme en ligne.

A propos des auteurs :

Tom Akhurst : Master en politiques publiques de Sciences Po, filière numérique, nouvelles technologies et politiques publiques ; titulaire d'une licence de lettres de l'université de Melbourne ; mémoire de première classe sur la "route de la soie numérique" de la Chine ; ancien rédacteur de discours pour un ministre du gouvernement australien ; ancien chercheur à l'institut Blueprint.

Laura Zurdo : Master en politique publique, filière numérique, nouvelles technologies et politique publique ; diplômée en droit et relations internationales, Universidad Pontificia de Comillas (Madrid) - ICADE ; réglementation des plateformes numériques européennes ; analyste politique chez Tremau.

Riccardo Rapparini : Master en politique publique - filière numérique, nouvelles technologies et politique publique ; licence en philosophie, politique et économie (PPE), Vrije Universiteit Amsterdam ; consultant externe auprès de l'Observatoire des politiques d'IA de l'OCDE.

Christoph Mautner Markhof : Master en politique publique : filière numérique, nouvelles technologies et politique publique ; Politique, Psychologie, Droit and Economie (PPLE), Université d'Amsterdam ; Major en Politique.

À propos de la chaire Digital, gouvernance et souveraineté:

La Chaire Digital, Gouvernance et Souveraineté de Sciences Po a pour mission de créer un forum réunissant des entreprises techniques, des universitaires, des décideurs politiques, des acteurs de la société civile, des incubateurs de politiques publiques ainsi que des experts de la régulation numérique. Hébergée par l'Ecole d'affaires publiques, la Chaire adopte une approche multidisciplinaire et holistique pour rechercher et analyser les transformations économiques, juridiques, sociales et institutionnelles induites par l'innovation numérique. La Chaire Digital, Gouvernance et Souveraineté est présidée par **Florence G'sell**, professeur de droit à l'Université de Lorraine, maître de conférences à l'Ecole d'affaires publiques de Sciences Po. Elle est professeur invitée à Stanford en 2023-2024.

Les activités de la chaire sont soutenues par :