Prédiction algorithmique : enjeux en termes de protection du consommateur et de la concurrence. Les enseignements de la pratique décisionnelle de la Federal Trade Commission américaine

Frédéric Marty

Prédiction algorithmique : enjeux en termes de protection du consommateur et de la concurrence

Les enseignements de la pratique décisionnelle de la Federal Trade Commission américaine

Frédéric Marty

Résumé. Le développement de l'intelligence artificielle passe par la maîtrise de flux de données massives, renouvelées en temps réel, variées et susceptibles d'être croisées. L'avantage lié au contrôle de ces flux peut se traduire par un avantage algorithmique qui peut placer un opérateur économique en position de force vis-à-vis de ses concurrents mais également de ses utilisateurs. Le contrôle des données a donc un aspect déterminant dans la concurrence. Se basant sur l'analyse de la pratique décisionnelle de la Federal Trade Commission américaine notre contribution envisage deux dimensions de cette question. Premièrement, dans quelle mesure peut-on extraire indûment des données au détriment de ses utilisateurs et quels sont les risques qui en découlent pour ces derniers ? Secondement, ces stratégies peuvent-elles être à la source d'un avantage concurrentiel déloyal et le cas échéant comment y remédier ?

Mots-clés. Données personnelles, intelligence artificielle, plateformes numériques, distorsions de concurrence.

Prédiction algorithmique : consommation et concurrence

Le recours à des algorithmes alimentés par des bases de données particulièrement riches en termes de volume, de rapidité de renouvellement et de variété des sources et des segments d'information concernés a permis des avancées considérables en termes de prédiction algorithmique avant même les derniers développements de l'intelligence artificielle (ci-après IA). L'économie des plateformes numériques au sens le plus large s'est alimentée au cours des vingt-cinq dernières années de ces progrès qui tiennent à la fois au développement des algorithmes et à l'inédite disponibilité de données. La performance des algorithmes de recherche, d'appariement et de prix mis en œuvre par les entreprises concernées est indubitablement à l'origine de gains significatifs en termes économiques. De meilleures recommandations, des appariements plus fins et des prix mieux calibrés génèrent des gains en termes de bien-être du consommateur, de liberté de choix pour ce dernier, d'accès au marché pour les firmes etc…

Cependant, si les gains économiques ne sont guère contestables, des questions demeurent. Le surplus créé est-il « équitablement » réparti entre les différentes parties-prenantes (plateforme d'intermédiation, entreprises utilisatrices de leurs services, consommateurs) ? L'opacité intrinsèque des algorithmes ne risque-t-elle pas de donner lieu à des pratiques d'auto-préférence ? La segmentation de plus en plus fine de la clientèle ne pourrait-elle pas se traduire par des prix discriminants, certes efficaces économiquement mais générateurs de transferts de bien-être entre les différents segments ?

Ces enjeux ne peuvent être qu'exacerbés par le développement de l'IA. L'entraînement des algorithmes sur des bases de données de plus en plus riches permet à ces derniers de faire des prédictions de plus en plus fines en matière de comportements attendus des consommateurs. La segmentation fine des consommateurs peut à terme laisser la place à une quasi-personnalisation ; l'analyse de leur comportement peut à terme conduire à un ajustement en temps réel des offres qui leur sont faites ou des stimuli auxquels ils sont exposés.

En d'autres termes, l'IA permet d'individualiser les offres et de les adapter de façon dynamique. Cela n'est bien sûr possible que par la collecte et le traitement des données, à la fois pour entraîner les algorithmes et pour rattacher chaque consommateur à un segment de plus en plus précis au fil des interactions.

La capacité de tirer profit des informations collectées et déduites sur les consommateurs peut générer des comportements problématiques en termes de droit de la consommation. Des conditions inéquitables peuvent leur être proposées. Il est en effet possible d'ajuster le prix proposé à ce qui est inféré quant à la capacité maximale à payer de chaque consommateur, d'ajuster la qualité des produits et services proposés à son niveau d'expertise déduit. De telles stratégies de discrimination sont d'autant plus

aisées à mettre en œuvre que les prix et les caractéristiques des biens offerts à chaque consommateur sont difficiles, sinon impossibles, à comparer.

L'opacité des décisions algorithmiques – qui est également en jeu dans les stratégies d'auto-préférence au détriment des entreprises utilisatrices de services d'intermédiation numérique – peut être combinée avec l'utilisation d'architectures de choix trompeuses ou manipulatrices. Il s'agit en l'espèce de *dark patterns*. Ces derniers peuvent d'abord consister en des *bad nudges* qui vont pousser le consommateur à agir contre ses intérêts ou du moins à agir dans l'intérêt de l'entreprise. Ils peuvent ensuite consister en des *bad sludges* qui vont l'empêcher d'agir dans le sens de son intérêt ou du moins entraver les actions qu'il pourrait prendre en ce sens.

Les architectures de choix trompeuses existent également dans le monde physique. Elles peuvent être mises en œuvre en ligne sans recours à l'intelligence artificielle. Ce que va changer l'IA en la matière c'est l'efficacité de la manipulation. Elle va pouvoir être personnalisée (ou quasi personnalisée) et dynamique. On parle alors d'*hyper nudges*[1] ou d'*augmented dark patterns*. L'efficacité de la manipulation du comportement n'en est que plus élevée. Cependant, cela repose sur une ressource essentielle : la donnée.

Il est nécessaire pour ce faire de collecter des données sur les utilisateurs des services numériques. Ainsi, la collecte d'informations, leur traitement et leur utilisation dans le cadre d'algorithmes peut faire courir des risques aux consommateurs et induire des dommages plus ou moins importants en fonction de la portée de la prédiction algorithmique qui en résulte et du domaine dans lequel celle-ci s'exerce. Cette approche par les risques sous-tend de nombreuses initiatives en matière de régulation de l'IA, qu'il s'agisse du projet de Règlement européen présenté en avril 2021, de l'avis rendu par la CNCDH en avril 2022[2] ou encore le projet d'Artificial Intelligence Risk Management Framework américain publié en mars 2022[3].

Nous nous proposons ici de discuter la façon dont ces risques sont pris en considération par les autorités chargées de la protection de la concurrence et des consommateurs[4]. Nous considérons le cas de la Federal Trade Commission (FTC) américaine en ce que ses décisions en matière de pratiques relatives à la collecte et à l'utilisation de données de consommateurs

---

[1] Viktorija Morozovaite (2021, p.105) définit ainsi l'hypernudge : " Hypernudging refers to one of the most sophisticated data-driven nudging processes that allow for dynamically personalised user steering, where (when executed perfectly), the right user is reached with the right message, by the right means, at the right time, as many times as needed".

[2] Commission Nationale Consultative des Droits de l'Homme, (2022), *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux,* A-2022-6, avril.

[3] National Institute of Standards and Technology, (2022), *Artificial Intelligence Risk Management Framework, US Department of Commerce*, March.

[4] Ce travail s'articule avec deux précédentes contributions (de Marcelis-Warin N. et al., 2020 et 2022).

illustrent la prise en compte des risques non seulement en termes de protection du consommateur en lui-même mais également de protection du processus de concurrence.

Dans ce cadre, notre contribution se structure en deux parties. Une première partie traite des biais dans le consentement du consommateur quant à la collecte de données le concernant et des risques qui peuvent en procéder. Une seconde partie montre que les risques en question ne se limitent pas à la seule sphère du droit de la consommation mais sont porteurs de distorsions concurrentielles dans des domaines dans lesquels la pérennité d'une concurrence par les mérites est interrogée.

Des limites des outils de protection du consommateur face aux risques de manipulation algorithmique

Nous nous attachons d'abord aux outils existants quant à la protection du consommateur en ligne en matière de protection des données personnelles avant de mettre en perspective ces derniers avec la pratique décisionnelle de la FTC.

Des limites des stratégies basées sur le consentement et la transparence

Les manipulations algorithmiques reposent sur l'exploitation de données personnelles des consommateurs mais également sur des données collectées lors de la connexion sur des sites ou de l'utilisation d'applications et des données déduites de leur comportement en ligne.

Les deux derniers types de données sont d'autant plus aisées à collecter, générer et exploiter pour une firme pivot d'un écosystème numérique. Les utilisateurs de leurs services évoluent souvent dans un univers logué. Ils s'identifient pour accéder aux services. Non seulement la firme peut étayer ses prédictions sur leurs historiques mais de surcroît elle possède des données liées à de nombreuses activités différentes (navigation internet, localisation géographique, achats passés…). Enfin, la richesse des données accumulées sur de très nombreux consommateurs (les 4V : volume, vitesse, variété, véracité) leur permet de disposer d'algorithmes performants leur permettant de déduire en quasi-temps réel les préférences des utilisateurs à partir de leur comportement en ligne. Cela est efficace à la fois vis-à-vis d'un consommateur précis (qui s'est identifié) et de consommateurs dont un peut déduire qu'ils appartiennent à un

segment homogène. Même sans données personnelles, il est possible de rattacher un nouvel utilisateur à un segment donné et d'engager une stratégie de micro-ciblage.

Un enjeu spécifique porte sur le premier type de données citées : les données personnelles, notamment pour les nouveaux utilisateurs ou pour ceux qui n'ont pas encore consenti à leur collecte. La question est celle des conditions de recueil du consentement de l'utilisateur et de la transparence de l'information délivrée en matière de condition de collecte, de traitement et de valorisation des données recueillies.

La littérature en économie comportementale a mis en évidence un biais décisionnel de la part des utilisateurs de services numériques, tenant à une myopie quant aux enjeux liés à la protection des données personnelles. Les gains liés à un accord sont immédiats alors que les dommages sont potentiels, décalés dans le futur et seront difficilement attribuables à l'accord donné pour un service internet précis.

Il convient donc dans cette perspective de délivrer une information complète à l'utilisateur dans le cadre du recueil de son consentement. Le Règlement Général sur la Protection des Données Personnelles (RGPD) européen a apporté une première réponse. Des travaux ont montré que l'architecture de choix pouvait biaiser la décision des utilisateurs (Santos et al., 2020).

Les architectures de choix trompeuses en ligne ou *dark patterns* peuvent entrer en jeu à la fois pour la manipulation des décisions des consommateurs en ligne (de Marcellis-Warin et al., 2020 et 2022) mais également donc pour le recueil de leur consentement à la collecte de leurs données. Les architectures de choix trompeuses sont au cœur des préoccupations des autorités de concurrence, notamment en Europe. En avril 2022, la Competition and Markets Authority britannique publia un rapport sur les dommages potentiels des architectures de choix en ligne, tant pour les consommateurs que pour la concurrence elle-même (CMA, 2022).

En mai 2022, un rapport sur le même thème fut remis à la Commission européenne par Lupiáñez-Villanueva et ses collègues. Ces derniers montrent que les *dark patterns* sont souvent mis en œuvre dans une zone grise. Ils s'inscrivent entre des tentatives commerciales légitimes de persuasion et les techniques déloyales de manipulation. Leur étude montre que la quasi-totalité des plateformes sur lesquelles ont porté les investigations met en œuvre de telles architectures biaisées. Les *dark patterns* les plus répandus apparaissent être (1) les informations cachées, notamment quant au prix et la fausse hiérarchie, (2) la présélection des options, (3) le harcèlement ou *nagging*, (4) les annulations difficiles ou *roach motel* et (5) l'enregistrement forcé.

Luguri et Strahilevitz (2021) étaient parvenu à un résultat particulièrement intéressant et lourd de conséquences. Si les utilisateurs réagissent négativement aux *dark patterns* les plus

évidents, ils ne détectent que rarement les plus détournés, lesquels peuvent pourtant induire des dommages significatifs.

En avril 2021, la FTC organisa un atelier de recherche sur la question : "*Bringing Dark Patterns to Light: An FTC Workshop*[5]". La description des différents thèmes alors abordés peut utilement éclairer notre propos. Au-delà de questions de définition et de mesure de la diffusion des procédés, plusieurs questions tenaient à la capacité des consommateurs à les détecter et à l'appréhension des dommages pour les consommateurs et la concurrence qui peuvent procéder de leur mise en œuvre. Les préoccupations de la FTC étaient notamment liées à la vulnérabilité des consommateurs vis-à-vis de ces derniers. Non seulement, certains consommateurs sont particulièrement vulnérables aux manipulations en ligne mais la simple information délivrée au consommateur apparait comme insuffisante pour éviter les manipulations algorithmiques et donc pour prévenir des dommages. Face aux limites de l'autorégulation que pourraient mettre en place les firmes, la solution envisagée tenait à un enforcement plus résolu des règles du FTC Act[6].

Il convient en effet de relever que les *dark patterns* revêtent une importance particulière dans le contexte du développement de l'IA Premièrement, les informations collectées sont essentielles au développement des outils prédictifs, notamment d'apprentissage machine. Les utiliser pour collecter des données peut donc être particulièrement tentant. Deuxièmement, l'IA peut rendre leur mise en œuvre particulièrement efficace et donc lucrative à la fois au travers de la personnalisation croissante des prédictions algorithmiques et de la possibilité d'ajuster en temps réel les propositions faites aux clients en fonction des réponses apportées aux sollicitations proposées. La personnalisation et l'adaptation en temps réel des prédictions et des manipulations algorithmiques peuvent faire passer les architectures de choix biaisées de l'ère du *nudge* à celui de l'*hypernudge* (Yeung, 2017).

L'*hypernudging* peut conduire les consommateurs à agir à l'encontre de leur intérêt dans une mesure bien plus difficile à apprécier et à contrôler que par le passé dans la mesure où leurs préférences mêmes peuvent être construites par l'information qui leur est transmise et les stimuli qui leurs sont adressés[7].

Le contrôle de la captation des données est donc essentiel dans la mesure où la traçabilité de la mise en œuvre des stratégies

---

[5] https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop

[6] "Given that consumers may be unaware of dark patterns' effects on their behavior and decisions and therefore less likely to complain, what can the FTC and other regulators do to identify and combat deceptive, unfair, or otherwise unlawful dark patterns?" *Ibid*

[7] Notons en outre que dans la proposition de régulation européenne d'avril 2021 sur l'IA, les pratiques manipulatrices du consommateurs (en dehors des manipulations subliminales) ne sont pas prises en compte dans la liste des pratiques pouvant conduire à des décisions hautement conséquentes (voir de Marcellis-Warin et al., 2022).

manipulatrices en ligne peut être particulièrement difficile à réaliser. L'opacité des prix en ligne peut être liée à leur foisonnement mais également à leur personnalisation. Les différents messages ou stimuli qui peuvent être présentés à tel ou tel consommateur sont difficiles à mettre à jour dans des procédures lancées ex post. La question de la collecte des données est donc une première ligne de défense essentielle. Dans la mesure où les tactiques en causes ne peuvent être que très partiellement contrecarrées par les consommateurs via l'exercice d'une *option de sortie*, l'appui sur l'action des autorités de protection de la concurrence et des consommateurs est essentiel.

Les enseignements issus de la pratique de la Federal Trade Commission

La possibilité de développer, d'entraîner et de mettre en œuvre des solutions d'IA permettant un micro-ciblage des consommateurs voire des *augmented dark patterns* dépend étroitement de la capacité des firmes à collecter des flux de données nombreuses, diversifiées et sans cesse réactualisées. Si la phrase selon laquelle ces flux de données sont devenus le carburant de nos algorithmes est devenue un marronnier, elle n'en recouvre pas moins une validité certaine.

Nous nous proposons donc de nous pencher sur l'activité récente de la FTC pour envisager la façon dont elle se saisit de la question et les risques qu'elle a pu identifier pour le consommateur.

La supervision constante des caractéristiques et des comportements des consommateurs qui découle de la mise en œuvre des algorithmes constitue un risque significatif pour les consommateurs. Ces risques se subdivisent, selon la FTC, en quatre ensembles : la manipulation, la discrimination, l'exploitation et enfin la désincitation à participer à l'économie numérique (Levine, 2022).

Premièrement, les données accumulées sur l'utilisateur d'un service numérique peuvent être retournées contre ses intérêts : « *Bad actors can weaponize data to predict which types of techniques are likely to be most effective against an individual consumer* » (Levine, 2022, p.3). En d'autres termes, l'accès aux données permet de passer d'architectures de choix trompeuses uniformes quel que soit l'utilisateur à des stratégies individualisées. Le *dark pattern* passe du prêt à porter au sur mesure.

L'accès aux données ne doit pas d'ailleurs être réduit aux seules données collectées, observées ou déduites au sein d'un écosystème particulier. Il existe un marché secondaire de la donnée. Des courtiers en données (*data brokers*) peuvent accumuler des données de différentes sources pour proposer des services de ciblage

publicitaires. De la même façon, des plateformes peuvent passer des accords avec ces derniers ou avec d'autres acteurs (tels des opérateurs de cartes de crédit) pour compléter les données dont ils disposent et notamment les croiser pour en garantir la véracité.

L'activité des courtiers en données peut induire un double risque pour les consommateurs. D'une part, ils peuvent transmettre des données permettant à des vendeurs indélicats de cibler des catégories de clientèles particulières de consommateurs facilement manipulables car présentant un faible discernement ou souffrant d'assuétudes[8].

Deuxièmement, l'accès aux données personnelles permet la mise en œuvre de manipulations. Celles-ci se caractérisent en premier lieu par la réduction de l'éventail des choix possibles (de Marcellis-Warin et al., 2022). Une tactique (également détaillée par Ezrachi et Stucke, 2020) consiste à limiter l'exposition à certaines offres. Il s'agit du *boxing*. Les consommateurs ne peuvent savoir que certaines offres ne leur sont pas accessibles. Ils sont enfermés dans une bulle de filtre[9].

Cette discrimination a également un volet en matière d'exclusion de certaines catégories sociales pour lesquelles les données accumulées ou inférées conduisent à un refus d'accès au marché ou à un accès dans des conditions dégradées. Ce faisant, l'accumulation des données conduit à pérenniser et à renforcer des biais sociaux.

Le cas de l'accès au marché du crédit est emblématique de telles discriminations. La proposition de Règlement européen sur l'IA rendue publique en avril 2021 souligne cette question et met en exergue son impact en termes de risques pour les usagers : "AI systems used to evaluate the credit-score, or creditworthiness of natural persons should be classified as high-risk AI systems". Il s'agit donc de système d'IA à hauts risques. Ce souci est également déterminant dans des lois américaines comme l'Equal Credit Opportunity Act (ECOA) and le Fair Housing Act (FHA). Ce n'est pas la collecte de données qui créé la discrimination mais elle la confirme et produit des effets d'autant plus négatifs qu'ils ne sont plus autant visibles dans la mesure où les algorithmes fonctionnent comme des boîtes noires.

Troisièmement, l'accumulation de données facilite la mise en œuvre de stratégies d'exploitation. Ces stratégies peuvent prendre la forme de discriminations tarifaires comme nous le verrons dans

[8] Voir le cas de la procédure de plaider coupable d'un courtier devant la FTC en septembre 2020 pour avoir vendu des listes de consommateurs souffrant de la maladie d'Alzheimer (*suffering seniors*) ou âgés de plus de 55 ans et présentant une addiction au jeu (*oldies but goodies*). FTC. *List brokerage firm plead guilty to facilitating elder fraud schemes*. Press Release, 28 September 2020.

[9] Les applications sur le *marché des idées* sont à prendre en compte. Elles peuvent conduire à des phénomènes de cloisonnement de l'espace public et donc de polarisation politique, particulièrement nocifs pour le bon fonctionnement du système démocratique.

notre seconde partie. Elles peuvent également être mises en œuvre dans d'autres segments de la vie sociale, notamment dans le cadre de stratégies de surveillance des employés ou encore des assurés[10].

Les risques étant présentés, quels peuvent être les outils limitant les conséquences potentielles liées à l'accumulation des données ? A l'inverse de la solution adoptée dans le cadre du RGPD européen, la FTC américaine fait montre d'un très fort scepticisme quant à la solution de l'information de l'utilisateur et du recueil de son consentement.

Le cas de la sollicitation ATT mise en œuvre par Apple dans son iOS 14 en matière de recueil du consentement témoigne des biais qui peuvent exister en la matière. Imposer aux services concurrents un schéma d'*opt-in* alors que le refus du consentement au recueil des données pour ses propres services suppose un *opt-out* peut être à l'origine de phénomènes d'auto-préférence. Cela revient en l'espèce à faire bénéficier son service d'un biais de statu quo (*default settings*) alors que l'acceptation du service concurrent est présentée comme faisant courir un risque additionnel[11].

Le raisonnement de la FTC considère que faire peser la charge informationnelle sur le consommateur n'offre qu'une protection illusoire du fait du coût de l'accès à l'information : « *These notices are often vague and confusing even for careful readers, and they can be outright impenetrable to the average consumer* » (Levine, 2022, p.6).

Les différents outils algorithmiques qui pourraient être mis à disposition des utilisateurs pour identifier les conditions les plus critiques (voir de Marcellis-Warin et al., 2020) peuvent en outre être inopérants pour trois raisons. Premièrement, l'utilisateur est soumis à une surcharge informationnelle et veut consommer le service immédiatement. Deuxièmement, l'offre est souvent de type *take or leave it*[12]. Troisièmement les conditions sont volontairement

[10] Les employeurs et les compagnies d'assurance passent des contrats en situation d'information imparfaite (incomplète et asymétrique). La collecte de données avant la signature d'un contrat et durant celui-ci permet de réduire les difficultés liées à l'anti-sélection et à l'aléa moral. Il peut en découler pour certains employés ou assurés une impossibilité d'accéder au marché ou des conditions plus défavorables et précaires.

[11] Voir en la matière la décision de l'Autorité de la concurrence de mars 2021 qui a refusé la demande de mesures conservatoires présentée par des développeurs tiers et d'acteurs du marché de la publicité en ligne devant accéder au système d'exploitation mobile d'Apple mais qui a conclu à la nécessité de poursuivre l'instruction au fond. Autorité de la concurrence, décision n°21-D-07 du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS.

[12] Certaines plateformes devenant des infrastructures critiques de notre vie économique et sociale et certains écosystèmes numériques devenant incontournables pour les consommateurs, ces derniers ne peuvent refuser les conditions posées à l'accès au service. L'un des problèmes vient du rôle dual des firmes qui sont à la fois les opérateurs de services essentiels et des acteurs de

opacifiées (autoriser le transfert des données, à qui, avec quelle granularité ?) et changeantes dans le temps.

Comme le note Samuel Levine le directeur du bureau chargé de la protection du consommateur à la FTC (2022, p.6) : "*Even in the rare instances when notices are understandable, they might simply inform consumers that the company collects anything and everything it can, and can do with it whatever it wants. These notices can also be subject to repeated change, putting the consumer in the impossible situation of having to constantly monitor their products and services for amended terms and policies*".

De la même façon, la propension à accepter de transmettre des données personnelles est liée pour le consommateur à une mauvaise évaluation des risques. Le dommage possible est décalé dans le temps, il peut être occasionné dans une autre activité de marché et ne pas pouvoir être rattaché à une acceptation précise. La cession, la recombinaison, le traitement et la valorisation des données par de nombreux acteurs des marchés physiques et numériques créent des risques pour les consommateurs qu'ils ne peuvent raisonnablement prévenir eux-mêmes.

Dans la mesure où le recueil d'un consentement éclairé est biaisé par ces paramètres comportementaux et apparaît comme contraint par la nécessité d'accéder à un service, il en résulte aux yeux de la FTC l'existence d'une *coercition* sur le comportement des utilisateurs de services numériques. La voie qu'annonce suivre la FTC tient à l'activation de la Section 5 du FTC Act laquelle vise particulièrement les *unfair and deceptive practices.*

Ne pas révéler aux consommateurs la façon dont les données sont collectées ainsi que la façon dont elles sont traitées, valorisées et commercialisées peut être sanctionné comme une pratique trompeuse[13].

De la même façon, la Section 5 du FTC Act permet de sanctionner les pratiques déséquilibrées : « *The FTC Act defines unfair practices, as those that cause or are likely to cause consumers substantial harm that is neither reasonably avoidable nor outweighted by countervailing benefits to consumer or competition*[14] ». La Section permet également, à la

marché qui peuvent d'autant plus légitimement utiliser les données collectées qu'il s'agit de plateformes bifaces pour lesquelles la valorisation des données permet de « subventionner » une infrastructure et de rendre un service gratuit.

[13] La FTC a par exemple engagé une procédure en juin 2021 contre l'entreprise Flo Health Inc. qui s'était engagée à ne pas transmettre à des tiers les données accumulées sur ses utilisateurs en matière de santé (service de *data analytics*) mais qui les a valorisées auprès de grandes plateformes. La firme a dû dans le cadre d'une procédure négociée mettre en place un programme de conformité et ouvrir la possibilité d'une indemnisation des utilisateurs concernés. In the Matter of Flo Health Inc., 22 June 2021, 192 3133.

[14] Il convient également de relever que le FTC Act de 1914 donne les moyens à l'agence de réaliser des enquêtes sectorielles (Section 6b). Cela correspond à la finalité même de la FTC qui devait dans l'esprit de ses créateurs, au premier rang desquels Louis Brandeis, d'étudier des pratiques de marché problématiques et de mettre un terme à ces dernières de façon préventive. Voir son opinion dissidente

différence d'ailleurs de la Section 2 du Sherman Act, de traiter de pratiques qui pourraient être désignées dans le cadre européen comme des abus d'exploitation. Il ne s'agit pas en l'espèce de prix excessifs mais d'extraction excessive de données par rapport aux besoins liés à l'utilisation du service. La collecte excessive de données peut par exemple donner lieu à des utilisations conduisant à des discriminations sur d'autres marchés[15].

Comme nous le verrons *infra* dans le domaine de la concurrence, les remèdes qui se dégagent de la pratique décisionnelle de la FTC tiennent souvent à la suppression des données indûment collectées[16].

Un cas récent et emblématique tient à la procédure négociée conclue le 25 mai 2022 entre la FTC et Twitter[17]. L'opérateur de la plateforme de micro-blogging a indûment présenté jusqu'en 2019 sa procédure de double identification (numéro de téléphone cellulaire et adresse de courriel) comme un outil de récupération et de sécurisation des comptes des utilisateurs sans autre utilisation des données collectées. Or, il s'est avéré que cette procédure d'information et de recueil du consentement était biaisée. Non seulement la revente des données était cachée aux utilisateurs mais l'argument de sécurité affiché était de nature *déceptive*[18]. Un utilisateur standard ne pouvait aller au-delà des déclarations de la firme pour analyser les termes généraux d'utilisation du service.

De la manipulation du consommateur à la distorsion de concurrence

Nous montrons tout d'abord que la manipulation du consommateur peut être à la source d'un avantage concurrentiel au profit de la firme qui la met en œuvre. Nous revenons ensuite, comme dans notre première partie, sur la pratique décisionnelle de la FTC pour envisager les mesures correctives à même de corriger ces effets.

---

dans l'arrêt Gratz de la Cour Suprême américaine (FTC v. Gratz, 253 U.S. 421, 1920).

[15] Voir le *Joint Statement* de Lina Khan et Rebecca Slaughter dans le cas *In Re Napoleon Auto Group,* FTC 202 3195, 31 March 2022.

[16] Voir le communiqué de presse de la FTC du 15 mars 2022 : FTC Takes Action Against CafePress for Data Breach Cover Up.

[17] See United States District Court, Northern District of California, May 2022, US v Twitter Inc., Complaint for civil penalties, permanent injunction, monetary relief, and other equitable relief.

[18] Statement of Lina Khan Joined by Rebecca Slaughter in the Matter of Twitter Inc. Commission File n°2023062, 25 May 2022.

« Deception distorts competition »

La manipulation du comportement du consommateur et la restriction artificielle de l'éventail des choix qui lui sont offerts peuvent induire des dommages non seulement à ce dernier mais également au processus de concurrence lui-même.

Il ne s'agit pas pour autant de considérer que les manœuvres en cause sont négatives en elles-mêmes. Restreindre l'éventail des choix offerts aux consommateurs peut répondre au problème de la *tyrannie des choix* (*choice overload*) et générer des gains d'efficacité en réduisant les coûts de transaction (en l'espèce les coûts de recherche). De la même façon, le propre même des recommandations est de réaliser un meilleur appariement entre l'offre et la demande, voire de faire découvrir de nouvelles solutions non encore connues par le consommateur. Les *nudges* et les *sludges* peuvent être bienveillantes (*bénévolentes*) et se rattacher à une logique de parternalisme libéral. Enfin, l'existence même d'une discrimination (par les prix ou par les qualités) ne conduit pas inéluctablement à une perte en termes d'efficacité (i.e. de maximisation du bien-être du consommateur en termes agrégés) et peut avoir des mérites en termes redistributifs (Marty, 2019a). Les subventions croisées entre consommateurs qui résultent de prix personnalisés peuvent permettre à certains d'accéder à la consommation ce qu'ils n'auraient pu faire en cas d'application d'un prix uniforme.

Pour autant, des risques concurrentiels sont à prendre en considération. Premièrement, l'efficacité n'est pas le seul objectif légitime de la politique de concurrence. De façon subséquente, il est possible de considérer que le critère de la maximisation du bien-être du consommateur, n'est pas le seul critère envisageable pour la mise en œuvre des règles de concurrence[19].

La concurrence repose également sur la préservation de la liberté de choix des consommateurs et sur l'exercice tant par ces derniers que par les autres acteurs du marché (notamment les firmes utilisatrices des services d'intermédiation numérique) de leur souveraineté économique. Même si la plateforme exerce ses choix dans un sens purement bénévolent (i.e. maximise le bien-être de l'ensemble des participants à son écosystème), la liberté des agents économique et la libre concurrence comme processus de découverte et de révélation des connaissances ne sont plus garantis.

[19] Voir Jonathan Kanter (2022), Assistant Attorney General à la tête de la Division Antitrust du DoJ, pour une critique récente du critère du bien-être du consommateur par les autorités américaines.

Protéger la concurrence revient à permettre la pérennité d'un processus et non sanctionner un résultat[20]. Cette approche est celle de la législation européenne sur les marchés numériques (ci-après DMA, Digital Markets Act) définitivement adopté par le Conseil de l'U.E. le 18 juillet 2022. L'objet n'est pas l'efficacité économique en elle-même, qui est le résultat d'une concurrence libre et non faussée, mais la garantie des conditions de cette même concurrence. Celles-ci se décomposent en deux sous-objectifs : la préservation de la contestabilité des marchés et celle de la loyauté des relations commerciales qui se nouent sur ces derniers. Le premier sous-objectif vise à la fois à permettre l'accès au marché des entreprises utilisatrices des services d'intermédiation et à pérenniser les conditions d'une mise en cause des positions dominantes de l'heure[21]. Le second objectif vise à garantir l'équité et la loyauté de la concurrence dans des écosystèmes où un opérateur dominant est à la fois un acteur du marché et son « régulateur privé ».

Orienter les choix des consommateurs pose problème dans ce cadre que l'objectif soit bienveillant (maximisation du bien-être des participants à l'écosystème numérique) ou non (mise en œuvre de stratégies d'auto-préférence). Les enjeux sont d'ailleurs les mêmes qu'il s'agisse du marché des biens et services ou de celui « des idées ». Orienter les propositions adressées aux utilisateurs des services numériques en matière d'information politique ou de contenus conduit inéluctablement à la réduction du périmètre des choix possibles et à leur orientation. L'exposition biaisée peut être conforme aux préférences mêmes des consommateurs ou être alignée avec les intérêts d'une firme active sur le marché de l'attention. Elle peut maximiser le bien-être de l'utilisateur ou celui de la plateforme… mais elle peut produire des effets politiques collectivement non souhaitables.

Ce qui est vrai de l'orientation utilitariste des choix l'est encore plus pour la tromperie et la manipulation. Vis-à-vis du consommateur, la question est celle d'une extorsion de surplus ; laquelle est d'autant plus dommageable que le consommateur est vulnérable. Vis-à-vis des autres opérateurs du marché, la question est celle de l'entrave au processus même de concurrence ou de l'exploitation d'une situation de dépendance économique.

Mentir au consommateur ou à plus forte raison le manipuler induit une distorsion de concurrence. Une concurrence non faussée doit préserver les préférences du consommateur. Décevoir celles-ci par des manœuvres déloyales offre à l'entreprise concernée

[20] Cette approche qui conduit à protéger le processus de concurrence en lui-même et non de limiter l'examen à seule efficacité allocative fait écho à une approche ordolibérale (Wörsdöfer, 2022).

[21] Notons que l'avantage lié aux données peut d'autant plus s'accroître que les opérateurs dominants se proposent, pour défendre leurs usagers, de limiter la possibilité de mise en œuvre de traceurs (*cookies*) par les tiers. Les effets en termes de protection du consommateur peuvent alors avoir pour contrepartie des effets restrictifs de concurrence (Coeuré, 2022).

un avantage dont ne peuvent disposer les entreprises qui n'engagent pas de telles manœuvres.

Comme l'a montré à l'automne 2020, Rohit Chopra dans son opinion dissidente dans la procédure négociée entre la FTC et Zoom[22], *deception distorts competition*. Une tromperie sur des caractéristiques essentielles du service (en l'espèce son niveau de sécurité – apprécié ici au travers de son chiffrage) peut permettre à une entreprise de gagner un avantage concurrentiel déterminant sur ses concurrents[23]. Non seulement elle supporte moins de coûts mais elle attire plus d'utilisateurs. Les effets sur la concurrence dans le numérique peuvent être particulièrement importants dans le numérique dans la mesure où il s'agit d'un secteur où les coûts marginaux sont faibles et les effets de réseaux particulièrement élevés. Un avantage « indu » lors de la phase de décollage du marché peut se traduire par un avantage productif de long terme. Une position dominante écrasante et durable peut être le résultat d'une stratégie de tromperie initiale. La cessation des pratiques en cause permet en aucun cas à elle seule de rétablir les conditions qui auraient été celles de la concurrence en l'absence des pratiques en cause. La faute peut être lucrative…

Ce point conduisit d'ailleurs Rohit Chopra a considéré que le remède était peu dissuasif, peu effectif et ne permettrait pas de rétablir les conditions de la concurrence. Pour reprendre les termes utilisés par deux autres commissaires de la FTC, Rohit Chopra considérait que « the final order is "weak," provides "no money" and that the injunctive relief constitutes "paperwork requirements" with no real accountability »[24].

Se pose alors la question de la portée des remèdes concurrentiels.

Quels remèdes concurrentiels ? Analyse de la pratique décisionnelle de la Federal Trade Commission

La législation européenne sur les marchés numériques (DMA) insiste sur deux dimensions concurrentielles qui ne peuvent être réduites au critère habituel de l'efficacité. Le premier tient à la contestabilité des positions dominantes et le second à la loyauté de la concurrence dans l'espace numérique. Il s'agit en effet de mettre l'accent sur plusieurs problèmes spécifiques à l'économie des écosystèmes numériques.

Premièrement, les opérateurs dominants ont une forte probabilité d'être plus efficaces que leurs concurrents, non pas du

[22] Dissenting Statement of Commissioner Rohit Chopra regarding Zoom Video Communication Inc. February 2021.
[23] Pour une présentation du cas se reporter à de Marcellis-Warin et al. (2020).
[24] Concurring Statement of Commissioner Christine Wilson and Noah Philipps, FTC, Twitter, Matter n°2023062, 25 May.

fait de leurs capacités à innover mais du fait du contrôle de vastes flux de données et de leur capacité à orienter le comportement de l'ensemble des participants à leur écosystème. Les effets de réseaux et l'avantage lié aux données ont pour effet de verrouiller les positions dominantes mais également de rendre ces opérateurs bien plus profitables que leurs concurrents. En effet, leurs capacités de micro-ciblage des profils et de manipulation des comportements en ligne leur donnent des avantages déterminants sur le marché de la publicité en ligne.

Cet avantage sur le marché de l'attention doit être replacé en perspective avec les deux autres caractéristiques citées qui sont déterminantes dans le DMA européen. Il s'agit d'abord de la faible contestabilité des positions. Le verrouillage de la position dominante est lié au contrôle des flux de données et aux avantages qui en découlent tout autant qu'aux effets de réseaux, aux coûts de changement pour les autres parties prenantes etc… Le second critère, celui de la *fairness* – ou en l'espèce loyauté – est également lié à cette situation. Il est aisément possible d'induire des distorsions de concurrence à son profit en manipulant l'information accessible aux consommateurs au profit de ses produits et au détriment de ceux proposés par ses concurrents[25]. Il est également possible de créer un avantage informationnel vis-à-vis de ces derniers pour pouvoir cloner leurs produits ou faire peser sur eux une menace crédible d'éviction de nature à les pousser à accepter des conditions contractuelles même si elles sont manifestement déséquilibrées[26].

L'action promue par la FTC en la matière se subdivise en deux voies qui peuvent être riches d'enseignements tant en matière de protection du consommateur qu'en matière de protection de la concurrence. La première est de *reverse structural incentives to maximise information collection and abuses*. La seconde tient à *obtaining strong, forward-learning remedies that […] cure the underlying harm* (Levine, 2022, p.10).

Les remèdes proposés ne vont pas aussi loin que ceux qui le furent par Gal et Petit (2021). Il ne s'agit pas de partager les algorithmes indûment entraînés avec ses concurrents, de cesser transitoirement son activité sur le marché concerné par la pratique ou de subventionner d'une façon ou d'une autre les investissements des concurrents pour leur permettre de corriger les effets de l'avantage acquis au travers de la pratique incriminée. La pratique décisionnelle de la FTC s'oriente vers des injonctions conduisant à l'annulation de l'avantage compétitif indûment acquis. Ces remèdes tiennent non seulement à l'effacement des données accumulées

[25] Pour une application à l'adoption d'une application ou d'une autre dans les écosystèmes mobiles voir notamment Ezrachi et Stucke (2020).

[26] Voir sur ce sujet la procédure formelle ouverte par la Commission européenne à l'encontre d'Amazon à l'automne 2020 (Commission européenne, affaire AT.40703, communiqué de presse du 10 novembre 2020 – IP 20_277). Sur les pratiques alléguées et les avantages informationnels tenant à la position de pivot d'un écosystème numérique, voir Marty F., (2019b).

dans le cadre des pratiques en cause[27] mais aussi à la destruction des algorithmes qui ont été développés ou entraînés grâce à elles[28].

Discussion sur l'efficacité de la protection du consommateur et de la concurrence

La loi européenne sur les services numériques (DMA) s'est en grande partie fondée sur la prise en compte de la faible effectivité des remèdes concurrentiels. Sont-ils suffisamment élevés pour être dissuasifs ? Permettent-ils d'imposer des remèdes suffisants pour rétablir les conditions de la concurrence qui auraient été celles qui auraient prévalu en l'absence des pratiques. De la même façon, malgré l'augmentation du quantum des sanctions pécuniaires, le RGPD fournit-il un cadre suffisamment dissuasif pour prévenir les infractions à la protection des données personnelles[29] ?

Le DMA semble porter sur cette question en posant ex ante des pratiques interdites – pour prévenir l'occurrence du dommage -, en augmentant les plafonds de sanctions encourues (20% du chiffre d'affaires contre 10% en matière concurrentielle) et en ouvrant la voie à des mesures structurelles.

La FTC fait-elle face à de mêmes difficultés ? A nouveau le cas Twitter du 25 mai 2022 peut être instructif en ce qu'il illustre de façon très opportune ce débat. Le *consent decree* entre la FTC et Twitter se traduit par une injonction à cesser les pratiques mais également par une transaction à hauteur de 150 millions de dollars. La somme peut paraître anecdotique en regard des trois sanctions qu'avait prononcé la Commission européenne contre Google entre 2017 et 2019 et qui avaient avoisiné les 10 milliards de dollars. Nous allons cependant voir que cette somme est significative.

Un premier point à considérer tient au fait qu'une « sanction pécuniaire[30] » a été prononcée. A l'inverse du *consent decree* de l'automne 2020 avec Zoom, la seule cessation des pratiques ne suffit pas. L'écart entre les deux procédures négociées s'explique aisément. Le but du FTC Act n'est pas de sanctionner des pratiques

[27] Communiqué de presse de la FTC du 21 décembre 2021 : FTC Finalizes Order Banning Stalkerware Provider from Spyware Business.

[28] Communiquées de presse de la FTC du 4 mars 2022 : FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data. Voir également hors du champ des activités économiques pour une illustration dans la sphère de l'information : communiqué de presse de la FTC du 6 décembre 2019 : FTC Issues Opinion and Order Against Cambridge Analytica for Deceiving Consumers about Collection of Facebook Data, Compliance with EU-US Privacy Shield.

[29] Pour une comparaison des sanctions en matière de protection des données personnelles et de concurrence, se reporter à Bouthinon-Dumas et al. (2022).

[30] Le terme de sanction est impropre dans la mesure où elle s'agit d'une procédure négociée, en l'espèce de l'équivalent d'une transaction.

mais de prévenir les effets de pratiques déloyales sur le marché. Son but est préventif et non curatif. Ensuite, cette procédure négociée fait suite à un premier *consent decree* de 2011 par lequel Twitter s'engageait à ne pas utiliser indûment les données des utilisateurs et de présenter de façon non biaisée ses règles en matière de protection des données personnelles[31]. Pourquoi somme nous ici à nouveau dans le cadre d'une procédure transactionnelle ? La raison que Twitter qui s'était écarté de ses engagements entre mai 2013 et septembre 2019 du fait de la mise en place de la procédure de double identification a mis volontairement fin aux pratiques en cause et les a publiquement révélées[32].

Il s'agit du point le plus important, le changement de stratégie de Twitter s'explique par la procédure entamée en 2019 par la FTC contre Facebook[33]. Les remèdes sont équivalents dans les deux cas. Le signal constitué par la procédure entamée dans l'affaire Cambridge Analytica a conduit à une mise en conformité de Twitter.

Ces remèdes sont-ils suffisants ? Un élément de réponse peut être apporté par le *concurring statement* des commissaires Wilson et Phillips cité *supra*. Tant dans Facebook (2019) que Twitter (2022), les deux plateformes s'engagent dans une politique de conformité qui passe notamment par les procédures suivantes : réaliser une évaluation préalable des risques liés à la protection des données personnelles pour chaque modification du service, engager des audits de conformité en matière de protection des données personnelles, mettre en œuvre des procédures de publicité et de retour d'expérience pour chaque incident et responsabiliser les dirigeants directement.

Dans les deux cas, le modèle économique de la firme n'est pas remis en cause. Il est possible d'utiliser les données à des fins de ciblage publicitaire mais l'information donnée au public doit être exploitable. Dans les deux cas, un souci particulier doit peser sur l'utilisation des numéros de cellulaire.

Ces remèdes montrent l'importance de la conformité comme remède concurrentiel. L'entreprise doit auto-évaluer ses pratiques

---

[31] FTC, communiqué de presse du 11 mars 2011, FTC accepts final settlements with Twitter for failure to safeguard personal information.

[32] Le modèle économique de Twitter repose sur la monétisation des données relatives à ses utilisateurs. En 2019 sur 3,4 milliards de dollars de chiffre d'affaires, 2,99 venaient de la publicité. La valorisation publicitaire vient de trois canaux. Le premier est celui des tweets sponsorisés, le second celui des comptes suggérés et le dernier celui des tendances personnalisées. Au-delà de ces trois prestations les services marketing de Twitter proposent des audiences personnalisées. Celles-ci se basent les numéros de téléphone et les adresses de courriel des utilisateurs. Les annonceurs peuvent croiser ces données avec celles qu'ils possèdent par ailleurs pour identifier leurs comptes cibles. Le programme Partner Audience permet à ce titre d'importer des listes issues de certains courtiers en données (Axciom ou Datalogic) pour opérer ces croisements. Voir la plainte US v Twitter de mai 2022 citée *supra*.

[33] U.S. v. Facebook, No. 1:19-cv-2184 (D.D.C. July 24, 2019).

et s'auto-contrôler dans une logique de supervision déléguée (Kirat et Marty, 2015).

Pour autant, une pratique trompeuse à l'encontre du consommateur et porteuse de distorsions au détriment des concurrents peut-elle être « pardonnée » par la seule cessation des pratiques et mise en œuvre d'un programme de conformité ?

Les dommages liés à l'avantage induit par l'accès aux données et à partir de là à l'entraînement des algorithmes pourraient ne pas être compensés et le comportement fautif pourrait être « rationnel » considéré sous l'angle d'un calcul coûts-avantages. Ce serait oublier trois points.

Premièrement dans certains cas, la FTC a imposé la destruction des algorithmes indûment entraînés pour éliminer une source déloyale d'avantage concurrentiel. Ce fut le cas dans l'affaire Everalbum[34].

Deuxièmement, une procédure même négociée a un impact sur la réputation de la firme qui peut être lourd de conséquences si ses parties prenantes et notamment les porteurs de parts sociales s'engagent dans une démarche éthique de responsabilité sociale des entreprises.

Troisièmement, le montant auquel s'établit la transaction avec la FTC peut ne pas apparaître comme anecdotique même pour une grande firme. Dans le cas de Facebook en 2019, la transaction s'est faite pour 5 milliards d'euros soit 9% du revenu annuel de l'entreprise[35]. Dans le cas de Twitter, les 150 millions représentent 3% de ses revenus. Ils ont un impact d'autant plus élevé que la société faisait l'objet d'un projet de rachat.

---

[34] Everalbum, Inc., In the Matter of, FTC, case 192 3172, 7 May 2021."Within ninety (90) days after the issuance of this Order, delete or destroy all Face Embeddings derived from Biometric Information Respondent collected from Users who have not, by that date, provided express affirmative consent for the creation of the Face Embeddings, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed; and Within ninety (90) days after the issuance of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction".

[35] Dans leur *concurring statement*, Wilson et Phillips (2022) s'opposent à l'analyse que fit en 2019 Rohit Chopra du montant imposé dans le cas de Facebook. Pour ce dernier les 5 milliards de dollars n'étaient pour le groupe qu'un *slap on the wrist*. Voir Dissenting Statement of Commissioner Rohit Chopra, In Re Facebook, FTC 24 July 2019.

Bibliographie

Bouthinon-Dumas H., Marty F. and Voss W.G. (2022). Une comparaison des sanctions en droit financier, droit des données personnelles et droit de la concurrence, *in* Bréhier B., dir., *Mélanges AEDBF VIII*, pp.379-387, Revue Banque éditions.

Coeuré B., (2022), Droit de la concurrence et protection des données personnelles, Autorité de la Concurrence – intervention devant le Collège de la CNIL, juin. https://www.autoritedelaconcurrence.fr/sites/default/files/2022-06/20220608-CNIL-discours_0.pdf

Competition & Markets Authority. (2022). Online Choice Architecture. How digital design can harm competition and consumers. Discussion Paper CMA 155, April.

De Marcellis-Warin N., Marty F., Thelisson E., et Warin T. (2020), Intelligence artificielle et manipulations des comportements de marché : l'évaluation ex ante dans l'arsenal du régulateur. *Revue Internationale de Droit Economique*, volume XXXIV, 2020/2, pp.203-245.

De Marcellis-Warin N., Marty F., Thelisson E., and Warin T. (2022), Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools. *AI & Ethics,* 2(2), May, pp.259-268.

Gal M. and Petit N. 2021. Radical Restorative Remedies. *Berkeley Technology Law Journal.* 36. Pp. 617-674.

Ezrachi, A., Stucke, M.E. (2020) Digitalisation and its impact on innovation. *Working Paper* 2020/07, October R&I Paper Series, European Commission. https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/digitalisation-and-its-impact-innovation_en

Kanter J., (2022), "Remarks at New York City Bar Association's Milton Handler Lecture", US DoJ, 18 May.

Kirat T. and Marty F. (2015). The regulatory practice of the French Financial Regulator, 2006-2011. From substantive to procedural financial regulation? *Journal of Governance and Regulation*, 4(4), pp.441-450.

Levine S. (2022). Concluding Remarks. Cleveland-Marshall College of Law – Cybersecurity and Privacy Protection Conference. FTC, 19 May.

Luguri J., Strahilevitz L.J. (2021). Shining a Light on Dark Patterns, *Journal of Legal Analysis.* Volume 13, Issue 1, pp. 43–109

Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al.. (2022). Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization. European Commission, Directorate-General for Justice and Consumers, final report. May.

Marty F. (2019a). Plateformes numériques, algorithmes et discrimination, *Revue de l'OFCE*, volume 164, 4-2019, pp.47-86

Marty F. (2019b). Plateformes de commerce en ligne et abus de position dominante : réflexions sur les possibilités d'abus d'exploitation et de dépendance économique". *Revue Juridique Thémis de l'Université de Montréal*, volume 53, 2019, pp. 73-104

Morozovaite V. (2021). Two Sides of the Digital Advertising Con: Putting Hyernudging into Perspective. *Market and Competition Law Review*, V(2), pp.105-145.

Santos C., Bielova N., and Matte C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *International Journal on Technology and Regulation* (TechReg), 91–135.

Wörsdörfer M. (2022). What Happened to 'Big Tech' and Antitrust? And How to Fix Them! *Philosophy of Management, à paraître.*

Yeung A. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society.* 20(1), pp. 118-136.