Groupe de travail sur le citoyen et le consommateur numérique

Rapport – Août 2021

Présenté au nom du GTCCN par les coprésidents – Commissariat à la protection de la vie privée du Canada (CPVP) et l'Office of the Australian Information Commissioner (OAIC)

Table des matières

Résumé

Formé en 2017, le Groupe de travail sur le citoyen et le consommateur numérique (GTCCN) se concentre sur l'examen des intersections des sphères réglementaires de la protection de la vie privée, de la protection des consommateurs et de la concurrence (également appelée antitrust) ainsi que sur la promotion de la coopération réglementaire en la matière. Notre travail, qui est au cœur de la stratégie de l'Assemblée mondiale pour la protection de la vie privée (AMVP)[1], vise à faciliter la coopération et la collaboration en matière de réglementation afin de créer un environnement réglementaire mondial doté de normes claires et strictes en matière de protection des données[2]. Le GTCCN offre une tribune qui favorise le dialogue, la coopération et le partage des expériences en lien avec les questions d'intersection. Il vise également à faire avancer l'utilisation des cadres existants, ou à favoriser la création de nouveaux cadres, par les autorités des trois sphères réglementaires pour que ces derniers puissent travailler ensemble et obtenir des résultats supérieurs en matière de protection des données et des consommateurs au profit de la société.

Le mandat et le travail du GTCCN n'ont jamais été aussi pertinents. Cette constatation se reflète dans l'attention grandissante apportée aux questions d'intersection qui prend la forme de nouvelles lois et réglementations, d'initiatives stratégiques, de demandes de renseignements et d'une application croissante de la loi par les autorités de réglementation dans l'ensemble des sphères réglementaires. Cet entrecroisement, qui a souvent donné des résultats positifs, a parfois créé de nouvelles tensions. Les données, qui sont au centre de notre économie numérique, ne se conforment pas aux limites réglementaires ou géographiques. Il est évident qu'une meilleure compréhension et collaboration de la part des autorités à travers ces sphères réglementaires s'avère nécessaire pour obtenir des résultats réglementaires optimaux sur les plans de la protection de la vie privée, de la protection des consommateurs et de la concurrence. En fait, comme il est indiqué dans le présent rapport ainsi que dans ses annexes, nous avons constaté que, lorsqu'une collaboration de ce genre prend forme, il est possible de mettre l'accent sur les aspects qui sont complémentaires et d'atténuer les tensions afin de faire avancer les objectifs de chaque sphère réglementaire.

Les autorités de protection des données, les autorités de protection des consommateurs, les autorités en matière de concurrence, d'autres autorités publiques, la société civile et des organismes s'intéressent de plus en plus à notre travail. Nous regroupons 18 organismes, dont quatre nouveaux membres. Le GTCCN a également accueilli son troisième observateur, le Bureau Européen des Unions de Consommateurs, également appelé le BECU[3], qui apporte une nouvelle perspective sur les questions d'entrecroisement. Tandis que les organismes de réglementation puisent dans les leçons tirées à travers ces sphères réglementaires, notre groupe de travail

[1] Qui s'appelait à l'époque la Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC).

[2] Global Privacy Assembly, 'Strategic Plan 2019-2021', page 4-6. Voir : http://globalprivacyassembly.org/wp-content/uploads/2019/11/GPA-Strategic-Plan-2019-2021.pdf.

[3] L'acronyme du Bureau Européen des Unions de Consommateurs.

continue d'offrir une tribune pour cette collaboration importante dans le contexte d'un paysage technologique en constante évolution. En parallèle, les représentants du GTCCN sont très sollicités pour prononcer des allocutions dans le cadre d'événements qui favorisent la collaboration inter-réglementaire ainsi que la sensibilisation aux questions d'entrecroisement. Ces forums de mobilisation englobent les réseaux, les conférences, les forums universitaires ainsi que les événements d'associations professionnelles.

La résolution du GTCCN, adoptée par les membres de l'AMVP en 2019, a établi un mandat de deux ans pour le groupe de travail. Alors que nous arrivons à la fin du mandat, le présent rapport annuel nous donne l'occasion de faire un survol de notre œuvre. En posant un regard sur l'avenir, le GTCCN est emballé de continuer à consolider ses réalisations et il constate la pertinence de poursuivre cette tâche importante en tant que groupe de travail permanent de l'AMVP en réponse à la demande à l'échelle mondiale.

Nous sommes heureux de présenter ce rapport à l'occasion de la session fermée 2021 de l'AMVP en espérant que les membres jugeront nos contributions utiles.

Office of the Australian Information	Commissariat à la vie privée du Canada
Coprésident	Coprésident

Introduction

Le GTCCN étudie les intersections entre la protection de la vie privée et les données ainsi que la protection des consommateurs et la concurrence. Le travail, qui fait partie intégrante de l'AMVP et qui s'inscrit dans sa stratégie, soutient ses ambitions stratégiques qui entourent le leadership ainsi que la coopération et la collaboration en matière de réglementation afin de créer « un environnement réglementaire mondial doté de normes claires et élevées en matière de protection des données »[4].

Le groupe de travail a initialement été créé à l'occasion de la 39e Conférence internationale des commissaires à la protection des données et de la vie privée (maintenant appelé l'AMVP) grâce à la résolution portant sur la collaboration entre les autorités de protection des données et de protection des consommateurs pour améliorer la protection des citoyens et des consommateurs dans l'économie numérique.

En 2019, l'AMVP a adopté une résolution qui revisitait le mandat du groupe de travail afin qu'il tienne compte des interactions entre les sphères réglementaires de la protection de la vie privée et des données, de la protection des consommateurs et de la concurrence[5]. Cette résolution a façonné l'orientation stratégique du groupe de travail dans les buts suivants :

- **nous amener à mieux comprendre** l'entrecroisement de la protection de la vie privée et de la concurrence;
- **continuer d'explorer, de comprendre et de cartographier les entrecroisements réglementaires**, surtout celles qui concernent les progrès dans les activités liées aux politiques, aux lois et à l'application de la loi;
- **sensibiliser les autorités et les réseaux** aux problèmes liés aux entrecroisements réglementaires et favoriser une collaboration inter-réglementaire;
- **déterminer les initiatives collaboratives et miser et s'appuyer sur elles** et les réseaux qui tiennent compte des questions d'entrecroisement.

Le présent rapport vise à renseigner l'AMVP au sujet du travail accompli par le GTCCN au cours de l'année 2021 et à définir les grandes lignes des tâches à venir tandis qu'il poursuit son exploration des entrecroisements entre la protection de la vie privée, la protection des consommateurs et la concurrence et qu'il se tourne vers d'autres domaines potentiels d'entrecroisement réglementaire dans l'économie numérique.

---

[4] Global Privacy Assembly, 'Strategic Plan 2019-2021', page 4-6. Voir : http://globalprivacyassembly.org/wp-content/uploads/2019/11/GPA-Strategic-Plan-2019-2021.pdf.

[5] Lors de 41e Conférence internationale des commissaires à la protection des données et de la vie privée, on a adopté une résolution pour favoriser et faciliter la coopération réglementaire entre les autorités de protection des données, les autorités de protection des consommateurs et les autorités en matière de concurrence afin d'atteindre des normes claires et constamment élevées en matière de protection des données dans l'économie numérique. Voir : http://globalprivacyassembly.org/wp-content/uploads/2019/11/DCCWG-Resolution_ADOPTED.pdf.

Le GTCCN a régulièrement fait rapport au sous-comité de l'orientation stratégique (SDSC) sur les progrès de son travail dans le cadre de présentations à des réunions de réflexion approfondie et sous la forme de rapports trimestriels par écrit. Les coprésidents du GTCCN ont fait des exposés lors de la septième réunion du SDSC en mai 2021. Les présentations du GTCCN ont été bien accueillies par le SDSC, qui a reconnu la contribution importante du GTCCN à la réalisation des objectifs de coopération réglementaire énoncés dans la stratégie politique de l'AMVP. Plus particulièrement, le GTCCN a fait rapport sur les efforts de sensibilisation déployés pour attirer l'attention du monde extérieur sur les travaux du GTCCN et de l'AMVP.

Voici les membres et/ou les observateurs actuels du GTCCN :

- Office of the Australian Information Commissioner (coprésident)
- Commissariat à la vie privée du Canada (coprésident)
- Autorité belge de protection des données, Belgique
- Datatilsynet, Danemark
- Datatilsynet, Norvège
- Contrôleur européen de la protection des données, Europe
- Commissaire fédéral chargé de la protection des données et de l'accès à l'information, Allemagne
- Federal Trade Commission, États-Unis
- Information Commissioner's Office, Royaume-Uni
- National Privacy Commission, Philippines
- Surintendance de l'industrie et du commerce, Colombie
- Commissaire à la protection des données personnelles, Sénégal (nouveau membre)
- Commission nationale pour la protection des données personnelles, Gabon (nouveau membre)
- Service de l'inspecteur de l'État de la Géorgie, Géorgie (nouveau membre)
- Institut national pour la transparence, l'accès à l'information et la protection des données personnelles (INAI), Mexique (nouveau membre)
- Bureau Européen des Unions de Consommateurs (BEUC) (nouvel observateur)
- Autorité des consommateurs et des marchés, Pays-Bas (observateur)
- Personal Data Protection Commission, Singapour (observateur)

Activités du groupe de travail

Le plan de travail 2020-2021 du GTCCN compte quatre champs de travail :

1. Mener une réflexion approfondie sur la protection de la vie privée et la concurrence
2. Poursuivre la sensibilisation et la mobilisation dans d'autres forums
3. Suivre et faciliter une coopération inter-réglementaire réelle
4. Contribuer au manuel de coopération en matière d'application de la loi de l'AMVP

La deuxième année du mandat actuel du GTCCN a été couronnée de succès. Tout au long de l'année 2021, le GTCCN a respecté les engagements de la résolution et atteint les objectifs dans son plan de travail. Cette section du rapport donne un aperçu du travail accompli au cours de la deuxième année de notre mandat.

1. *Mener une réflexion approfondie sur la protection de la vie privée et la concurrence*

Dans le cadre de notre plan échelonné sur deux ans, nous nous sommes donné comme objectif de mieux comprendre les intersections entre la protection de la vie privée et la concurrence. Le GTCCN a réalisé cet objectif en diffusant deux rapports complémentaires – le rapport rédigé par le GTCCN qui est intitulé Privacy and Data Protection as *Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration* [La protection de la vie privée et des données en guise de facteurs dans la réglementation de la concurrence : sondage auprès des autorités de réglementation de la concurrence visant à améliorer la collaboration inter-réglementaire] et le rapport universitaire indépendant commandé de la professeure Erika Douglas intitulé *Digital Crossroads: The Intersection of Competition Law and Data Privacy* [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données].

Privacy and Data Protection as Factors in Competition Regulation [La protection de la vie privée et des données en guise de facteurs dans la réglementation de la concurrence]

Comme il est mentionné dans notre rapport annuel de 2020, le GTCCN s'était donné comme objectif de mener une série d'entrevues avec des autorités de réglementation de la concurrence afin de recueillir d'autres perspectives sur cette intersection. Après avoir réalisé nos entrevues avec 12 autorités en matière de concurrence différentes des quatre coins du monde, nous avons distillé leurs opinions, leurs pratiques et leurs études de cas dans le rapport intitulé Privacy and Data Protection as *Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration* [La protection de la vie privée et des données en guise de facteurs dans la réglementation de la concurrence : sondage auprès des autorités de réglementation de la concurrence visant à améliorer la collaboration inter-réglementaire].

Le rapport visait à :

(i) comprendre comment les autorités en matière de concurrence tiennent compte des éléments liés à la protection de la vie privée et aux données lorsqu'elles effectuent leurs analyses antitrust;

(ii) tirer parti des points de vue et des exemples fournis afin de préconiser une plus grande collaboration entre les autorités de réglementation de la concurrence et de la protection de la vie privée[6].

Le rapport mentionne les enseignements clés, les domaines de synchronicité potentielle entre les régimes réglementaires ainsi que les obstacles à surmonter et les tensions potentielles à atténuer.

Le rapport met en évidence des questions d'intersection contemporaines, notamment :

- les données qui sont partagées comme un remède concurrentiel;
- la possibilité d'une réglementation privée pour faciliter une conduite anti-concurrentielle;
- l'importance de comprendre la terminologie de chaque champ de réglementation;
- la perception de la vie privée et des données comme étant des facteurs qui entrent en compétition dans l'analyse de la concurrence.

Fait peut-être encore plus important, le rapport comprend plusieurs exemples pratiques qui illustrent comment les autorités en matière de concurrence sont parvenues à intégrer avec succès des éléments liés à la protection de la vie privée dans leurs efforts d'application de la loi ainsi que dans la collaboration ou la considération inter-réglementaire et ont réussi à trouver un juste équilibre entre les deux sans sacrifier les objectifs de l'une ou de l'autre en cours de route. Les avantages d'une telle collaboration sont des résultats supérieurs qui servent globalement une économie numérique forte tout comme le droit à la vie privée des personnes et les intérêts des consommateurs. Le rapport complet est présenté à l'**annexe 1.**

Digital Crossroads: The Intersection of Competition Law and Data Privacy [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données]

Tandis que le rapport ci-dessus révèle de quelles façons les organismes responsables de la concurrence tiennent compte de la protection de la vie privée dans leurs analyses antitrust et dans quels domaines ils collaborent, le rapport universitaire qui l'accompagne contribue, quant à lui, à l'orientation et à l'éclaircissement des discussions et des travaux fondamentaux qui sous-tendent cette collaboration ainsi qu'à la détermination des autres orientations stratégiques à adopter.

Commandé par le GTCCN, l'examen universitaire indépendant, rédigé par la professeure Erika Douglas de la Temple University Beasley School of Law, qui s'intitule Digital Crossroads: The

[6] Conformément au mandat du DCCWG qui consiste à favoriser les possibilités de coopération inter-réglementaire.

Intersection of Competition Law and Data Privacy[7] [Carrefours numériques : l'entrecroisement du droit de la concurrence et de la confidentialité des données], est le premier rapport du genre à se pencher de façon exhaustive sur l'intersection entre l'antitrust et la confidentialité des données. Il donne un aperçu détaillé du paysage réglementaire actuel, il fait ressortir les compléments ainsi que les tensions entre les philosophies qui sont au centre de ces deux domaines et il souligne son élaboration émergente comme un défi inter-réglementaire important qui nécessite l'établissement d'un plus grand consensus ainsi qu'une collaboration à l'échelle internationale.

La professeure Douglas a diffusé publiquement son rapport universitaire indépendant en juillet 2021. Le rapport a ensuite fait l'objet d'une promotion dans les médias sociaux par la Temple University (@TempleLaw) et par l'AMVP auprès d'un public combiné de près de 14 000 abonnés. Le rapport a ensuite été diffusé par le Global Privacy Enforcement Network (Réseau mondial pour l'application des lois sur le respect de la vie privée) (GPEN) ainsi que par les membres du Réseau international de la concurrence (RIC). Le rapport peut être téléchargé à l'aide du réseau de recherche sur les sciences sociales (SSRN) de la professeure Douglas[8] au lien suivant : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737. Il est aussi présenté à l'**annexe 2.** Pendant cette courte période de diffusion, soit un peu plus d'un mois avant la transmission du rapport annuel au secrétariat de l'AMVP, le rapport de la professeure Douglas a engendré un nombre considérable de téléchargements et de visionnements du résumé à l'échelle mondiale[9].

2. Poursuivre la sensibilisation et la mobilisation dans d'autres forums

Les travaux du GTCCN ont suscité beaucoup d'attention et d'intérêt sur la scène mondiale tandis que ses membres ont réussi à mieux faire connaître les questions d'intersection et à encourager la collaboration inter-réglementaire. Les membres du GTCCN sont régulièrement sollicités pour faire des exposés, pour participer à des débats d'experts et pour prononcer des discours principaux à travers un vaste éventail de réseaux et de forums internationaux.

Un instantané des engagements en 2021

- L'Office of the Australian Information Commissioner (OAIC) a participé à un débat d'experts lors du sommet 2021 en Australie et en Nouvelle-Zélande de l'Association internationale des professionnels de la protection de la vie privée (IAPP) sur les progrès locaux et mondiaux qui ont des incidences sur la protection de la vie privée, la concurrence, la réforme de la consommation et la réglementation.
- Le Commissariat à la protection de la vie privée du Canada (CPVP du Canada), l'OAIC et la Federal Trade Commission des États-Unis (FTC des É.-U.) ont fait des exposés à l'occasion

[7] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737.

[8] Social Science Research Network.

[9] Depuis la transmission de ce rapport annuel au secrétariat de l'AMPV, le document a été téléchargé 357 fois tandis que le résumé a été vu 1 262 fois.

du sommet mondial sur la protection de la vie privée ou Global Privacy Summit 2021 de l'IAPP qui avait pour thème *Blurred Regulatory Lines* [Les limites réglementaires floues]. Le groupe d'experts était modéré par la professeure Erika Douglas, l'universitaire mandatée par le GTCCN qui possède une expertise dans les questions d'intersection réglementaire dans le droit de la concurrence et la protection de la vie privée.

- IAPP Canada a également tenu un débat d'experts sur la vie privée et la concurrence similaire qui comportait une conversation entre le Bureau de la concurrence Canada et le CPVP du Canada et qui mettait en évidence un exemple de l'utilisation (en vain) de la protection de la vie privée comme un mécanisme de défense antitrust dans un cas saisi par le Tribunal de la concurrence du Canada.

- Le RIC a tenu un débat d'experts sur la vie privée et la concurrence auquel a participé un représentant du CPVP du Canada ainsi que l'ancien président de la FTC des É.U. Timothy Muris, l'universitaire australienne spécialisée en droit de la concurrence et en droit relatif à la protection de la vie privée Katharine Kemp ainsi que l'avocate brésilienne spécialisée en antitrust Marcela Mattiuzo. Le groupe d'experts a été modéré par l'Autorité de la concurrence de la France.

- Le Contrôleur européen de la protection des données (CEPD) et le CPVP du Canada ont pris part à un débat d'experts à l'occasion de la Computer, Privacy and Data Protection Conference (CPDP), qui s'est penché sur les interactions entre la protection de la vie privée, la protection des consommateurs et la concurrence.

- L'OAIC et le CPVP du Canada ont donné une présentation sur le travail du GTCCN lors du 55^{e} forum des autorités de protection de la vie privée pour l'Asie et le Pacifique.

    - Au forum, l'OAIC a aussi fait un exposé sur le cadre Consumer Data Right australien, un cadre de portabilité des données qui repose sur de solides protections de la vie privée. L'OAIC a aussi fait une présentation afin de montrer comment le cadre Consumer Data Right favorise le flux de données transfrontalier et a souligné comment l'interopérabilité à l'échelle mondiale dans d'autres mécanismes de portabilité des données pourrait réduire le fardeau et la complexité réglementaires pour les entreprises.

- Le Bureau de la concurrence Canada, le CPVP du Canada et les plus grands avocats canadiens spécialisés en protection de la vie privée ont pris part à un débat d'experts dans le cadre d'un webinaire de l'Association du Barreau canadien intitulé *Happy Together: Privacy & Competition Law in a Digital Economy* (Le droit de la protection de la vie privée et le droit de la concurrence font bon ménage dans une économie numérique).

- L'Information Commissioner's Office du Royaume-Uni (ICO du R.-U.), la FTC des É.-U. et le CEPD ont participé à un débat d'experts au Centre for Economic and Policy Research Competition Policy dans le cadre duquel ils ont discuté de l'intégration de l'antitrust et de la protection de la vie privée.

- La Consumer Markets Authority (CMA) du R.-U., l'ICO du R.-U. et la professeure Erika Douglas ont participé à la série de conférences virtuelles sur les lois sur la protection

de la vie privée et les affaires dans le cadre d'un débat d'experts intitulé *Collaboration and Collision: Competition, Consumer and Privacy Law* (Collaboration et collision : le droit de la concurrence, de la consommation et de la protection de la vie privée). Modérée par le CPVP du Canada, la séance représentait le jour du lancement du rapport *Digital Crossroads: The Intersection of Competition Law and Data Privacy* [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données] de la professeure Douglas.

Dans l'ensemble, le GTCCN a constaté une augmentation de la demande et de l'intérêt pour des événements publics qui explorent les questions d'intersection réglementaire entre le droit de la protection de la vie privée et de la concurrence de la part des organismes et des réseaux de protection de la vie privée internationaux. Ce phénomène a engendré une plus grande connaissance et sensibilisation à l'égard des questions d'intersection parmi les intervenants et les réseaux clés.

3. Suivre et faciliter une coopération inter-réglementaire réelle

Ce volet s'appuie sur les travaux antérieurs entrepris par le GTCCN. Le groupe de travail continue de trouver des exemples et de multiplier les possibilités de coopération réglementaire le long d'un continuum allant de mesures **officieuses** (comme participer à des ateliers du Réseau mondial pour l'application des lois sur le respect de la vie privée (*GPEN) ou du Réseau international pour l'application des lois de protection des consommateurs (*ICPEN) à **plus officielles** (comme des lettres d'avertissement, une coordination ou une collaboration dans le cadre des enquêtes, etc.).

Le groupe de travail surveille les actions individuelles des autorités de réglementation (peu importe la sphère réglementaire dont elles sont responsables) qui démontrent les intersections entre les régimes réglementaires et les mesures de collaboration réelles prises par les autorités de réglementation dans les trois domaines réglementaires (le tableau cartographique des entrecroisements réglementaires et des actions de collaboration véritable du GTCCN). Le GTCCN déploie ces efforts pour permettre aux membres de se renseigner sur les questions d'intersection réglementaire auxquelles les autorités de toutes les sphères sont confrontées. Ce tableau cartographique, qui s'appuie sur le travail accompli par le GTCCN depuis 2017, est présenté à l'**annexe 3.**

Voici un instantané des actions de coopération réelle entreprises à l'échelle mondiale et surveillées par le groupe de travail

- Les membres du groupe de travail (la Surintendance de l'industrie et du commerce de la Colombie, la FTC des É.-U., le CPVP du Canada, l'ICO du R.-U. et l'OAIC) ont assisté au tout premier atelier conjoint sur les pratiques exemplaires du GPEN et de l'ICPEN, qui a réuni 175 professionnels de l'application des lois sur la protection de la vie privée et la protection des consommateurs afin de discuter des intersections significatives et des stratégies de coopération possibles entre ces sphères réglementaires. Compte tenu de l'expérience du groupe de travail avec les travaux inter-réglementaires, nous avons été invités à concevoir

et à superviser les séances en petits groupes de l'atelier. Les participants étaient appelés à considérer un scénario hypothétique et à discuter des entrecroisements ainsi que des obstacles et des stratégies possibles pour la coopération. L'événement conjoint en tant que tel représentait un exemple pragmatique de la collaboration inter-réglementaire, qui est un objectif clé du groupe de travail.

- L'ICO du R.-U. a uni ses forces avec les autorités de réglementation de la concurrence, de la protection des consommateurs, des communications et des finances du R.-U. dans le cadre d'un forum de coopération pour la réglementation numérique dans le but d'améliorer les efforts inter-réglementaires et d'assurer une réglementation efficace dans l'ensemble du paysage numérique. Le forum a planifié ses travaux pour 2021-2022.
    - En parallèle avec les travaux du forum, l'ICO du R.-U., l'autorité en matière de concurrence du R.-U. et la CMA ont publié une déclaration commune qui énonce leurs opinions sur le lien entre la concurrence et la protection des données dans l'économie numérique. La déclaration affirme l'engagement des deux autorités à travailler ensemble afin de maximiser la cohérence réglementaire et à promouvoir et à favoriser des résultats qui sont compétitifs et qui autonomisent les consommateurs grâce à un plus grand choix, à une transparence, à une conception du service et à une protection du droit à la vie privée des personnes. Cet engagement encourage simultanément la concurrence tout en améliorant la protection des données et le droit à la vie privée.
- L'organisme de protection des données, l'autorité en matière de concurrence, l'autorité nationale de protection des consommateurs et le service fédéral des poursuites du Brésil ont transmis une recommandation conjointe à WhatsApp et à Facebook leur demandant de reporter l'introduction de leur politique de confidentialité en raison des préoccupations liées à la protection de la vie privée, à la concurrence et aux droits des consommateurs.
- Le CEPD a publié deux opinions sur la loi sur les marchés numériques et sur la loi sur les services numériques proposée par la Commission européenne. Les opinions du CEPD apportent à la Commission européenne des considérations variées ainsi qu'une rédaction alternative qui vise à éviter tout conflit avec le RGPD. En tenant compte des opinions, le CEPD a reconnu que le droit de la concurrence, le droit de la protection des consommateurs et le droit de la protection des données étaient trois secteurs politiques inextricablement liés dans le contexte de l'économie des plateformes en ligne.
- À la suite des conclusions du rapport du Conseil de la consommation de la Norvège intitulé *Out of Control* (Hors de contrôle) sur les pratiques du secteur de la publicité en ligne, le conseil de la consommation de la Norvège a déposé des plaintes officielles contre les pratiques de Grindr en matière de données auprès du Datatilsynet en Norvège, alléguant une violation du *Règlement général sur la protection des données* de l'Union européenne. Le Datatilsynet de la Norvège a accueilli la plainte du conseil de la consommation et a fait parvenir un préavis à Grindr qui l'informait de son intention d'imposer une amende administrative pour la divulgation de données à de tiers publicitaires sans fondement légal et pour la divulgation de catégories spéciales de données sans une exemption valide.

- À la suite de l'intervention internationale par les membres de l'ICPEN, également approuvée par les membres du comité du GPEN, Google a annoncé que les fournisseurs d'applications devront indiquer dans Google Play Store les données personnelles que chaque application conserve et pourrait partager sur ses utilisateurs. Il s'agit de la première action d'application de la loi inter-réglementaire qui concerne les régimes de protection de la vie privée et de protection des consommateurs.

4. Contribuer au manuel de coopération en matière d'application de la loi de l'AMVP

Le GTCCN a continué de coordonner les révisions en cours du manuel de coopération en matière d'application de la loi de l'AMVP (le manuel) avec le Groupe de travail sur la coopération internationale en matière d'application de la loi (IEWG) de l'AMVP. Comme il est indiqué dans le rapport annuel de 2020 du GTCCN, nous avons contribué à la conception d'un sondage sur la coopération générale en lien avec le manuel. Afin de susciter des réponses variées, le groupe de travail a approché des membres sélectionnés du RIC.

À l'avenir, le GTCCN misera sur les liens tissés lors des entrevues approfondies réalisées auprès des autorités de réglementation de la concurrence en demandant à des autorités de réglementation choisies d'aider à l'élaboration d'études de cas sur la collaboration inter-réglementaire qui seront incluses dans le manuel révisé.

Les études de cas que le GTCCN veut préparer seront axées sur des stratégies de coopération entre les autorités de réglementation de la vie privée et de la concurrence ainsi que sur les avantages que les autorités de réglementation de la concurrence peuvent obtenir en collaborant avec leurs homologues de protection de la vie privée. Devant le besoin pour une coordination entre plusieurs groupes de travail et autorités de réglementation, on mettra la dernière main au manuel mis à jour avant la séance à huis clos à venir de l'AMVP.

Plan prospectif de 2021-2022

En déterminant son orientation future ainsi que son mandat à venir, le GTCCN a réfléchi à la focalisation de son travail jusqu'à présent. Tel qu'il est mentionné, compte tenu de la pertinence continue et grandissante de son travail, le GTCCN a l'intention de demander le « statut de groupe de travail permanent » sous l'AMVP. Veuillez voir ci-dessous un aperçu général des objectifs du GTCCN depuis 2017, de ses réalisations, ainsi qu'un plan axé sur l'avenir qui s'appuie sur les travaux antérieurs.

Veuillez noter que notre plan axé sur l'avenir corrobore la pertinence continue de ces objectifs tout en faisant évoluer notre focalisation qui consiste à accroître la collaboration entre les trois sphères réglementaires.

Objectif	Extrants généraux et activités du plan axé sur l'avenir
Explorer, cartographier et mieux comprendre l'intersection grandissante des sphères réglementaires de la protection de la vie privée, de la protection des consommateurs et de la concurrence	Le GTCCN a pris de l'avance pour cet objectif dans ses travaux sur son livre blanc de 2017-2018, qui portaient sur la protection des consommateurs, ainsi qu'en 2019-2021 dans ses travaux sur les examens approfondis des interactions entre la protection de la vie privée et la concurrence. **La complexité analytique de ces derniers nécessite une réflexion et une élaboration plus ciblées. Plus particulièrement, le GTCCN devrait se pencher précisément sur l'ensemble des répercussions des fusions et des acquisitions pour la protection de la vie privée des personnes.**
Sensibiliser les autorités à travers les sphères réglementaires à l'intersection afin que les autorités de protection de la vie privée puissent reconnaître une question de concurrence lorsqu'elles en voient une et vice-versa	Le GTCCN a connu beaucoup de succès depuis sa création en sensibilisant des intervenants externes clés aux questions d'entrecroisement. Il y a une augmentation évidente de la demande et de l'intérêt pour les présentations du GTCCN et les débats d'experts cette année. **Le GTCCN poursuivra son travail comme une activité continue qui contribue à la priorité stratégique de l'AMVP qui consiste à maximiser la voix et l'influence de l'AMVP.**
Repérer des stratégies et des outils **de collaboration** là où ils se trouvent et les préconiser ou les recommander lorsqu'il n'y en a pas	Cet objectif, qui a pris naissance à l'atelier du GPEN à Macao, **restera central au développement du plan axé sur l'avenir afin d'y tirer des leçons et des exemples.**
Enfin, rassembler le tout et **encourager une collaboration réelle** entre les trois sphères réglementaires	La facilitation d'une collaboration réelle entre les trois sphères réglementaires est au cœur des priorités stratégiques de l'AMVP qui visent à créer un environnement réglementaire mondial assorti de normes claires et élevées en matière de protection des données, alors que la numérisation évolue à un rythme soutenu. En gardant cette notion à l'esprit et en tenant compte de l'objectif ci-dessus, **cela devrait représenter une plus grande**

	focalisation dans notre plan axé sur l'avenir : la facilitation de la collaboration. Les stratégies consistent notamment à tenir un autre atelier sur la collaboration inter-réglementaire, à participer au RIC, à tenir un événement conjoint entre le RIC et l'AMVP et à miser sur nos ajouts dans le manuel de coopération en matière d'application de la loi de l'AMVP.
Analyse environnementale des autres domaines d'intersection réglementaire avec la protection de la vie privée (Remarque : Ce sera un nouvel objectif du GTCCN)	Les lois et les règlements sur la protection des consommateurs et la concurrence ont des incidences énormes, mais ce ne sont pas les seules sphères réglementaires à avoir des intersections avec les lois sur la protection de la vie privée et sur les données. Il y a déjà des questions d'intersection dans des domaines comme la sécurité électronique et les télécommunications qui pourraient faire l'objet d'études. **Une analyse environnementale permettrait de déterminer les autres sphères réglementaires et de les évaluer de façon générale en fonction des risques, des possibilités et de l'impact potentiel sur la société et l'économie numériques.**

Conclusion

La reconnaissance de l'importance de la coopération réglementaire dans la protection des renseignements personnels, surtout à une époque où la numérisation est accélérée, est au centre de la mission du GTCCN. Comme il est mentionné dans notre plan de travail de 2020-2021, le GTCCN a pour objectif de faire prendre conscience et d'encourager la compréhension des questions d'intersection entre les sphères réglementaires et de favoriser une coopération réglementaire entre elles. Ces questions d'intersection deviendront de plus en plus pertinentes au fur et à mesure que nous réagiront aux défis de l'économie numérique.

Dans le cadre de notre mandat de deux ans, nous nous sommes engagés à explorer les compléments et les tensions entre les sphères réglementaires de la protection de la vie privée et de la concurrence. Le GTCCN est satisfait des perspectives recueillies lors de notre réflexion approfondie sur la protection de la vie privée et la concurrence qui nous ont aidés à mieux comprendre les interactions entre la réglementation de la protection de la vie privée et de la concurrence et qui guideront et éclaireront les interactions ainsi que les collaborations de nos membres avec les autorités en matière de concurrence.

Nos travaux ont démontré non seulement que les frontières réglementaires traditionnelles continuent d'embrouiller les limites, mais qu'il existe des chevauchements considérables entre nos domaines réglementaires. Tandis que les autorités de réglementation des trois horizons se demandent comment réagir à ce phénomène, le besoin pour une coopération réglementaire entre les autorités afin d'obtenir des résultats globaux pour la protection de la vie privée et des consommateurs apparaît évident.

C'est un domaine que le GTCCN continuera de cibler et d'explorer en espérant devenir un groupe de travail permanent de l'AMVP. Le prolongement de notre mandat nous permettra de faire avancer la priorité stratégique de l'AMVP qui consiste à faire progresser la protection de la vie privée à l'échelle mondiale à l'ère du numérique et de continuer d'œuvrer en faveur d'un environnement réglementaire mondial assorti de normes claires et élevées en matière de protection des données.

Les coprésidents du GTCCN remercient sincèrement tous les membres pour leur contribution et leur soutien précieux à l'avancement de son mandat ainsi que pour leurs excellents résultats pratiques pour les citoyens et les consommateurs. Nous sommes impatients de poursuivre notre collaboration tandis que nous établissons le GTCCN comme un groupe de travail permanent afin de continuer d'accomplir cette tâche importante.

Annexe 1.

Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration [La protection de la vie privée et des données en guise de facteurs dans la réglementation de la concurrence : sondage auprès des autorités de réglementation de la concurrence visant à améliorer la collaboration inter-réglementaire], par le DCCWG

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES, FACTEURS DE LA RÉGLEMENTATION DE LA CONCURRENCE :

Enquête auprès des organismes de réglementation de la concurrence pour améliorer la collaboration intersectorielle

Groupe de travail du citoyen et du consommateur numérique
Rapport de la 43e Assemblée des autorités
Octobre 2021

TABLE DES MATIÈRES

RÉSUMÉ

1. Depuis sa création, le Groupe de travail du citoyen et du consommateur numérique (**GTCCN**) de l'Assemblée mondiale pour la protection de la vie privée s'efforce à la fois de mieux comprendre les entrecroisements entre les règlements et de promouvoir activement la collaboration intersectorielle. Les deux premières années de ce groupe ont été consacrées à l'étude du rapport entre la protection de la vie privée ou des données, et la protection des consommateurs, tandis que les deux dernières années ont porté sur l'intersection entre la vie privée et la concurrence. Ces quatre années d'études ont permis de mettre en évidence le fait que ces entrecroisements vont continuer à croître, tant en fréquence qu'en ampleur, car leur interaction façonne l'économie et la société numérique d'aujourd'hui.

2. Le présent rapport est le deuxième produit dans le cadre de notre « étude approfondie » des intersections entre la réglementation de la protection de la vie privée et celle de la concurrence. Le premier rapport a été publié en juillet 2021 et s'intitule *Digital Crossroads : The Interaction of Competition Law and Data Privacy*[1] [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données], une « étude universitaire » indépendante, commanditée par le GTCCN et rédigée par la professeure Erika Douglas de l'école de droit Beasley de l'Université Temple. Ce rapport porte sur une évaluation des complémentarités et des difficultés liées aux intersections entre la protection de la vie privée et des données et les objectifs et mandats des organismes responsables de la concurrence, ainsi que sur la manière dont les autorités responsables de la concurrence prennent en compte la protection de la vie privée et des données dans l'exercice de leur mandat. Ces deux rapports se complètent, apportant à la fois la théorie et l'application pratique qui forment la base de notre compréhension actuelle de ces entrecroisements.

3. Se fondant sur une série d'entretiens menés auprès des autorités responsables de la concurrence, le présent rapport vise à :

[1] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

i. comprendre la manière dont les autorités interrogées prennent en compte des considérations relatives à la protection de la vie privée et des données lorsqu'elles effectuent leurs analyses concurrentielles;

ii. exploiter les points de vue et les exemples fournis pour identifier les importantes possibilités de collaboration entre les autorités responsables de la concurrence et celles chargées de la protection de la vie privée ou des données.

Grâce à ces entretiens, le présent rapport fournit des commentaires, des analyses et des avis pertinents permettant d'identifier et de préconiser des possibilités de collaboration intersectorielle.

4. Les conclusions du présent rapport sont divisées en trois sections :

   i. La partie « Construire une base commune » porte sur certains concepts généraux qui faciliteront les futures discussions et collaborations intersectorielles. On peut notamment citer :

      i. La réglementation « traditionnelle » de la concurrence, selon laquelle les autorités devraient se concentrer sur leurs propres sphères réglementaires afin d'atteindre leurs objectifs de manière plus efficace. Toutefois, l'incidence croissante de la confidentialité en tant que facteur non tarifaire des évaluations concurrentielles représente une possibilité, voire une nécessité, de renforcer la collaboration, même pour les partisans de cette réglementation traditionnelle.

      ii. Les mécanismes essentiels formant la base des évaluations concurrentielles. Dans les faits, la confidentialité ne sera pertinente que lorsqu'elle aura une incidence sur le domaine de la concurrence. En partageant leurs connaissances asymétriques sur les modèles fondés sur la protection de la vie privée et les données, les autorités de protection de la vie privée peuvent contribuer au renforcement de la précision et du pouvoir de prédiction des évaluations concurrentielles menées par les autorités chargées de la concurrence relatives aux éventuelles conséquences de la protection de la vie privée et des éléments liés aux données.

iii. La capacité de l'intelligence artificielle à faciliter les comportements anticoncurrentiels, et comment un intérêt commun dans ce domaine représente une opportunité aux autorités des deux sphères d'apprendre les unes des autres et de mieux comprendre cette technologie naissante.

iv. L'examen de la manière dont les données sont partagées dans le cadre de recours concurrentiel permet aux autorités de la protection de la vie privée de mieux comprendre la nature concurrentielle de ces données, tandis que les organismes responsables de la concurrence peuvent recenser les éventuelles conséquences sur la confidentialité et savoir si les données partagées sont véritablement des renseignements personnels.

ii. La section intitulée « Avancer ensemble » présente les défis à relever en plus d'exemples pratiques de la manière dont l'application des lois sur la concurrence a déjà intégré les considérations relatives à la confidentialité. Notamment :

i. la manière dont les différentes sphères réglementaires parlent des langues différentes. Rétablir la compréhension est donc la première étape pour collaborer de manière efficace;

ii. l'importance d'éviter les résultats dichotomiques, profitant à un régime au détriment de l'autre, et la manière dont le Digital Regulation Cooperation Forum du Royaume-Uni peut servir d'exemple pour limiter la fréquence de tels résultats en vue de soutenir une économie numérique stable;

iii. l'examen du paradoxe en matière de protection de la vie privée et de la manière dont il peut être le résultat d'une défaillance du marché due à une mauvaise communication en matière de protection de la vie privée ainsi qu'à des paramètres par défaut et à une architecture de sélection favorisant les intérêts commerciaux de l'entreprise, plutôt que de promouvoir véritablement l'engagement du consommateur et de faciliter ses choix;

iv. l'examen de la manière dont les difficultés liées à l'attribution d'une valeur et d'un poids à la confidentialité en tant que facteur concurrentiel peut permettre aux autorités chargées de la protection de la vie privée et des données d'aider

celles responsables de la concurrence à mieux comprendre les préférences en matière de confidentialité et les conséquences qui en découlent;

v. la présentation d'exemples pratiques et progressifs de la manière dont les organismes ont déjà appliqué les considérations de la protection de la vie privée et des données dans l'exercice de leurs mandats. Cette partie aborde l'élaboration de nouvelles lignes directrices pour l'application des lois sur la concurrence, en définissant la protection de la vie privée et des données comme étant à la fois la cause et la justification d'un comportement anticoncurrentiel dans deux affaires litigieuses, et en présentant deux recours concurrentiels ayant réussi à partager des informations personnelles à des fins concurrentielles tout en protégeant les intérêts privés.

iii. La partie « *Enseignements du rapport Digital Crossroads* » met en évidence trois thèmes clés recensés par la professeure Douglas, qui se retrouvent également dans le présent rapport :

i. le fait que « la législation antitrust et celle relative à la protection des données se rencontrent de manière complexe et variée, en particulier dans l'économie numérique »[2];

ii. l'idée selon laquelle « la théorie et la pratique à cette frontière législative sont à un stade précoce » et les exemples pratiques sont eux « nouveaux et présentent d'importantes possibilités de développement »[3];

iii. le sentiment que « les autorités antitrust et celles chargées de la protection des données ne peuvent plus atteindre leurs objectifs de manière isolée ».[4] Les autorités partageant des « intérêts politiques communs » ainsi que l'objectif ultime de « satisfaire les consommateurs », il est primordial qu'elles travaillent

[2] Voir Erika Douglas, « Digital Crossroads: The Interaction of Competition Law and Data Privacy », Rapport à l'Assemblée mondiale pour la protection de la vie privée, GTCCN, 2021, p. 3. - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

[3] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

[4] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

ensemble afin d'élaborer des « stratégies d'application cohérentes et efficaces ».

5. Nous sommes convaincus que les idées et les exemples du présent rapport aideront les autorités des deux sphères réglementaires à acquérir une meilleure compréhension pratique de la manière dont elles peuvent aborder et améliorer leurs interactions intersectorielles. Vous verrez dans ce document que tous nos entretiens sont fondés notamment sur l'hypothèse que la collaboration et la communication entre les sphères réglementaires ne peuvent que servir à mieux satisfaire l'ensemble des citoyens. Nous espérons que la préparation du présent rapport sera l'une des premières étapes vers l'obtention de meilleurs résultats en la matière.

INTRODUCTION

LE GROUPE DE TRAVAIL DU CITOYEN ET DU CONSOMMATEUR NUMÉRIQUE DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE

6. Le groupe de travail du citoyen et du consommateur numérique (**GTCCN**) a été établi car, « étant donné que la protection de la vie privée et des données est de plus en plus prise en considération par les particuliers en leur qualité de consommateurs, les intersections entre les questions relatives à la protection des consommateurs, de la vie privée et des données sont de plus en plus nombreuses, notamment en ligne ».[5] À la suite de l'adoption de la résolution de septembre 2017 sur la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique, adoptée par la Conférence internationale des commissaires à la protection des données et de la vie privée, désormais nommée Assemblée mondiale pour la protection de la vie privée, le GTCCN a commencé à explorer la relation entre protection de la vie privée et protection des consommateurs. En plus de promouvoir et d'encourager la collaboration intersectorielle, le GTCCN a mené une étude approfondie sur la

[5] Conférence internationale des commissaires à la protection des données et de la vie privée : Résolution sur la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique, 26-27 septembre 2017, Hong Kong - http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-collaboration-on-consumer-protection.pdf

relation entre la protection de la vie privée et celle des consommateurs et a publié un livre blanc, dans le cadre de son rapport annuel de 2018, présenté à l'Assemblée à Bruxelles, en Belgique[6].

7. Mis en évidence par notre livre blanc et confirmé par les exemples intersectionnels de plus en plus nombreux que nous avons enregistrés,[7] le chevauchement entre la protection de la vie privée et la protection des consommateurs est relativement bien établi et bien surveillé. La protection de la vie privée et la protection des consommateurs étant, de par leur nature, comparables, il est courant que des pratiques préjudiciables, trompeuses ou mensongères en matière de protection de la vie privée soulèvent également des préoccupations en matière de protection des consommateurs (consentement par tromperie), nécessitant l'application de mesures dans les des deux régimes réglementaires. Le respect de la vie privée continue de s'imposer comme un facteur important dans les décisions d'achat des consommateurs, et les organisations fonctionnent de plus en plus selon ce principe.

8. C'est sur cette conclusion que l'attention du GTCCN s'est tournée vers la concurrence et l'antitrust.[8] Les recherches sur les entrecroisements, généralement plus complexes, entre la vie privée et la concurrence ont donné lieu à un certain nombre de résultats importants, dont le

[6] Rapport du groupe de travail du citoyen et du consommateur numérique sur la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique - http://globalprivacyassembly.org/wp-content/uploads/2019/11/GTCCN-Report-Albania-2011014.pdf

[7] Parmi les exemples de l'Annexe 2 - Cartographie des intersections réglementaires et tableau des actions de collaboration en cours du rapport annuel de 2020 du GTCCN, on peut citer : 1/ en juillet 2020, la Commission nationale de la protection de la vie privée des Philippines a publié un Bulletin d'urgence de santé publique servant de ligne directrice pour les établissements sur le traitement approprié des informations relatives aux clients et aux visiteurs pour le traçage des contrats; 2/ en juin 2020, le Bureau du Commissaire australien à l'information a contribué à l'élaboration d'un répertoire conjoint des services de sécurité en ligne avec l'Australian Competition and Consumer Commission, le Commissaire australien à la télésécurité et le Centre australien de cybersécurité; et 3/ en février 2020, Datatilsynet, l'autorité de protection des données de la Norvège, et l'Autorité norvégienne des consommateurs ont élaboré et publié conjointement un guide sur les services numériques et les données personnelles des consommateurs ayant pour but d'aider les opérateurs commerciaux, les développeurs, les spécialistes du marketing et les prestataires de services numériques à mettre en place des questions pratiques lorsque les questions de protection des consommateurs et de la vie privée se chevauchent.

[8] Plus particulièrement, la Conférence internationale des commissaires à la protection des données et de la vie privée a adopté à l'unanimité la résolution du GTCCN de 2019 : Résolution visant à soutenir et à faciliter la coopération réglementaire entre les autorités chargées de la protection des données et les autorités de protection des consommateurs et de la concurrence afin de parvenir à des normes claires et globalement élevées en termes de protection des données dans l'économie numérique - http://globalprivacyassembly.org/wp-content/uploads/2019/11/GTCCN-Resolution_ADOPTED.pdf

présent rapport et son équivalent universitaire indépendant intitulé Digital Crossroads : The Interaction of Competition Law and Data Privacy (Digital Crossroads)[9], rédigé par la professeure Erika Douglas de l'école de droit Beasley de l'Université Temple.

TENDANCES ACTUELLES DE L'ÉCONOMIE NUMÉRIQUE : INTERSECTIONS RÉGLEMENTAIRES EN MATIÈRE DE CONFIDENTIALITÉ ET DE CONCURRENCE

9. Comme c'est le cas pour la protection des consommateurs, l'intersection entre confidentialité et concurrence est ancrée dans l'économie numérique, sa croissance et son innovation. L'émergence et l'évolution des modèles d'entreprise fondés sur les données ont permis d'extraire la valeur des données avec plus de succès que jamais. Certains facteurs, tels que la monétisation des renseignements personnels, ont contribué à accroître la disponibilité des données à un niveau jamais vu auparavant, non seulement pour les entreprises sociales et commerciales internationales dominantes, mais également pour les petites et moyennes entreprises. Alors que l'économie numérique continue d'évoluer, il en va de même pour les conséquences sur la concurrence découlant de la conduite de ses acteurs. Reconnaissant que les données ne se conforment pas aux limites réglementaires, les entreprises qui amassent et utilisent de grandes quantités de données personnelles provoquent des effets sur la protection de la vie privée ou des données plus importants que jamais.

10. Jusqu'à maintenant, l'économie numérique a rapproché la sphère réglementaire de la protection de la vie privée et des données et celle de la concurrence d'une manière inexplorée ou incomprise. Suite à ce rapprochement, les intersections entre les sphères semblent actuellement présenter autant de complémentarités réglementaires que de difficultés. On peut dire que toutes les autorités, quel que soit leur secteur, sont forcées à évoluer et à développer des stratégies quant à la meilleure façon de traiter les intersections réglementaires. Ces défis et cette tendance sont devenus plus évidents en 2020 et 2021, en raison de la pandémie, qui a entraîné une dépendance accrue des consommateurs, des entreprises et de la société à l'égard de tout ce qui est d'ordre numérique. C'est dans cette optique que nous avons tenté de mieux comprendre comment la relation entre protection de la vie privée et des données et concurrence s'articule, en théorie et en pratique.

[9] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

OBJECTIFS DU PRÉSENT RAPPORT

11. Le présent rapport est le résultat d'une série d'entretiens menés auprès des autorités responsables de la concurrence du monde entier. Celui-ci vise à :

    i. comprendre la manière dont les autorités responsables de la concurrence interrogées tiennent compte des considérations relatives à la confidentialité et à la protection des données lorsqu'elles effectuent leurs analyses antitrust; et

    ii. exploiter les points de vue et les exemples fournis pour identifier les importantes possibilités de collaboration entre les autorités responsables de la concurrence et celles chargées de la protection de la vie privée et des données.

12. Le présent rapport est divisé en quatre parties. La première présente la méthodologie à la base des entretiens et du présent rapport. La deuxième partie donne un aperçu des observations générales faites lors des entretiens, et la troisième fournit des exemples spécifiques de thèmes communs et de mesures d'application pratiques discutés lors des entretiens. Enfin, la quatrième partie compare certaines de nos observations faites lors des entretiens avec les thèmes présentés dans le rapport *Digital Crossroads*.

PARTIE 1 – MÉTHODOLOGIE

13. Le GTCCN a envisagé la rédaction de rapports complémentaires dans le cadre d'une « étude approfondie » de l'intersection entre la réglementation de la protection de la vie privée et celle de la concurrence.

14. Le premier rapport a été déjà publié et s'intitule *Digital Crossroads*, une « étude universitaire » indépendante, commanditée par le GTCCN et rédigée par la professeure Erika Douglas. Celui-ci porte sur une évaluation des complémentarités et des difficultés liées aux intersections entre la protection de la vie privée et des données et les objectifs et mandats des organismes responsables de la concurrence, ainsi que sur la manière dont les autorités responsables de la concurrence prennent en compte la protection de la vie privée et des données dans l'exercice de leur mandat. Ce faisant, le rapport *Digital Crossroads* présente également de nombreux exemples de collaborations existantes, ou possibles à l'avenir, entre les sphères réglementaires.

15. De manière complémentaire, la professeure Douglas explore la théorie qui forme la base de ces intersections de manière bien plus détaillée dans son rapport *Digital Crossroads*. Le présent rapport s'appuiera sur certaines des observations et analyses de la professeure Douglas en tenant compte des points de vue des autorités responsables de la concurrence qui ont été interrogé.

16. Le présent rapport constitue la seconde partie de « l'étude approfondie » du GTCCN sur l'intersection entre la réglementation de la protection de la vie privée et celle de la concurrence. Le rapport *Digital Crossroads* étant une recherche universitaire indépendante, le présent rapport présente les perspectives et les réalités pratiques auxquelles sont confrontées les autorités chargées de la concurrence dans l'exercice de leur travail quotidien. À cette fin, et comme décrit ci-après, le présent rapport s'appuie sur une série d'entretiens menés auprès des autorités responsables de la concurrence. Nous espérons que ces rapports, pris en compte de manière conjointe, attireront une attention à long terme sur ces intersections et présenteront des domaines pratiques dans lesquels les autorités chargées de la protection de la vie privée et celles responsables de la concurrence peuvent collaborer. Cette collaboration permettra aux autorités de mieux comprendre l'interaction entre les sphères réglementaires et d'obtenir de meilleurs résultats en matière de confidentialité et de concurrence pour l'ensemble des citoyens.

17. Le présent rapport a commencé par l'élaboration d'un questionnaire, afin d'assurer la cohérence des entretiens. Le questionnaire a abordé les points suivants :

    i. les paramètres opérationnels de l'organisme interrogé;

    ii. si et dans quelle mesure il a tenu compte de la protection de la vie privée dans le cadre de ses évaluations des fusions, des abus de position dominante et de l'emprise générale sur le marché;

    iii. des exemples pratiques de la façon dont la protection de la vie privée ou des données a été prise en compte dans son travail;

    iv. la collaboration intersectorielle.

    Les membres du GTCCN ont ensuite communiqué avec leurs homologues responsables de la concurrence, et les ont invités à participer à un entretien. Parallèlement, la Superintendencia de

Industria y Comercio (**SIC**) de la Colombie, dont le mandat porte à la fois sur la protection de la vie privée et la concurrence (entre autres), a demandé à certains de ses partenaires chargés de la concurrence de participer à un entretien.

18. Tous les moyens ont été mis en œuvre pour mener des entretiens en personne par vidéoconférence. Si cela n'était pas possible, les autorités chargées de la concurrence ont pu soumettre leurs réponses au questionnaire par écrit.

19. Les équipes chargées des entretiens étaient composées soit de membres provenant du Commissariat à la protection de la vie privée du Canada, de la SIC ou d'une combinaison de ces deux organismes. De manière générale, les entretiens personnels ont été menés par des équipes de trois personnes : une personne menant l'entretien et les autres prenant des notes et posant occasionnellement des questions de suivi. Ces entretiens étaient fluides, c'est-à-dire que, bien qu'ils abordaient tous les points du questionnaire, ils ne respectaient pas de manière stricte la formulation ou la séquence exacte de chaque question. Ils ont plutôt suivi le cours de la discussion et ont parfois abordé des sujets intéressants et pertinents au-delà du questionnaire lui-même.

20. 12 entretiens ont été conduits avec les représentants des organismes suivants :

    i. Australian Competition and Consumer Commission;

    ii. Autoriteit Consument & Markt (Pays-Bas);

    iii. Bundeskartellamt (Allemagne);

    iv. Comisión Federal de Competencia Económica (COFECE) (Mexique);

    v. Comisión Para Promover la Competencia (Costa Rica);

    vi. Competition and Consumer Commission of Singapore;

    vii. Competition and Markets Authority (Royaume-Uni);

    viii. Bureau de la concurrence Canada;

    ix. Autoridad de Fiscalización de Empresas del Ministerio de Desarrollo Productivo y Economía Plural (Bolivie);

x. Federal Trade Commission (États-Unis d'Amérique);

xi. Konkurrence og forbrugerstyrelsen (Danemark); et

xii. Superintendencia de Industria y Comercio (Colombie).

21. Sur les 12 organismes interrogés, la majeure partie d'entre eux fonctionne selon un mandat double lié à la concurrence ainsi qu'à la protection des consommateurs. Deux organismes sont responsables de la concurrence, de la protection des consommateurs et de la vie privée. De plus, bien qu'une autorité dispose de responsabilités limitées en matière de concurrence, il est important de noter qu'elle opère actuellement dans une administration qui n'a pas encore d'autorité dédiée à la concurrence ou à la protection des consommateurs ou de la vie privée. Parallèlement, plusieurs de ces organismes sont également chargés de remplir des mandats réglementaires supplémentaires, allant au-delà de la concurrence et de la protection des consommateurs.

22. Les réponses aux entretiens ont été évaluées afin de recenser les points de vue généraux et spécifiques à inclure dans le présent rapport. Ce dernier n'a pas pour but de retranscrire les réponses aux entretiens mot pour mot ou dans leur intégralité. Au contraire, il présente et développe les thèmes généraux récurrents ayant été recensés, tout en présentant des exemples pratiques de coopération intersectorielle ou des opinions quant à celle-ci.

23. Enfin, il convient de noter que, conformément au mandat du GTCCN consistant à faciliter la coopération intersectorielle, le présent rapport fournit des commentaires, des analyses et des avis pertinents permettant d'identifier et de préconiser des possibilités de collaboration. Bien que ce rapport s'adresse principalement à un public chargé de la protection de la vie privée, il présentera certains concepts fondamentaux liés à la concurrence, plutôt que de s'engager dans une discussion de fond à propos de la théorie de la concurrence. Par ailleurs, bien que les notions de « protection de la vie privée » et de « protection des données » portent des significations différentes, le présent rapport utilisera ces deux termes de manière interchangeable, en reconnaissance du fait que, indépendamment de leur titre, ces autorités visent les mêmes objectifs.

24. Comme indiqué dans le rapport *Digital Crossroads*, nous ne faisons que commencer à comprendre les intersections entre la protection de la vie privée et la concurrence. Le GTCCN est

convaincu que les autorités des deux sphères peuvent collaborer afin de mettre en œuvre une application de la loi réactive, qui s'adaptera facilement aux pratiques commerciales de demain et qui, finalement, permettra de garantir de meilleurs résultats généraux en ce qui concerne le droit à la protection de la vie privée et les intérêts des consommateurs. Le GTCCN espère que le présent rapport et le rapport *Digital Crossroads* nous permettront de démarrer ce processus de collaboration.

PARTIE 2 – CONSTRUIRE UNE BASE COMMUNE

25. Les intersections entre la protection de la vie privée et la concurrence sont apparues assez récemment. Alors que tous les organismes interrogés ont réussi à décrire les défis et les possibilités présentés par ces intersections, toutes n'ont pas été en mesure de donner des exemples de la manière dont elles se sont matérialisées dans la pratique. L'exemple le plus ancien recensé au cours des entretiens provient de la Federal Trade Commission des États-Unis (**FTC**). Il s'agit d'un énoncé de divergence d'un commissaire datant de 2007 sur la fusion entre Google et DoubleClick, qui affirmait que « si aucune condition n'est imposée à la fusion, les intérêts des consommateurs en matière de concurrence et de protection de la vie privée n'auraient pas été traités de manière adéquate. »[10] À l'exception d'un autre exemple datant de 2014, les exemples mentionnés au cours des entretiens (et examinés ci-après dans la Partie 3 – Avancer ensemble) ont principalement eu lieu au cours des dernières années.

26. Avant d'aller plus loin, il convient de reconnaître que certaines juridictions ne disposent pas d'une gamme complète d'autorités chargées de la protection des consommateurs, de la concurrence ou de la protection de la vie privée (indépendantes ou faisant partie d'autorités à mandats multiples). Les travaux menés par le GTCCN, en parallèle d'un projet comparable entrepris par le Réseau international de la concurrence (RIC),[11] permettront d'accroître la sensibilisation intersectorielle et de faciliter l'élaboration de stratégies visant à tirer parti des

[10] Dans l'affaire Google/DoubleClick, Dossier de la FTC n° 071-0170, Énoncé de divergence de la commissaire Pamela Jones Harbour, p. 1 – https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf

[11] Scoping paper – Competition law enforcement at the intersection between competition, consumer protection, and privacy. Document destiné au groupe directeur du RIC (2020) - https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/05/SG-Project-comp-cp-priv-scoping-paper.pdf

complémentarités et à réduire les difficultés entre la concurrence et la protection de la vie privée. Cependant, il est important de noter que les juridictions ne disposent pas toutes de protections réglementaires complètes ou équitables dans ces domaines. Dans de nombreux cas, les lois sur la concurrence sont plus ancrées dans l'histoire (certaines remontent à plus d'un siècle) que celles sur la protection de la vie privée, adoptées plus récemment. Lorsqu'il y a des lacunes de réglementation, il y a généralement une situation où une loi sur la concurrence existe, mais les lois ou des règlements sur la protection de la vie privée n'existent pas. Dans un contexte où de nouvelles autorités sont instaurées, l'évolution du paysage réglementaire représente l'occasion de créer des régimes mieux intégrés dès le départ, dont les fondements sont la collaboration et la coopération intersectorielle, plutôt que de chercher à adopter et à incorporer des stratégies de collaboration dans des régimes déjà établis.

27. Venons-en au thème central de l'intersection entre la réglementation de la concurrence et la réglementation de la protection de la vie privée. Plusieurs personnes interrogées ont mentionné une tendance favorable quant à une approche « traditionelle » de la réglementation. Cela ne veut pas dire qu'une majorité des organismes préconisent cette approche, mais plutôt qu'il s'agissait d'un sujet abordé lors des entretiens, recensé comme un débat en évolution au sein de la globalité de la communauté responsable de la concurrence. Cette approche part de l'idée selon laquelle les autorités chargées la concurrence peuvent remplir plus efficacement leur mandat en se concentrant sur les questions et les éléments de concurrence lors de l'évaluation du comportement en cause, en écartant tout facteur n'ayant aucun aspect concurrentiel. Selon cette approche, les évaluations concurrentielles reposent sur des indicateurs concurrentiels traditionnels, tels que les prix ou les parts de marché, et excluent généralement les facteurs tels que la protection de la vie privée. Certains partisans de cette approche réglementaire considèrent que les différentes sphères réglementaires ont été créées pour une raison précise et que les autorités devraient concentrer leurs efforts dans les limites de leur mandat, en espérant que les autres autorités en feront de même pour tout problème accessoire survenant au sein de leurs sphères réglementaires. En d'autres termes, les autorités chargées de la concurrence réglementent la concurrence et devraient laisser les questions liées à la protection de la vie privée aux autorités responsables de celle-ci.

28. Le débat autour de cette approche est beaucoup plus complexe et nuancé pour que le présent rapport soit en mesure de l'explorer dans son intégralité. Toutefois, le présent rapport continue

de plaider en faveur d'une collaboration intersectorielle, même dans le cadre d'une telle approche. Plus précisément, la protection des données devrait être prise en compte dans les analyses lorsqu'elles représentent un facteur concurrentiel réel (par exemple, lorsque deux entités fusionnantes sont en concurrence sur le degré de protection de la vie privée fourni aux clients). Comme décrit ci-après, cela représente une possibilité pour les autorités responsables de la concurrence de collaborer avec celles chargées de la protection de la vie privée, qui jouissent d'un avantage comparatif en termes de compréhension du fonctionnement de certains mécanismes de protection de la vie privée, afin d'améliorer le niveau de confiance statistique dans les analyses antitrust.

29. Comme indiqué dans l'introduction, toutes les autorités, quel que soit leur secteur, sont forcées à évoluer et à développer des stratégies quant à la meilleure façon de faire face à la croissance dynamique et à la relation intersectorielle de l'économie numérique. L'augmentation de la dépendance des entreprises, des sociétés et des particuliers à l'égard de tout ce qui est d'ordre numérique a mis en lumière les défis et ce dynamisme. Du recours accru aux services de vidéoconférence, remplaçant les réunions en personne, à l'explosion du nombre de détaillants de toutes tailles développant de nouvelles plateformes en ligne, la pandémie de COVID-19 a encouragé le monde à vivre à l'intérieur et en ligne. Face à un changement aussi rapide et radical, le présent rapport estime que toutes les autorités, en plus des organismes chargés de la protection de la vie privée et de la concurrence, doivent réévaluer leur approche quant à l'économie numérique. Cela constitue une possibilité de collaboration, lorsque cela est pertinent et justifié, et une possibilité de nous assurer que nous, en tant que communauté de régulateurs, faisons face aux réalités de l'économie numérique actuelle de manière adéquate. Cette collaboration nous permettra de mieux comprendre, de manière collective, les problèmes auxquels chaque sphère réglementaire est confrontée, et de développer une stratégie cohérente, fondée sur cette compréhension commune. Plus particulièrement, étant donné la relation entre la protection des données et la concurrence, cela représente une possibilité de prendre des décisions mieux informées sur la manière dont les actions d'une sphère peuvent avoir une influence sur l'autre. À cette fin, le présent rapport détaille ci-après certains enseignements tirés des entretiens, susceptibles de faire avancer ces discussions.

COMPRENDRE LES MÉCANISMES D'UNE ANALYSE CONCURRENTIELLE

30. Pour commencer, il convient d'examiner les objectifs réglementaires fondamentaux qui sous-tendent la réglementation en matière de concurrence et de protection des données. Les entreprises mondiales fondées sur les données étant examinées au titre de lois antitrust le sont également en ce qui concerne les pratiques en matière de protection de la vie privée, mais si les deux régimes réglementaires peuvent s'intéresser à la même entreprise, les raisons fondamentales les poussant à le faire proviennent d'origines différentes. Alors que les autorités chargées de la protection de la vie privée se préoccupent de protéger la confidentialité des individus, celles responsables de la concurrence cherchent à préserver la santé des économies concurrentielles et des marchés.

31. Les évaluations concurrentielles des autorités responsables de la concurrence sont ancrées dans les théories et les pratiques économiques, et également limitées par celles-ci. Les analyses au titre de lois antitrust cherchent à évaluer les effets concurrentiels d'un comportement mis en cause. À cette fin, si la protection de la vie privée ne constitue pas un élément direct ou annexe du comportement concurrentiel en cause, elle n'est pas automatiquement considérée comme pertinente et prise en considération, peu importe la quantité de renseignements personnels qu'une partie peut détenir. Prenons l'exemple d'une fusion hypothétique entre une entreprise qui développe des gadgets logiciels et une autre qui développe des moniteurs d'activité physique. Le fait que l'entreprise de gadgets logiciels gagne accès à l'intégralité des renseignements personnels détenus par l'entreprise de moniteurs d'activité ne pose aucun souci à l'autorité responsable de la concurrence, car il n'y a pas de chevauchement concurrentiel entre les deux entreprises. En revanche, la protection de la vie privée deviendrait un facteur pertinent pour cette autorité lors de l'évaluation d'une fusion entre deux fabricants de moniteurs d'activités se faisant activement concurrence sur le niveau de confidentialité offert aux utilisateurs (par exemple, lorsque l'un attire les utilisateurs en raison de son niveau élevé de protection de la vie privée, tandis que l'autre gagne des clients grâce à sa présence écrasante sur le marché).

32. De même, le fait que de nombreuses juridictions et autorités chargées de la protection de la vie privée considèrent celle-ci comme un droit fondamental ne lui donne pas automatiquement plus de valeur dans les évaluations concurrentielles. Comme cela a été indiqué au cours d'un entretien, le fait de considérer quelque chose comme un droit ne se traduit pas forcément par l'élaboration de lignes directrices pratiques sur la manière dont ce droit doit être appliqué dans

différents contextes réglementaires. Les entretiens ont fait ressortir certains défis, notamment le fait que les considérations en matière de protection de la vie privée sont difficiles à évaluer pour diverses raisons (certaines seront discutées de manière plus détaillée ci-après), et que le simple fait de considérer que « la vie privée est un droit » n'aide pas, ou peu, les autorités responsables de la concurrence à surmonter ces difficultés et à attribuer une valeur ou un poids à la protection de la vie privée dans les évaluations concurrentielles.

33. Un point commun soulevé dans deux entretiens est le fait que les organismes responsables de la concurrence n'en sont encore qu'au début de leurs analyses de l'évaluation des conséquences des ensembles de données combinés après une fusion sur l'emprise sur le marché. L'évaluation de ces conséquences peut être entravée par les défis associés à l'évaluation de nouveaux ou différents types d'opérations numériques et de comportements anticoncurrentiels inédits auxquels les organismes responsables de la concurrence n'ont pas l'habitude d'être confrontés. Armés de très peu d'informations historiques, il est difficile pour eux d'évaluer d'emblée les conséquences complètes de tels comportements.

34. La situation a conduit certains gouvernements à adopter des lois rendant possible une analyse plus efficace du développement des marchés numériques et de leurs conséquences sur la concurrence économique. En 2020, le gouvernement mexicain a par exemple modifié l'état de sa Comisión Federal de Competencia Económica (**COFECE**) pour créer une Direction générale des marchés numériques. Il incombe, entre autres, à cette direction de surveiller le développement des marchés numériques dans lesquels les données personnelles des utilisateurs deviennent un facteur de l'efficacité de la concurrence, tant du point de vue des entreprises que de celui des utilisateurs.

35. Les défis décrits ci-dessus présentent les possibilités de collaboration où les autorités chargées de la protection de la vie privée peuvent être en possession d'un avantage asymétrique en termes de connaissances sur l'utilisation des données du marché numérique et la dynamique qui sous-tend les considérations générales relatives à la protection de la vie privée. Dans ce scénario, la collaboration avec les autorités chargées de la protection de la vie privée en vue de tirer parti de leurs expériences pourrait contribuer à renforcer la précision et le pouvoir de prédiction des évaluations menées par les autorités chargées de la concurrence relatives aux

éventuelles conséquences de la protection de la vie privée et des éléments liés aux données sur la concurrence.[12]

LES DONNÉES PEUVENT FACILITER DES COMPORTEMENTS ANTICONCURRENTIELS DE DEMAIN

36. En ce qui concerne les innovations axées sur les données, nous avons appris au cours des entretiens que les réalités pratiques actuelles en ce qui concerne la manière dont les entreprises exploitent les données personnelles et utilisent les innovations technologiques peuvent mettre davantage en évidence le lien entre la théorie et la pratique. L'entretien avec la FTC des États-Unis a été le premier de deux entretiens ayant signalé et décrit le potentiel croissant de l'intelligence artificielle (**IA**), un domaine d'intérêt évident pour la protection des données, permettant de faciliter les pratiques anticoncurrentielles. Le prix étant un élément clé des analyses concurrentielles, on peut se demander si, grâce à l'IA, une entreprise peut être en mesure :

    i. de faire accroître les prix après une fusion;

    ii. d'utiliser sa position dominante pour maintenir les prix à un niveau trop bas pour que les autres entreprises puissent rivaliser; ou

    iii. parvenir à une entente avec d'autres entreprises visant à augmenter artificiellement le prix d'un produit.

37. C'est sur la base de cette dernière question que la FTC des États-Unis a expliqué que l'IA a le potentiel théorique de permettre la collusion, qu'elle soit tacite ou intentionnelle. Par exemple, supposons que **l'entreprise A** développe un algorithme d'IA pour suivre les fluctuations des prix sur le marché et pour faciliter l'établissement de ses prix. Parallèlement, **l'entreprise B**, principal concurrent de **l'entreprise A**, déploie un algorithme similaire. Dans leur forme la plus simple, les deux algorithmes, interagissant avec le même univers de données, peuvent essentiellement « apprendre l'un de l'autre » et, afin de maximiser les profits, arriver au même prix, augmenté de manière artificielle. Bien que cela soit alarmant et qu'il ne s'agisse en théorie que de l'extension logique d'un système d'IA, apprenant par lui-même et visant à maximiser les profits,

[12] La théorie selon laquelle l'expertise des régulateurs de la protection de la privée est précieuse pour les évaluations concurrentielles est également un thème important du rapport Digital Crossroads.

aucune des entreprises l'ayant déployé n'avait connaissance de sa mise en pratique. L'autre entreprise était d'avis que, dans l'environnement technologique actuel, cette idée semble intéressante, mais ne reste qu'une théorie.

38. Étant donné la nature automatisée et le caractère « auto-apprenant » de ces scénarios, l'IA peut devenir encore plus problématique et difficile à détecter, notamment lorsqu'elle est pilotée par des systèmes facilitant la tarification personnalisée ou analysant les habitudes des utilisateurs sur les marchés en ligne. Dans les deux cas, les algorithmes de « fixation des prix » peuvent évoluer de décisions basées sur des prix annoncés publiquement vers des décisions fondées sur des pratiques réelles et des modèles de tarification discriminants ciblant des consommateurs individuels, avec d'éventuelles conséquences sur la protection de la vie privée.

39. Peu importe si de tels risques surviennent de la manière décrite ci-dessus ou sous toute autre forme, étant donné que les autorités chargées de la protection des données et celles de la concurrence se concentrent, indépendamment, mais simultanément, sur l'effet de l'IA sur la concurrence ou les droits à la vie privée, elles ne peuvent que bénéficier du partage des ressources, des connaissances et de l'expertise en matière de gestion des efforts d'application de lois ou de politiques liées à l'IA.

NATURE DES DONNÉES PARTAGÉES DANS LE CADRE D'UN RECOURS CONCURRENTIEL

40. Les recours visant à empêcher le monopole du marché suite à une fusion ou à rétablir l'équilibre concurrentiel dans les marchés comportant des acteurs dominants sont apparus dans de nombreux entretiens comme des situations où des incohérences entre les objectifs en matière de concurrence et de protection de la vie privée sont susceptibles de se manifester. Par exemple, lorsqu'un recours relatif à une fusion prévoit le partage de données avec d'autres acteurs du marché, et si ces acteurs sont extérieurs à l'entité fusionnée, cela peut très bien améliorer, ou du moins préserver, la concurrence. À l'inverse, un partage important des données et des renseignements personnels peut entraver le droit à la vie privée des individus.

41. Cependant, nous avons également appris que de tels conflits apparents ne signifient pas nécessairement que des solutions ne peuvent pas être trouvées pour appuyer, ou respecter, les deux objectifs réglementaires. Par exemple, la COFECE du Mexique a mentionné une enquête qu'elle avait menée et qui avait conclu qu'un acteur dominant du secteur des agences d'évaluation du crédit devait être sanctionné pour avoir refusé de partager des renseignements

de base relatifs aux clients avec ses concurrents. La COFECE a constaté qu'en refusant l'accès aux informations financières générées par ses clients, l'acteur dominant a effectivement créé une barrière à l'entrée sur le marché de l'information sur le crédit. La COFECE a également déclaré que même si la législation régissant les agences d'évaluation du crédit stipule que celles-ci doivent partager un minimum de renseignements de base relatifs aux utilisateurs suffisant pour développer des produits financiers de base, les renseignements détaillés ne peuvent être partagés que par les agences d'évaluation du crédit à un prix réglementé et avec le consentement du client. Cela protège les données relatives aux consommateurs tout en permettant aux nouvelles entreprises concurrentes d'avoir un accès garanti à une quantité minimale de données de ce type.

42. L'entretien avec la Competition and Markets Authority (**CMA**) du Royaume-Uni a permis de recueillir des informations précieuses sur l'élaboration de recours concurrentiels nécessitant un partage de données. En bref, il a été suggéré qu'il était utile de considérer la nature des données désirées par les entreprises lorsque le partage de données fait partie d'un éventuel recours concurrentiel. À cette fin, la CMA a souligné les situations potentiellement moins attentatoires à la vie privée dans lesquelles, pour rétablir la concurrence (ou empêcher l'exercice d'une emprise sur le marché), les concurrents tiers obtiennent l'accès à des modèles ou des tendances de recherche plus larges, sans obtenir de renseignements personnels réels sur les utilisateurs effectuant ces recherches.

43. Ces considérations gagnent en importance à mesure que de multiples juridictions s'efforcent d'établir ou d'ancrer des règlements en matière de portabilité des données. Permettre aux consommateurs d'emporter leurs données aura une incidence évidente sur la concurrence et la protection de la vie privée. La possibilité de passer facilement d'un prestataire de services à un autre incitera les entreprises à continuellement évaluer si leurs produits, services ou prix restent attirants pour les clients existants et potentiels. Parallèlement, le transfert de données relatives aux clients entre concurrents doit se faire de manière à garantir la protection des renseignements personnels.

44. Reconnaissant que le contexte est essentiel, nous pensons fermement que les autorités chargées de la protection des données et celles responsables de la concurrence peuvent tirer parti de discussions plus approfondies sur les types de renseignements partagés dans le cadre de recours concurrentiels. Les autorités de protection de la vie privée peuvent obtenir une

meilleure compréhension de la nature concurrentielle de ces données, tandis que les organismes responsables de la concurrence peuvent recenser les éventuelles conséquences sur la confidentialité et savoir si les données partagées sont véritablement des renseignements personnels. L'idéal serait de trouver une solution permettant d'atteindre les objectifs de compétitivité tout en respectant le droit à la vie privée. Pour une excellente illustration de l'équilibre à trouver pour parvenir à un tel résultat, veuillez consulter les exemples australien et colombien décrits ci-après, dans la partie intitulée *Équilibre atteint entre confidentialité et concurrence.*

PARTIE 3 – AVANCER ENSEMBLE

45. L'équipe chargée des entretiens a également obtenu une variété d'informations spécifiques relatives à :

    i. la manière dont les organismes responsables de la concurrence ont incorporé la protection des données dans leurs efforts d'application de la loi, et dans quelle mesure;

    ii. l'état actuel de la coopération intersectorielle.

46. Plusieurs de ces informations étaient communes à tous les entretiens. Les paragraphes suivants présentent quelques exemples spécifiques de situations où les organismes responsables de la concurrence ont pu intégrer des éléments de protection de la vie privée, ou ont entrepris une collaboration pratique.

NOUS PARLONS DES LANGUES DIFFÉRENTES

47. La première de ces idées est apparue au cours de l'entretien avec le Bureau de la concurrence Canada et est devenue évidentes dans presque tous les autres entretiens : les autorités chargées de la protection de la vie privée et celles responsables de la concurrence parlent des langages réglementaires différents et interprètent différemment certains concepts. Notre questionnaire d'entretien faisait référence à la manière dont la « confidentialité » était prise en compte dans les analyses antitrust. Les personnes interrogées ont naturellement répondu à la question en examinant la manière dont les entreprises peuvent se faire concurrence sur la base de la « protection de la vie privée », c'est-à-dire comment la « confidentialité » influe sur la concurrence entre les entreprises. Toutefois, lorsque la discussion a évolué vers le rôle des

« données » ou des « renseignements personnels » dans les analyses de fusion, nous avons souvent reçu un ensemble très varié d'exemples et de théories. En bref, en leur qualité d'autorités chargées de la protection de la vie privée, les équipes chargées des entretiens ont instinctivement traité les concepts de renseignements et de données personnels en même temps que la « confidentialité » au cours des premiers entretiens avec les organismes. Cependant, les personnes interrogées ont interprété ces termes différemment et ont constaté des conséquences différentes en matière de concurrence. À titre d'exemple, deux entreprises qui fusionnent ne vont pas nécessairement se faire concurrence sur la base de protection de la vie privée qu'elles offrent à leurs clients (rendant ainsi la confidentialité non pertinente pour leurs analyses). Cependant, l'ensemble de données fusionné peut conférer une emprise sur le marché à l'entité fusionnée (rendant les données hautement pertinentes).

48. La première étape pour pouvoir collaborer de manière productive est de s'assurer que l'on se comprend. Sans pour autant préconiser l'élaboration d'un nouveau lexique de la protection de la vie privée et de la concurrence, il est important que les autorités comprennent les significations nuancées de termes pertinents pour les deux secteurs. Alors que la protection de la vie privée emploie des termes comme le consentement de l'utilisateur, l'anonymisation et les renseignements accessibles au public, la concurrence s'intéresse aux termes comme l'emprise sur le marché, les facteurs tarifaires et non tarifaires, et les barrières à l'entrée. Les autorités chargées de la protection de la vie privée se concentrent sur les « renseignements personnels » ou les « données à caractère personnel » (selon la terminologie préférée de l'organisme), tandis que les autorités responsables de la concurrence ont tendance à se concentrer sur les « données » de manière plus générale (potentiellement personnelles ou non personnelles) comme l'un des multiples éléments permettant de déterminer un marché de produits pertinent.

49. Compte tenu de l'optique économique adoptée par les organismes responsables de la concurrence, les autorités chargées de la protection de la vie privée ne connaissent probablement pas le concept de « marché de produits pertinent », terme technique désignant tous les produits et les services qu'un consommateur pourrait trouver interchangeables. Parmi les produits et les services entrant dans un marché de produits, on peut citer : les voyages en avion, les services de prêt ou l'achat de voitures de taille moyenne. Les marchés de produits plus liés à la protection de la vie privée pourraient inclure les plateformes de réseaux sociaux ou les moteurs de recherche. Il convient également de tenir compte de la localisation du marché

pertinent pour les produits (nationaux, mondiaux, etc.) Enfin, les organismes responsables de la concurrence se concentrent sur le degré de concurrence de ces marchés de produits et de ces marchés géographiques, et sur l'existence d'un monopole par le biais d'acteurs dominants, ou l'existence d'un monopole potentiel si des fusions proposées étaient autorisées.

50. Tout comme les autorités chargées de la protection de la vie privée ne connaissent probablement pas les marchés de produits pertinents, il est tout aussi probable que celles responsables de la concurrence ne connaissent pas les principes de responsabilité ou de transparence utilisés dans le secteur de la protection de la vie privée. Peu importe la manière dont les concepts sont traduits d'une sphère à l'autre, il y a un intérêt commun d'assurer une compréhension de base de ce que l'autre dit. Au fur et à mesure que les autorités s'impliquent dans ce domaine, il sera important que chacune prenne le temps d'expliquer la signification de ses concepts clés. Au final, la rédaction d'un « glossaire intersectoriel » des termes clés peut s'avérer utile à cette fin.

COLLABORER POUR ÉVITER LES RÉSULTATS DICHOTOMIQUES

51. Les perspectives partagées au cours de l'entretien avec la Competition and Markets Authority du Royaume-Uni illustrent la manière dont les autorités ont fait face à l'idée fausse selon laquelle il existe une dichotomie inconciliable entre « bon pour la confidentialité » et « mauvais pour la concurrence », et inversement. Des mandats et des objectifs différents amènent parfois les autorités à s'orienter dans des directions opposées. Le partage de données en est un bon exemple. Du point de vue de la protection de la vie privée, l'utilisation et le partage non autorisés de renseignements personnels vont généralement à l'encontre du droit à la vie privée. Cependant, du côté de la concurrence, limiter l'accès aux données relatives aux utilisateurs peut avoir un effet néfaste sur la concurrence ou constituer une barrière à l'entrée sur un marché pour de nouveaux concurrents.

52. Comme l'ont noté la CMA et d'autres organismes interrogés, le partage d'informations avec différents acteurs du marché peut réduire l'emprise sur le marché d'un acteur dominant. En fonction de l'approche spécifique employée pour le partage de données, le respect d'obligations en matière de protection de la vie privée peut poser des problèmes de concurrence, tandis qu'un recours concurrentiel nécessitant que des données soient partagées peut porter atteinte aux droits à la vie privée. Comme indiqué précédemment, le défi consiste à trouver un terrain

d'entente entre les deux sphères réglementaires, qui protège à la fois la confidentialité et la concurrence, sans se nuire mutuellement, tout en continuant à développer et à soutenir une économie numérique stable.

53. Afin de parvenir à des résultats complémentaires à l'appui de l'économie numérique au Royaume-Uni, la CMA est devenue membre du Digital Regulation Cooperation Forum (**DRCF**), récemment établi. Le DRCF a été formé en juillet 2020 et a fait part de ses objectifs principaux et de son plan de travail en mars de l'année suivante.[13] L'objectif principal du DRCF est de permettre aux autorités participantes d'être mieux préparées à l'ampleur et à la nature globale des vastes plateformes numériques et à la vitesse croissante à laquelle elles innovent. Composé de la CMA, du Bureau du Commissaire à l'information (**BCI**), du Bureau des communications (**Ofcom**) et de la Financial Conduct Authority (qui a rejoint le forum en avril 2021), le DRCF espère tirer parti d'une coopération intersectorielle renforcée pour soutenir une approche réglementaire numérique cohérente et coordonnée. Comme l'indique le plan de travail pour 2021-2022 du DRCF, « une meilleure coordination peut à la fois aider les organismes de réglementation à relever les défis [posés par la réglementation numérique] dans son propre mandat tout en garantissant la mise en place d'une approche réglementaire cohérente pour les entreprises et les particuliers ».[14] Le DRCF illustre parfaitement la manière dont les autorités peuvent accroître la coopération intersectorielle, tout en remplissant leurs mandats d'application de la loi respectifs, grâce à un engagement stratégique et formalisé de ce réseau.

54. Bien qu'il n'a pas été cité au cours de l'entretien avec la CMA (car non publié à ce moment), le document *Competition and data projection in digital markets: a joint statement between the CMA and the ICO* [Concurrence et projection de données sur les marchés numériques : déclaration conjointe de la CMA et de l'ICO], publié en mai 2021, présente un bon exemple de la manière dont le DCRF peut promouvoir une collaboration accentuée entre les autorités responsables de la concurrence et celles chargées de la protection de la vie privée. Dans le

[13] Digital Regulation Cooperation Forum: Plan de travail pour 2021-2022, 10 mars 2021 - https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022

[14] Digital Regulation Cooperation Forum: Plan de travail pour 2021-2022, 10 mars 2021 - https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022

prolongement des travaux du DRCF, cette déclaration commune des membres CMA et BCI aborde les domaines clés de leur collaboration future, tels que :

- le rôle important que les données, notamment celles à caractère personnel, jouent dans l'économie numérique;
- les fortes synergies présentes entre les objectifs de la concurrence et ceux de la protection des données;
- la manière dont les deux organismes de réglementation collaboreront pour surmonter toute difficulté perçue entre leurs objectifs;
- des exemples pratiques de la manière dont les deux organismes collaborent déjà pour obtenir des résultats satisfaisants pour les consommateurs.[15]

55. En abordant les risques liés à l'économie numérique de manière coordonnée, le DRCF peut aider les consommateurs à faire des choix éclairés et judicieux, tant en ce qui concerne leurs achats que leurs droits à la vie privée. En réalité, il est même raisonnable de supposer que les consommateurs s'attendent intuitivement à la mise en place de mesures coordonnées de la part de leurs régulateurs.

56. Le DRCF et la déclaration commune de la CMA et du BCI ne sont que deux exemples de la manière dont les réglementations en matière de concurrence et de protection de la vie privée peuvent tirer profit du chevauchement ou de la proximité de ces secteurs et collaborer au profit des consommateurs et de l'économie numérique en général.

LE « PARADOXE EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE » ISSU D'UNE DÉFAILLANCE DU MARCHÉ

57. Plusieurs entretiens ont mentionné les difficultés liées à l'attribution d'une valeur aux renseignements et aux données à caractère personnel lorsque la protection de la vie privée est traitée comme un facteur non tarifaire dans une évaluation concurrentielle. Lorsque le sujet était abordé, il s'accompagnait souvent d'une référence au paradoxe en matière de protection de la vie privée, selon lequel, même si les individus prétendent accorder de l'importance à leur confidentialité, leurs actions suggèrent le contraire. Quelle que soit la raison derrière ce comportement, il souligne la difficulté d'apposer une valeur à la confidentialité en tant que facteur concurrentiel non tarifaire.

[15] Competition and data protection in digital markets: a joint statement between the CMA and the ICO, 19 mai 2021 - https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law

58. La CMA suggère que le paradoxe en matière de protection de la vie privée pourrait en réalité provenir du manque d'engagement des entreprises envers les particuliers en matière de confidentialité, plutôt que l'expression d'une préférence individuelle (ou de l'absence de préférence). Il a essentiellement été suggéré que de nombreuses entreprises font le strict minimum pour se conformer aux réglementations en matière de protection de la vie privée plutôt que de s'engager de manière significative avec leurs clients en ce qui concerne leurs pratiques et leurs préférences en matière de confidentialité. Il se peut qu'elles ne déploient pas autant d'efforts et d'attention pour cibler leurs clients dans leurs communications sur la protection de la vie privée que pour d'autres types de communication, telles que leurs sites Web ou leur présence sur les médias sociaux.

59. En effet, les entreprises surveillent et évaluent en permanence la manière dont leurs clients interagissent avec leurs sites Web ou leurs messages sur les médias sociaux. Si ces interactions sont jugées insuffisantes ou problématiques, les entreprises recenseront les éléments défaillants et remanieront la manière dont elles ciblent leurs clients, le cas échéant. La CMA suggère que le même niveau d'attention et de réactivité ne semble pas être appliqué aux communications relatives à la confidentialité. Les communications des entreprises relatives à la protection de la vie privée semblent être motivées par une obligation réglementaire plutôt que par un véritable désir de garantir la compréhension de leurs clients. Plutôt que d'élaborer des politiques concises, faciles à comprendre et à assimiler par leurs clients, elles leur présentent des politiques de protection de la vie privée longues, techniques et complexes, obligeant les consommateurs à les traduire en langage simple s'ils souhaitent réellement comprendre les implications en matière de protection de la vie privée et de prendre une décision « éclairée » quant au partage de leurs renseignements personnels. Les entreprises peuvent également avoir recours à des paramètres par défaut ou à une architecture de sélection favorisant ses intérêts commerciaux, plutôt que de permettre au client de s'impliquer véritablement et de faire ses propres choix.

60. Il a également été mentionné qu'au lieu de permettre une sélection libre et éclairée, l'effet pratique de ces obstacles à la sélection est de pousser les individus à cliquer simplement sur « accepter » afin d'obtenir le produit ou le service souhaité. Cette perspective est cohérente

avec les arguments relatifs au choix du consommateur et à la distorsion de la demande mentionnés dans le rapport *Digital Crossroads.*[16]

61. Ces points de vue et perspectives ont fait écho auprès des membres de l'équipe du GTCCN chargée des entretiens. Bien que l'existence d'un certain niveau de paradoxe en matière de protection de la vie privée est largement reconnue, sa cause est clairement sujette à débat. Si l'on cherche à déterminer un lien causale, conclure que les personnes qui partagent leurs données ne se soucient pas de leur confidentialité semble s'avérer prématuré. Conclure ainsi représenterait un cas assez important de déni où un groupe répondrait à l'inverse de ce qu'il ressent.

62. Nous sommes plutôt de l'avis qu'un paradoxe en matière de protection de la vie privée est dû, potentiellement et partiellement, à un malentendu sur ce que la vie privée signifie réellement. Certains assimilent à tort la vie privée au secret, plutôt qu'au contrôle sur ses renseignements personnels, et comment et quand les individus décident de les partager (c'est-à-dire, faire valoir ses droits en matière de liberté). Les individus peuvent être disposés à partager leurs renseignements personnels à des fins spécifiques, mais cela ne signifie pas pour autant qu'ils ne se soucient pas de la manière dont ces renseignements seront utilisés ou divulgués. Ils peuvent par exemple autoriser la géolocalisation pour se faire livrer une pizza à domicile, mais sans se rendre compte que leurs renseignements personnels seront partagés avec des tiers à des fins publicitaires.

63. En retournant la question du paradoxe et en l'abordant du point de vue du marché, nous pensons qu'il est judicieux de se poser les questions suivantes :

    i. Le paradoxe n'est-il pas plutôt le signe d'une défaillance du marché?

    ii. Le rassemblement et le traitement d'informations relatives à la confidentialité sont-ils devenus si chronophages et si onéreux pour les consommateurs que, plutôt que d'indiquer s'ils sont d'accord pour partager ces renseignements, ils abdiquent et

[16] Voir la partie 1, paragraphe 4(c) : Consumer Choice and the Challenges of Demand-Side Distortions du document Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

acceptent simplement les choix proposés juste pour conclure la transaction et utiliser le service?

64. Ces questions soulèvent une autre possibilité de collaboration entre les autorités chargées de la protection de la vie privée et celles responsables de la concurrence. Peu importe le raisonnement derrière le paradoxe en matière de protection de la vie privée, qu'il provienne de consommateurs répondant à l'inverse de ce qu'ils ressentent ou d'une défaillance du marché, nous notons le parallèle avec la grande variété de préférences en matière de prix sur multiples marchés et la manière dont ces préférences ont été intégrées avec succès dans les analyses concurrentielles. L'étude de la véritable nature du paradoxe en matière de protection de la vie privée peut aider les organismes responsables de la concurrence à mener des évaluations concurrentielles et, plus particulièrement, à comprendre la manière dont la demande en protection de la vie privée doit être modélisée avec précision dans les analyses antitrust. Si ce phénomène est effectivement lié à une défaillance du marché, les entreprises qui impliquent de manière accentuée les consommateurs pourrait contribuer à combler les lacunes des préoccupations exprimés par ceux-ci en matière de confidentialité et la manière dont ils agissent en fonction de ces préoccupations, ce qui, à son tour, pourrait permettre aux autorités responsables de la concurrence de mesurer plus facilement les incidences concurrentielles de la protection de la vie privée en tant que facteur non tarifaire.

PROTECTION DE LA VIE PRIVÉE : UNE ÉNIGME CONCURRENTIELLE (PLUTÔT QU'UN PARADOXE)

65. Quelles qu'en soient les causes, comme l'a mentionné la FTC des États-Unis, le fait que les individus disposent d'un large choix de préférences en matière de protection de la vie privée ne fait que compliquer l'évaluation des impacts concurrentiels de celle-ci. Il est difficile de capturer une image claire, ou cohérente, des préférences des consommateurs en matière de protection de la vie privée, et cela se traduit par des défis comparables dans l'évaluation de l'impact concurrentiel de la protection de la vie privée.

66. Il ne s'agit pas simplement de savoir si la protection de la vie privée sera entravée, mais si elle est un élément de la concurrence et si le comportement en cause finira par réduire ou prévenir la concurrence de manière générale. Étant donné que le marché ne révèle pas toujours les préférences des consommateurs en matière de confidentialité, plutôt que d'évaluer celle-ci, les

organismes de réglementation de la concurrence peuvent devoir se tourner vers d'autres indicateurs alternatifs ou considérations plus nuancées, ce qui rend plus difficiles le recensement et la quantification précise des conséquences concurrentielles de la protection de la vie privée. Un élément est apparu au cours de multiples entretiens : il est plus difficile de déterminer et d'évaluer la confidentialité en tant que facteur concurrentiel (qu'il s'agisse d'une hausse ou d'une baisse des niveaux de protection de la vie privée, ou de celle-ci en tant qu'indicateur de la qualité du produit) que de déterminer et d'évaluer un concept concurrentiel plus traditionnel, comme une hausse ou une baisse des prix. Le risque d'imposer à tort un jugement de valeur sur la protection de la confidentialité sur un marché, sur lequel celle-ci peut n'avoir aucun impact concurrentiel, constitue un autre défi.

67. Cela représente une autre occasion de renforcer la collaboration entre les autorités responsables de la concurrence et celles chargées de la protection des données. Bien que la confidentialité ne soit pas toujours un facteur concurrentiel, lorsqu'elle l'est, les autorités qui en ont la charge sont bien placées pour contribuer à la contextualisation de la manière dont elle peut être évaluée ou mesurée. En étoffant leur compréhension des préférences en matière de protection de la vie privée, les organismes responsables de la concurrence seront en mesure de déterminer plus facilement les conséquences associées à un plus large éventail d'évaluations concurrentielles, permettant ainsi à toutes les parties d'obtenir de meilleurs résultats.

ORGANISME D'APPLICATION DE LA LOI EN MATIÈRE DE CONCURRENCE PRENANT EN COMPTE LA PROTECTION DE LA VIE PRIVÉE

68. Au cours des entretiens, plusieurs organismes ont fait part des diverses approches qu'ils avaient adoptées pour intégrer la protection de la vie privée dans l'exécution de leur mandat. Parmi ces approches, on peut citer : élaborer des lignes directrices sur la manière dont la confidentialité peut être prise en compte dans les évaluations concurrentielles, tirer parti des possibilités de réglementation croisée avec des accords négociés, remettre en question la notion selon laquelle la confidentialité peut justifier un comportement anticoncurrentiel, ou affirmer carrément que les pratiques relatives à la confidentialité peuvent constituer un comportement anticoncurrentiel.

LIGNES DIRECTRICES RELATIVES À LA CONFIDENTIALITÉ EN TANT QUE FACTEUR CONCURRENTIEL

69. Sur le plan stratégique, l'entretien avec la Competition and Consumer Commission of Singapore (**CCCS**) décrivait les mesures prises dans le domaine des lignes directrices relatives à l'application de la loi. L'équipe d'entretien a appris qu'en septembre 2020, la CCCS a amorcé une consultation publique relative aux modifications proposées de ses lignes directrices sur la loi sur la concurrence (Cap. 50B), qui, entre autres, identifient spécifiquement la protection des données comme un aspect de la concurrence sur la qualité pouvant être pris en considération dans ses évaluations des fusions.[17] Reconnaissant l'importance d'être en contrôle ou en possession de données, la CCCS a également proposé des modifications aux lignes directrices de la CCCS sur l'interdiction aux termes de l'article 47, qui concerne l'abus de position dominante, afin de préciser que la CCCS se réserve le droit de prendre en compte d'autres déterminants concurrentiels dans son évaluation de l'emprise sur le marché, tels que le contrôle ou la possession de données. Les modifications proposées précisent également que si une « entreprise dominante » refuse de donner accès à des éléments clés, tels que des actifs physiques, des droits de propriété ou des données, cela peut se révéler être un abus de position dominante. Les lignes directrices révisées de la CCCS en matière de concurrence n'ont pas encore été publiées au moment de la préparation du présent rapport. Dans l'ensemble, la situation de Singapour met clairement en évidence les manières dont la protection des données peut être prise en compte dans les analyses antitrust. Elle souligne également la possibilité de collaboration entre les autorités responsables de la concurrence et celles chargées de la protection des données et de la vie privée, compte tenu de l'expertise et de l'avantage comparatif de ces dernières dans ce domaine.

CONFIDENTIALITÉ : ÉPÉE ET BOUCLIER DE L'APPLICATION DE LA LOI EN MATIÈRE DE CONCURRENCE

70. Alors que de nombreux organismes responsables de la concurrence ont mentionné des exemples hypothétiques de la confidentialité en tant qu'élément concurrentiel, au cours des entretiens, deux organismes ont tout de même fourni des exemples pratiques pour lesquels la confidentialité était au centre de leurs efforts d'application de la loi. Dans deux affaires d'abus de position dominante, engagées respectivement par le Bundeskartellamt (**BKartA**) et le Bureau

[17] Consultation publique relative aux modifications proposées des Lignes directrices en matière de concurrence - https://www.cccs.gov.sg/public-register-and-consultation/public-consultation-items/2020-public-consultation-on-proposed-changes-to-competition-guidelines?type=public_consultation

de la concurrence Canada (**BC**), la confidentialité a été présentée à la fois comme la cause et la justification d'un comportement anticoncurrentiel.

71. Comme le décrivent les réponses écrites du BKartA aux entretiens, l'organisme considère la protection de la vie privée, entre autres, comme une épée pour combattre les comportements anticoncurrentiels.

> L'affaire Facebook en Allemagne est un exemple frappant dans lequel la protection de la vie privée a été prise en compte par le Bundeskartellamt pour conclure qu'une pratique abusive était utilisée. L'utilisation privée du réseau permet à Facebook, à partir de sources extérieures au site, de collecter une quantité quasi illimitée de tout type de données relatives aux utilisateurs, de les attribuer aux comptes Facebook des utilisateurs et de les utiliser à de nombreuses fins de traitement des données. Les sources extérieures comprennent les services appartenant à Facebook, tels qu'Instagram ou WhatsApp, mais aussi les sites Web tiers comprenant des interfaces telles que les boutons « J'aime » ou « Partager ».
>
> Le Bundeskartellamt a estimé que les conditions de service de Facebook ainsi que la manière et l'étendue de la collecte et de l'utilisation des données par l'entreprise constituent un abus de position dominante. Afin d'évaluer si le comportement de Facebook au regard du droit de la concurrence était approprié[,] le Bundeskartellamt a tenu compte d'une éventuelle violation des règlements européens sur la protection des données au détriment des utilisateurs. **Notre autorité a coopéré étroitement avec celles chargées de la protection des données pour clarifier les questions de protection des données en instance**.
>
> …
>
> La décision du Bundeskartellamt n'est pas définitive, Facebook ayant fait appel de la décision. [souligné par l'auteur]

72. Dans une affaire antérieure, le BC a gagné un procès contre le Toronto Real Estate Board (**TREB**). Alors que le BKartA considérait la protection de la vie privée comme une épée, le TREB a utilisé, en vain, la législation canadienne relative à la vie privée dans le secteur privé comme un bouclier pour tenter de justifier ce qui a été considéré comme un comportement anticoncurrentiel par les tribunaux. L'affaire du BC concernait les restrictions imposées par le TREB sur l'utilisation et la divulgation en ligne par ses membres de certaines données importantes contenues dans le système Multiple Listing Service (une base de données contenant les annonces de propriétés actuelles et les données de ventes antérieures), y compris l'interdiction d'afficher ces données en ligne au moyen de bureaux virtuels sur le Web (**BV**). « Le Bureau prétend que les restrictions du TREB ont limité les incidences de nouveaux modèles d'affaires innovateurs, qui auraient représenté une menace concurrentielle pour les membres du TREB qui préféraient utiliser des

modèles d'affaires traditionnels. »[18] La défense du TREB alléguait que ces restrictions « avaient pour but de protéger la vie privée des consommateurs en conformité aux lois fédérales et aux exigences provinciales sur la vie privée des organismes de réglementation du secteur immobilier. »[19]

73. En fin de compte, le Tribunal de la concurrence du Canada a rejeté la défense du TREB en matière de protection de la vie privée et, en réponse à l'appel de celui-ci, la Cour fédérale d'appel du Canada a confirmé la décision du Tribunal et a conclu que :

> [131] Au sujet de la protection des renseignements personnels comme justification commerciale au regard de l'alinéa 79(1)(*b*), le Tribunal a conclu que la « **raison principale pour laquelle le TREB a mis en œuvre les restrictions relatives aux BV [bureaux virtuels] était qu'il voulait protéger ses membres contre les effets perturbateurs de la concurrence** des maisons de courtage faisant affaire sur Internet » (MT, par. 430). **Il a conclu qu'il n'y avait guère d'élément démontrant que les restrictions découlaient de soucis pour la protection des renseignements personnels** des clients du TREB. Le Tribunal a également relevé peu d'éléments établissant que, lors de l'élaboration de la politique sur les BV, le comité avait discuté de la protection des renseignements personnels et avait agi en conséquence (MT, par. 321). **La protection des renseignements personnels est invoquée « a posteriori et constituent à servir de prétexte** au TREB pour l'adoption et le maintien des restrictions relatives aux BV » (MT, par. 390). …
>
> [146] Toutefois, plus haut dans ses motifs, le Tribunal a écrit que « des considérations juridiques, comme les dispositions législatives sur la protection des renseignements personnels, qui justifient de façon légitime une pratique contestée, à la condition que les éléments de preuve démontrent que les comportements contestés étaient essentiellement motivés par de telles considérations » (MT, par. 294). …
>
> [147] Toutefois, il demeure que la société est tenue d'établir un lien factuel et juridique entre les prescriptions de la loi ou du règlement et la politique contestée.[20] [souligné par l'auteur]

74. Si les tribunaux canadiens ont rejeté les arguments du TREB en matière de protection de la vie privée, ils ont néanmoins laissé penser qu'une loi sur la protection de la vie privée pouvait

[18] Précis d'information : Abus de position dominante du Toronto Real Estate Board - https://www.canada.ca/fr/bureau-concurrence/nouvelles/2018/08/precis-dinformation-abus-de-position-dominante-du-toronto-real-estate-board.html

[19] Précis d'information : Abus de position dominante du Toronto Real Estate Board - https://www.canada.ca/fr/bureau-concurrence/nouvelles/2018/08/precis-dinformation-abus-de-position-dominante-du-toronto-real-estate-board.html

[20] Toronto Real Estate Board c. Commissaire de la concurrence, 2017-12-01, Dossier de la Cour d'appel fédérale : A-174-16, Référence : 2017 CAF 236 - https://decisions.fca-caf.gc.ca/fca-caf/decisions/fr/item/301595/index.do

justifier une conduite anticoncurrentielle, à condition de disposer de suffisamment de preuves pour étayer un tel argument.

ÉQUILIBRE ATTEINT ENTRE CONFIDENTIALITÉ ET CONCURRENCE

75. Lorsqu'il s'agit des intersections entre les réglementations de la confidentialité et celles de la concurrence, l'un des défis principaux consiste à trouver un équilibre entre les deux. Parvenir à un tel équilibre représente un objectif clair de collaboration entre les autorités, ou au sein d'une même autorité (c'est-à-dire, lorsque les législations en matière de confidentialité et de concurrence sont appliquées par le même organisme). Lorsque cela peut être évité, les marchés concurrentiels ne doivent pas négliger la protection de la vie privée, et celle-ci ne doit pas se faire au détriment de la concurrence et du bien-être des consommateurs. Afin d'illustrer cette notion, les paragraphes suivants présentent deux exemples d'organismes responsables de la concurrence allant au-delà des limites strictes de leur mandat et qui parviennent à intégrer la confidentialité dans leurs recours en matière de concurrence.

76. Le premier exemple provient de l'Australian Competition and Consumer Commission (**ACCC**) et de l'engagement de Transurban d'août 2018 relatif à l'acquisition proposée d'une participation majoritaire de l'autoroute WestConnex. L'ACCC avait peur que les données relatives au trafic, généralement non accessibles aux autres entreprises, donnent à Transurban un avantage concurrentiel sur les entreprises qui font face à des barrières d'entrées pour concurrencer avec succès pour les concessions des péages routiers. Pour répondre à ces préoccupations, l'ACCC a mis en place une solution de secours, décrivant que « l'objectif de l'engagement de Transurban… [était] de fournir aux soumissionnaires qui concourent pour les futures concessions pour des péages routiers en Nouvelle-Galles-du-Sud un accès aux données relevées de circulation possédées par Transurban Group en raison de ses intérêts importants dans les concessions pour des péages routiers. »[21]

77. Reconnaissant que lorsque les parties s'engagent à partager des données pour résoudre des problèmes de concurrence, et que cela doit être fait conformément aux lois pertinentes sur la protection de la vie privée, l'ACCC a accepté l'engagement proposé par Transurban. L'engagement est rédigé de sorte que Transurban n'est pas tenue de publier des données si cela

[21] https://www.accc.gov.au/public-registers/undertakings-registers/transurban-limited

devait l'amener à enfreindre les « obligations en matière de protection de la vie privée » définies dans l'engagement.[22]

78. Le deuxième exemple provient de la Superintendencia de Industria y Comercio de la Colombie concernant son évaluation de la création d'une nouvelle coentreprise numérique entre Bancolombia S.A., Banco Davivienda S.A. et Banco de Bogotá S.A. (appelées collectivement les **Banques**) et des recommandations correspondantes de la SIC à la Superintendencia Financiera de Colombia (l'organisme de réglementation financière de la Colombie). Dans le cadre de cette coentreprise numérique, les trois plus grandes banques colombiennes ont créé une nouvelle société chargée de fournir des services de recensement numérique à l'appui des services financiers fournis par les banques à leurs clients.

79. Comme c'est le cas de la FTC des États-Unis et comme indiqué ci-dessus, la SIC exerce multiples mandats d'application de la loi, notamment en matière de protection des consommateurs, de concurrence et de confidentialité. Consciente des répercussions de cette coentreprise numérique en matière de protection de la vie privée, et du besoin de celle-ci de gagner la confiance des consommateurs dans leurs services à travers la transparence et le respect de la réglementation colombienne en matière de protection de la vie privée, l'équipe chargée d'évaluer la proposition des Banques a consulté ses homologues chargés de la confidentialité pour savoir quelles considérations relatives à la protection de la vie privée devaient être incluses dans les recommandations de la SIC. À cette fin, malgré la nature compétitive de l'évaluation, plusieurs recommandations de la SIC étaient axées sur la confidentialité. Parmi ces recommandations, on peut citer :

    i. veiller à ce que les données relatives aux clients soient traitées conformément aux lois colombiennes sur la protection de la vie privée;

    ii. autoriser le transfert de données relatives aux clients à la nouvelle coentreprise uniquement si les banques ont obtenu leur consentement pour le faire;

[22] Clause 5.11 de l'engagement de Transurban à l'Australian Competition and Consumer Commission - https://www.accc.gov.au/system/files/public-registers/undertaking/Transurban%20Limited%20s87B%20undertaking%20%28redacted%29.pdf

iii. permettre la portabilité des données si de nouveaux acteurs créent des plateformes concurrentes.[23]

80. Les exemples australien et colombien illustrent comment parvenir à un équilibre entre les deux sphères réglementaires, grâce à des recours élaborés avec précaution, en fonction des interactions entre les facteurs liés à la confidentialité et à la concurrence. Dans les deux cas, des résultats favorables à la concurrence ont pu être obtenus sans sacrifier, et même en préservant, la protection de la vie privée.

PARTIE 4 – ENSEIGNEMENTS DU RAPPORT DIGITAL CROSSROADS

81. Dans le cadre de son « étude approfondie », le GTCCN souhaitait associer les conclusions du présent rapport avec celles d'un rapport universitaire, afin de fournir une analyse indépendante et scientifique des intersections entre les sphères réglementaires chargées de la confidentialité et de l'antitrust ou de la concurrence.

82. Le rapport *Digital Crossroads: The Interaction of Competition Law and Data Privacy*[24] [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données] présente de manière détaillée et opportune le paysage réglementaire intersectoriel actuel et les façons dont ces intersections peuvent évoluer à l'avenir. Conçu pour un public qui s'intéresse à la protection de la vie privée, *Digital Crossroads* présente une vaste introduction aux principales caractéristiques de l'analyse concurrentielle, des cadres théoriques pertinents pour la protection de la vie privée en tant que facteur des analyses concurrentielles, ainsi que des exemples et des études de cas très pertinents illustrant la relation complexe entre les deux sphères réglementaires.

[23] (Évaluation des banques et recommandations) *Respuesta a solicitud de análisis de una operación de intefración empresarial entre* ***BANCOLOMBIA S.A., BANCO DAVIVIENDA S.A. Y BANCO DE BOGOTÁ S.A.***, p. 18, (en espagnol seulement) – https://www.sic.gov.co/sites/default/files/files/integracion_empresarial/pdf/2019/julio/BANCOLOMBIA%20-%20DAVIVIENDA%20-%20BANCO%20DE%20BOGOT%c3%81.pdf

[24] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

83. Bien que ces deux rapports abordent en partie le même contenu, *Digital Crossroads* a mis en évidence trois thèmes principaux visant à comprendre la relation entre lois antitrust et protection des données, qui se retrouvent dans plusieurs de nos conclusions générales. Il convient de les examiner plus en détail dans cette partie.

84. Tout d'abord, *Digital Crossroads* met en évidence le fait que « la législation antitrust et celle relative à la protection des données se rencontrent de manière complexe et variée, en particulier dans l'économie numérique ».[25] Il poursuit en précisant que la relation entre les deux sphères réglementaires est nuancée, ses nombreuses interactions commençant seulement à être comprises de manière fiable. Ce thème est également beaucoup ressorti au cours de nos entretiens avec les autorités responsables de la concurrence. Bien que de nombreuses autorités n'ont pas nécessairement prévu que ces interactions se produiraient à un rythme aussi rapide, et qu'elles ne les ont pas non plus soigneusement examinées au cours de leurs enquêtes, il est tout de même généralement admis que ces intersections existent et qu'il faudra en tenir compte, aujourd'hui et à l'avenir. Il y a plus de dix ans, la dissidence de la décision de la FTC des États-Unis quant à la fusion entre Google et Double-click a certainement servi de référence préalable aux impacts négatifs sur la confidentialité. De plus, la déclaration commune de la CMA et du BCI sur le droit en matière de concurrence et de protection des données dans l'économie numérique[26] constitue une reconnaissance importante du fait que les intersections entre ces domaines réglementaires ne se matérialisent pas de manière isolée.

85. Le deuxième thème abordé par *Digital Crossroads* évoque l'idée selon laquelle « la théorie et la pratique à cette frontière législative sont à un stade précoce » et que les exemples pratiques sont eux « nouveaux et présentent d'importantes possibilités de développement. »[27] Cette constatation est systématiquement ressortie au cours de nos entretiens avec les autorités responsables de la concurrence. Qu'il s'agisse d'organismes n'ayant pas encore fait face à ces intersections dans leur travail quotidien ou d'organisations qui commencent seulement à appliquer hypothétiquement leur analyse réglementaire en vigueur à des considérations

[25] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737
[26] Déclaration conjointe de la CMA et du BCI sur le droit en matière de concurrence et de protection des données - https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law
[27] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

intersectorielles telles que la confidentialité, il est clair que l'examen de ces intersections est majoritairement à un stade précoce. Cette nouvelle frontière offre une excellente occasion de collaboration nationale et internationale pour développer des connaissances, des consensus et des cadres susceptibles de s'appliquer à l'ensemble des juridictions.

86. Dans sa conclusion, le rapport *Digital Crossroads* décrit le sentiment que « les autorités antitrust et celles chargées de la protection des données ne peuvent plus atteindre leurs objectifs de manière isolée ».[28] Les autorités partageant des « intérêts stratégiques communs » ainsi que l'objectif ultime de « satisfaire les consommateurs », il est primordial qu'elles collaborent afin d'élaborer des « stratégies d'application cohérentes et efficaces ». Les entretiens que nous avons eus avec les organismes ont révélé une réelle volonté de renforcer les efforts de collaboration. Si les avis divergent quant à l'éventuelle adaptation du droit de la concurrence pour inclure la protection de la vie privée dans les analyses contextuelles des facteurs anticoncurrentiels, un large soutien a été exprimé en faveur du dialogue et de la coopération avec les partenaires nationaux, ainsi qu'en faveur du partage des meilleures pratiques et des renseignements avec les partenaires et organismes internationaux. Même si certains organismes étaient assujettis à une législation nationale limitant le partage de renseignements avec des organismes ou des réseaux internationaux, on peut noter une volonté permanente de collaborer à l'échelle internationale, par le biais de groupes de travail et d'autres forums internationaux.

87. Les thèmes présentés ci-dessus ne sont qu'un très bref aperçu du rapport nuancé et approfondi du professeure Douglas, et de la manière dont il s'aligne sur nos propres conclusions, tirées des entretiens auprès des organismes. Nous pensons que le rapport *Digital Crossroads* formera la base de notre compréhension des intersections entre la protection des données et la concurrence. Plus important encore, nous insistons sur le fait qu'au fur et à mesure que ces intersections se manifestent en pratique, il sera de plus en plus nécessaire de collaborer entre autorités afin de surmonter tout obstacle réglementaire potentiel.

[28] Digital Crossroads: The Interaction of Competition Law and Data Privacy, par la professeure Erika Douglas, 6 juillet 2021 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737

CONCLUSION

88. Tout d'abord, le GTCCN et l'équipe chargée des entretiens pour cette « étude approfondie » souhaitent remercier toutes les autorités responsables de la concurrence pour leur participation, ainsi que pour les précieuses idées et perspectives partagées.

89. Les autorités interrogées ont prouvé qu'elles adoptent une approche progressive et proactive dans la prise en compte de la protection de la vie privée et des données dans leurs analyses antitrust. Même dans les juridictions n'ayant pas encore en place d'autorité chargée de la protection de la vie privée, il a été admis que règlementer des marchés fondés sur les données aura inévitablement des conséquences sur la confidentialité.

90. Nous avons bien compris que même avec une stratégie réglementaire plus « traditionnelle », il demeure important de prendre en compte la protection des données, en particulier lorsque celle-ci entre directement en ligne de compte dans l'analyse antitrust.

91. Dans la mesure où la protection de la vie privée et des données est nécessaire aux analyses concurrentielles, la collaboration et la consultation avec les autorités chargées de la protection de la vie privée, ayant plus d'expérience en ce qui concerne la surveillance de la protection de la vie privée et des données, peuvent aider celles responsables de la concurrence à améliorer la valeur prédictive des évaluations antitrust, notamment compte tenu de la difficulté à mesurer les facteurs qualitatifs liés à la confidentialité, moins objectifs que les facteurs traditionnels de prix ou de coût.

92. Nous avons également eu vent de modèles de collaboration donnant lieu à des réseaux de coopération plus formels, ayant comme objectif général de soutenir et de construire une économie et une société numériques stables, dont la promotion des intérêts et du droit à la vie privée des consommateurs sont des composantes indispensables.

93. Nous avons également constaté des exemples et des cas où, malgré l'existence de tensions entre les objectifs réglementaires, la consultation et la coopération permettaient des résultats satisfaisants pour les deux objectifs, plutôt que de sacrifier l'un ou l'autre.

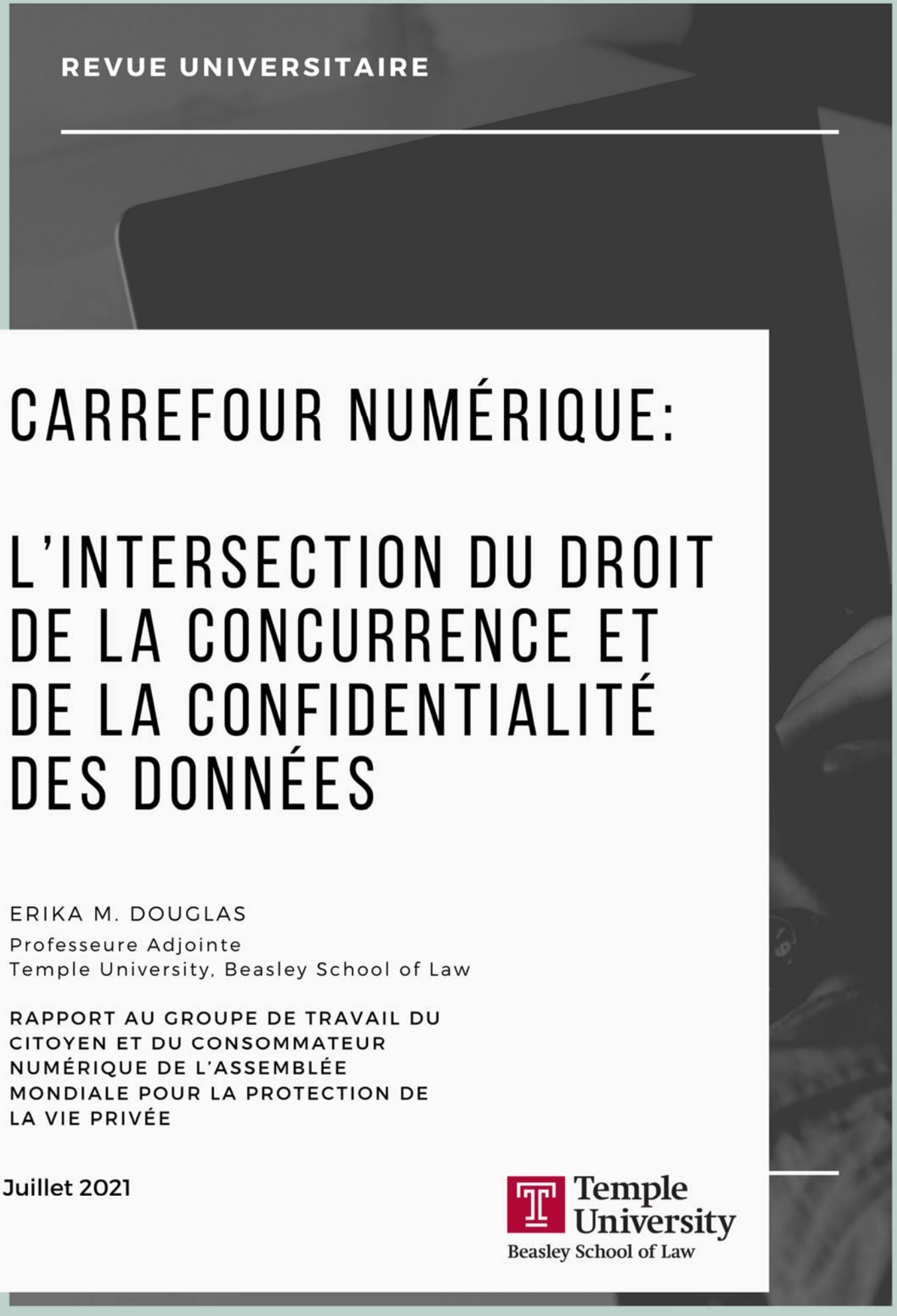
94. Le principal thème commun ressorti, quelle qu'en soit la forme ou la portée, est que la collaboration et la communication entre les sphères réglementaires ne peuvent que servir à

mieux satisfaire l'ensemble des citoyens. Un tel exercice, considéré de concert avec les réflexions de *Digital Crossroads*, sert à valider davantage un pilier clé du mandat du GTCCN : promouvoir et faciliter la coopération intersectorielle pour favoriser de manière générale l'intégralité des personnes que nous servons.

Annexe 2.

Digital Crossroads: The Intersection of Competition Law and Data Privacy [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données], par la professeure Erika Douglas de la Temple University Beasley School of Law

(Note – seulement l'Introduction et
Le Soummaire sont disponibles)



REVUE UNIVERSITAIRE

CARREFOUR NUMÉRIQUE:

L'INTERSECTION DU DROIT DE LA CONCURRENCE ET DE LA CONFIDENTIALITÉ DES DONNÉES

ERIKA M. DOUGLAS
Professeure Adjointe
Temple University, Beasley School of Law

RAPPORT AU GROUPE DE TRAVAIL DU CITOYEN ET DU CONSOMMATEUR NUMÉRIQUE DE L'ASSEMBLÉE MONDIALE POUR LA PROTECTION DE LA VIE PRIVÉE

Juillet 2021

Temple University
Beasley School of Law

Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données

Digital Crossroads: The Intersection of Competition Law and Data Privacy [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données]

Ce rapport a été rédigé avec l'aide dévouée à la recherche de Heather Kemp, Megan Gehret, Christopher Perkes, Megan Young et Alex Park. Nous remercions sincèrement l'équipe du Commissariat à la protection de la vie privée du Canada, Brent Homan, Adam Zimmerman et David Stenton, pour leur engagement à l'égard de la révision pendant le processus de rédaction. Toute erreur ou toute omission sont le fait de l'auteur.

Table des matières

Table des illustrations

Introduction

La législation antitrust et la législation sur la protection des données sont des forces puissantes qui façonnent notre économie. Il ne se passe guère de jour sans que l'un ou l'autre de ces régimes ne fasse la une des journaux. Il en résulte une multitude de nouvelles interactions entre ces domaines du droit, en particulier dans l'économie numérique.

La présente revue universitaire, *Digital Crossroads: The Intersection of Competition Law and Data Privacy* [Carrefour numérique : l'intersection du droit de la concurrence et de la confidentialité des données] (le rapport) a été rédigée pour le Groupe de travail du Citoyen et du consommateur numérique de la *Global Privacy Assembly (GPA)* (l'Assemblée mondiale pour la protection de la vie privée). Le rapport vise à recenser et à comprendre les interactions entre la législation antitrust et la confidentialité des données à l'échelle mondiale, du point de vue des organismes chargés de faire appliquer ces deux domaines du droit. Le rapport présente une typologie décrivant les points de croisement entre les deux domaines, sur la base d'une analyse des lois, des objectifs, de la politique, des priorités d'application et des préoccupations des organismes concernés.

Comme le décrit le présent rapport, les interactions entre les lois antitrust et la protection des données sont naissantes, variées et complexes. Bien que souvent décrite comme simplement complémentaire, la relation entre la législation antitrust, la concurrence elle-même et la confidentialité des données est souvent beaucoup plus nuancée et multiforme. Dans certains domaines, notamment l'examen des fusions, de nouvelles théories s'imposent pour aborder la question de la confidentialité des données. Dans d'autres, comme les recours antitrust, le sentiment que les deux domaines peuvent se recouper n'est que naissant. Il reste cependant beaucoup de place pour le perfectionnement de la théorie et de la pratique dans ce paysage du droit antitrust et de la confidentialité des données.

L'objectif de ce rapport est d'approfondir la compréhension commune des sources faisant autorité en matière de législation antitrust et de confidentialité des données concernant les nombreux chevauchements entre leurs domaines. Il s'agit d'une intersection juridique en évolution rapide qui revêt une grande importance pour les consommateurs. Elle exige une attention et une coopération entre les divers organismes afin de développer des stratégies d'application numérique cohérentes et efficaces. Nous espérons que ce rapport contribuera à une compréhension accrue des diverses doctrines et incitera les organismes du monde entier à élaborer des théories, des méthodes de collaboration et des pratiques exemplaires communes à ce nouveau carrefour numérique.

Sommaire

Le présent rapport, rédigé pour le Groupe de travail du citoyen et du consommateur numérique de l'Assemblée mondiale pour la protection de la vie privée, vise à examiner, à décrire et à classer les points de vue des organismes chargés de l'application de la loi sur l'intersection entre la confidentialité des données et la législation antitrust.

Comme en témoignent la longueur et l'ampleur de ce rapport, nous entrons dans une ère d'interaction sans précédent entre la législation antitrust et la législation sur la confidentialité des données. Cette intersection du droit s'est développée de façon spectaculaire ces dernières années, pour les raisons présentées ci-dessous.

- **L'expansion mondiale de la législation sur la confidentialité des données :** Aujourd'hui, environ 130 jurisdictions disposent d'une forme de législation sur la confidentialité des données ou la protection des données.[1] Au moins vingt autres jurisdictions indiquent qu'un projet de loi sur la confidentialité des données est à l'étude.[2] Plusieurs d'entre elles sont en train de modifier et d'étendre leurs lois existantes. Ce raz-de-marée de lois sur la protection de la vie privée, et leur application, a donné naissance à une nouvelle ère de la confidentialité des données autant pour les consommateurs que les entreprises.

- **Un regain d'attention mondiale pour l'application de la législation antitrust :** Le droit et la politique antitrust ont connu une relance mondiale, avec un regain d'attention pour la concurrence numérique et un certain nombre de nouvelles affaires importantes pour les organismes. Nombre de ces affaires antitrust sont dirigées contre de grandes plateformes numériques, les mêmes entreprises qui attirent souvent l'attention des responsables de la confidentialité des données.

- **Les deux régimes juridiques se concentrent sur l'économie numérique :** C'est dans l'économie numérique que les interactions entre la législation antitrust et la confidentialité des données sont les plus marquées, et les plus courantes. Qu'il s'agisse de publicité, de recherche, de médias sociaux ou d'une myriade de services de

[1] Conférence des Nations Unies sur le commerce et le développement (CNUCED), *Data Protection and Privacy Legislation Worldwide* [Législation relative à la protection ou la confidentialité des données à l'échelle mondiale] (4 février 2020), https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (mentionnant que 128 des 194 pays étudiés avaient adopté une forme quelconque de législation relative à la protection ou à la confidentialité des données).

[2] *Id.* (déclaration exhaustive des données au 27 février 2021).

géolocalisation en ligne, de nombreuses entreprises numériques sont régies par le traitement des données personnelles. Cette situation a placé l'économie numérique au centre de l'application des lois sur la confidentialité des données. La taille et l'importance économique de nombreuses plateformes numériques en ont fait une priorité stratégique pour la législation antitrust. Qu'il s'agisse de marchés numériques, de publicité, de mégadonnées, de produits à prix zéro ou autres, la législation antitrust et la confidentialité des données occupent les mêmes espaces dans la politique, le droit et l'application.

Cette évolution du droit et de l'économie a donné lieu à une multitude de nouvelles interactions entre la législation antitrust et la confidentialité des données. Tout au long de la discussion, le présent rapport met l'accent sur trois grands thèmes qui caractérisent ce carrefour juridique.

Thèmes du rapport : Comprendre l'intersection de la législation antitrust et de la confidentialité des données

1. **Le droit antitrust et le droit relatif à la confidentialité des données se recoupent de façon complexe et multiforme, en particulier dans l'économie numérique.** Bien qu'elle soit souvent résumée comme étant complémentaire ou en tension, la relation entre le droit antitrust et la confidentialité des données est plus nuancée. Un examen plus approfondi révèle un paysage d'interactions à multiples facettes, dont beaucoup commencent seulement à être reconnues et comprises.

2. **La théorie et la pratique à cette frontière du droit n'en sont qu'à leurs débuts.** Bien que l'interaction entre le droit antitrust et le droit relatif à la confidentialité des données soit de plus en plus reconnu, la théorie et la pratique au sein de ce paysage juridique demeurent relativement récentes, et présentent d'importantes possibilités de développement.

3. **Les autorités chargées de la protection des données et les autorités antitrust ne peuvent plus atteindre leurs objectifs en vase clos.** Ces autorités ont de nombreux intérêts stratégiques communs, l'accent étant mis sur l'économie numérique et l'objectif ultime étant d'en faire profiter les consommateurs. Cette intersection du droit, qui évolue rapidement, exige une coopération entre les organismes afin de rendre possible le développement des stratégies d'application cohérentes et efficaces pour l'économie numérique. Étant donné que ces domaines juridiques interagissent de plus en plus, l'application cloisonnée de la législation antitrust et de la législation sur la protection des données compromettra les intérêts communs des responsables de l'application des lois, en créant des lacunes, des chevauchements et des tensions inutiles ou involontaires entre les

deux domaines juridiques.

Méthodologie et portée de la recherche

- **Les recherches effectuées dans le cadre de ce rapport ont consisté en l'examen de plus de 200 documents en anglais, accessibles au public, relatifs aux organismes antitrust et de protection des données à l'échelle mondiale.** Ces documents vont des objectifs législatifs (dans la loi d'habilitation de l'organisme) aux décisions de l'organisme, en passant par le dépôt de plaintes, l'orientation, les discours, les soumissions, les études de marché ou de secteur et d'autres documents pertinents provenant d'entités telles que l'Organisation de coopération et de développement économiques (OCDE) et l'Assemblée mondiale pour la protection de la vie privée elle-même. La recherche s'est concentrée sur les administrations qui font partie du Groupe de travail du citoyen et du consommateur numérique et de l'Assemblée mondiale pour la protection de la vie privée.

- **Le rapport ne traite pas de l'interaction entre le droit de la protection des consommateurs et le droit relatif à la protection de la vie privée.** Bien qu'importante et souvent liée au sujet abordé ici, l'intersection entre la législation sur la protection des consommateurs et la confidentialité des données fait l'objet d'un rapport antérieur du Groupe de travail du citoyen et du consommateur numérique de l'Assemblée mondiale pour la protection de la vie privée .

- **Le rapport est utile aux responsables de l'application de la législation antitrust et de la confidentialité des données, mais il a été rédigé principalement pour un public de protection de la vie privée cherchant à comprendre la pertinence potentielle du droit et de la politique antitrust dans le cadre de leur travail.**

État de la collaboration entre les organismes antitrust et les organismes responsables de la confidentialité des données

- **Il n'existe pas de modèle unique de responsabilité des organismes pour l'application de la législation antitrust ou de la législation sur la confidentialité des données dans le monde.** Dans certains territoires de compétence, la législation antitrust et la législation sur la confidentialité des données sont appliquées par des autorités réglementaires

distinctes. Dans d'autres, la même autorité est responsable de l'application des deux domaines du droit, et parfois aussi de la législation relative à la protection des consommateurs.

- **Il y a quelques années à peine, le contrôleur européen de la protection des données s'est inquiété du fait que l'application de la législation antitrust et de la législation sur la confidentialité des données se font trop souvent séparément en vase clos,** et des défis croissants que cette séparation posera pour la réglementation de l'économie numérique.

- **De nos jours, la collaboration entre organismes s'accroît rapidement, autant en fréquence qu'en portée, dans les domaines de la législation antitrust et de la confidentialité des données. Les autorités de plusieurs juridictions ont pris des mesures pour approfondir ou renforcer la collaboration dans leurs sphères de responsabilité,** notamment en reconnaissant que la coopération est une question d'importance stratégique, en exécutant des accords de collaboration entre organismes, en publiant des consignes d'orientation communes, en coopérant sur des questions individuelles et en mettant sur pied des initiatives structurelles conçues pour renforcer les connaissances et les pratiques exemplaires entre les diverses doctrines. Les exemples d'une telle coopération sont résumés ici et font l'objet d'un suivi plus approfondi dans un rapport antérieur du Groupe de travail du citoyen et du consommateur numérique de l'Assemblée mondiale pour la protection de la vie privée.

Partie I. Comprendre la complémentarité et les tensions à la base de la législation antitrust et de la confidentialité des données

La première partie est consacrée à l'examen des fondements de la législation antitrust et de la législation sur la confidentialité des données, qui influent sur leurs interactions. On y examine le cadre juridique des droits et des intérêts en matière de protection de la vie privée, les raisons pour lesquelles les deux domaines du droit interagissent, les différences entre les objectifs législatifs de chaque régime et les intérêts stratégiques communs aux deux.

- **Les conceptions du « droit de la confidentialité des données » diffèrent à l'échelle mondiale.** Comme souligné dans cette section et discuté tout au long du rapport, la législation relative à la protection de la vie privée et la législation antitrust varient selon les territoires de compétence. Les interactions entre ces deux domaines du droit varient donc également.

    - Dans l'Union européenne et ses États-nations, la confidentialité des données est un droit protégé par la constitution. Dans des administrations comme les États-Unis, la loi fédérale sur la confidentialité des données est une sous-catégorie de la loi sur la protection des consommateurs. Dans d'autres pays encore, comme l'Australie et le Canada, la législation sur la confidentialité des données est conçue principalement en termes de principes, plutôt que de droits ou de protection des consommateurs. Les racines juridiques de la confidentialité des données évoluent dans certains territoires de compétence, avec l'émergence de conceptions des droits dans certains États et secteurs, et la reconnaissance judiciaire du statut quasi-constitutionnel du respect de la vie privée.

    - Ces différences conceptuelles à la base de la législation sur la confidentialité des données, sont susceptibles d'avoir une incidence sur son interaction avec la législation antitrust. Les conceptions fondées sur les droits peuvent renforcer les arguments en faveur d'une prise en compte expresse du respect de la vie privée dans l'analyse de la concurrence, et peuvent également présenter une réconciliation « pommes-oranges » entre les droits relatifs à la protection de la vie privée et les intérêts économiques avancés par le droit de la concurrence. Dans des administrations comme les États-Unis, où la concurrence et la protection de la vie privée sont toutes deux formulées en termes économiques, l'analyse des compromis entre les deux intérêts peut devenir moins complexe, en vertu de leurs bases conceptuelles communes.

        - Ces différences dans la façon dont la protection de la vie privée est conçue se retrouvent tout au long du présent rapport. Les organismes de l'Union européenne ont accordé une plus grande attention à la conciliation du droit de la concurrence et du droit relatif à la protection des données, au moins en partie parce que cette attention est exigée par la robustesse des droits relatifs à la protection de la vie privée du Règlement général sur la protection des données (RGPD) et leur pertinence correspondante pour la concurrence axée sur les données.

- Cette section adopte une définition de travail du « droit sur la protection des renseignements personnels » aux fins du rapport, laquelle est axée sur la façon dont le concept est perçu à son point d'intersection avec le droit et la politique antitrust. La définition se limite i) à la confidentialité des renseignements ou des données en ce qui concerne les droits ou les intérêts légalement protégés d'une personne à contrôler le traitement de ses renseignements personnels et ii) aux obligations en matière de confidentialité des entités non gouvernementales, étant donné que la législation antitrust s'intéresse principalement au rôle des données dans les entreprises et la concurrence, plutôt qu'à l'utilisation des données par le gouvernement.

- **Au plus haut niveau d'abstraction, la législation relative à la confidentialité des données et la législation antitrust cherchent toutes deux à procurer des avantages aux consommateurs. Toutefois, la législation relative à la confidentialité des données et la législation antitrust fixent des objectifs différents, qui reflètent les approches distinctes de chaque domaine pour obtenir des avantages pour les consommateurs.**

  - Alors que la législation relative à la confidentialité des données se concentre sur la protection des intérêts des personnes en matière de protection de la vie privée, le principal objectif de la législation antitrust moderne est de promouvoir le bien-être économique des consommateurs par l'entremise de la concurrence. La législation antitrust vise à bénéficier aux consommateurs par l'intermédiaire d'une prescription large d'efficacité économique, contrairement aux droits ou intérêts individuels protégés de façon caractéristique par la législation sur la protection des renseignements personnels.

  - Les juridictions comme les États-Unis, qui se concentrent étroitement sur l'objectif d'efficacité économique, sont plus réticents à intégrer d'autres considérations comme la protection de la vie privée dans l'analyse de la législation antitrust. L'inclusion de la protection de la vie privée dans l'analyse de la concurrence est une source de préoccupation – en particulier lorsque les effets de la protection des renseignements personnels ne sont pas liés à la concurrence – et pourrait diluer ou confondre l'application des normes fondées sur l'efficacité économique, ce qui ne permet pas d'établir clairement quels facteurs devraient déterminer les résultats des affaires ou des politiques antitrust.

  - En plus de l'objectif principal qu'est le bien-être économique des consommateurs, plusieurs juridictions incluent également des objectifs en matière de répartition dans leur législation sur la concurrence, tels que l'équité ou la fourniture

d'opportunités équitables pour les entreprises. Les juridictions qui poursuivent ces objectifs antitrust plus larges pourraient disposer d'une plus grande marge de manœuvre pour l'inclusion des considérations relatives à la confidentialité des données dans l'analyse antitrust, par rapport aux pays comme les États-Unis qui s'en tiennent strictement à l'objectif du bien-être économique des consommateurs.

- **Malgré les objectifs distincts de la législation antitrust et de la législation sur la confidentialité des données, les documents des organismes reflètent clairement plusieurs intérêts politiques communs. Nombre de ces intérêts communs sont liés à l'économie numérique.**

    - Les responsables de l'application de la législation antitrust et de la confidentialité des données visent à promouvoir la confiance des consommateurs dans les marchés numériques. La confiance est considérée comme un précurseur de la pleine participation économique et de ses avantages concomitants pour les consommateurs.

    - Les deux régimes juridiques considèrent que la portabilité des données est bénéfique, tant pour le respect de la vie privée que pour la concurrence.

        - Les juridiction partout dans le monde accordent et interprètent de nouveaux droits de portabilité des données dans le cadre de leurs lois sur la protection des données.

        - Ces droits à la portabilité des données sont devenus l'un des domaines de complémentarité sur lequel le plus grand accent a été mis entre la législation relative à la confidentialité des données et la politique en matière de concurrence. La portabilité des données est censée promouvoir la concurrence axée sur les données, en réduisant les obstacles au passage d'un service à un autre pour les consommateurs. On pense que cela permet aux nouvelles entreprises d'obtenir plus facilement les données nécessaires pour entrer sur un marché ou accroître le nombre de leurs produits ou services qui y sont offerts.

        - Les droits de portabilité des données sont généralement considérés comme un élément positif pour la concurrence, mais ces droits ne sont pas nécessairement suffisants pour assurer une concurrence solide sur certains marchés. Plusieurs autorités antitrust ont considéré qu'au-delà de la portabilité des données, des modèles plus étendus de mobilité des données,

comme les normes ouvertes ou l'interopérabilité, étaient potentiellement nécessaires pour rétablir la concurrence. Des initiatives antitrust notables ont été prises pour promouvoir la concurrence par l'interopérabilité dans le secteur bancaire.

- Les deux régimes juridiques visent à encourager et à maintenir le choix des consommateurs sur les marchés. Les autorités antitrust et les autorités chargées de la confidentialité des données se préoccupent toutes deux des phénomènes qui ont une incidence sur le choix du consommateur, notamment les biais comportementaux, les asymétries d'information et le choix limité ou complexe de produits et de services, en particulier dans le domaine des produits et services numériques.

Partie II. Théorie et pratique à l'intersection de la législation antitrust et de la confidentialité des données

La deuxième partie du rapport présente les principales théories sur l'interaction entre la législation antitrust et la confidentialité des données. Elle se penche ensuite sur l'application pratique de cette théorie, et d'autres, en passant par plusieurs thèmes majeurs de la législation antitrust : définition du marché et pouvoir de marché, examen des fusions, abus de position dominante, cartels ou collaborations entre concurrents, et recours.

- **La principale théorie sur cette intersection du droit postule que l'analyse antitrust doit tenir compte de la confidentialité des données lorsque - et seulement lorsque - la confidentialité est un paramètre de la qualité du produit (ou du service) qui est touché par la concurrence.** Dans le rapport, on fait allusion à la théorie du « respect de la vie privée en tant que qualité ».

  - Par exemple, les entreprises pourraient se faire concurrence pour offrir aux consommateurs des fonctions de protection des renseignements personnels plus efficaces, ou moins de collecte et de traitement des données personnelles. Prenons l'exemple d'une fusion entre deux sociétés de services de navigateurs Internet qui se font concurrence pour offrir aux utilisateurs des fonctions en ligne de protection de la vie privée. L'opération pourrait réduire le niveau de concurrence sur le marché des navigateurs pour offrir de telles fonctions. Si cette réduction de la concurrence est susceptible de provoquer un déclin de la protection de la vie privée parmi les navigateurs, l'évaluation antitrust de la fusion tiendra compte de cet effet sur la qualité liée à la protection de la vie privée. Le déclin de la qualité de la protection de la vie privée pourrait inclure une dégradation du niveau de

protection de la vie privée offert, ou une augmentation du volume de données personnelles traitées sans avantages compensatoires.

- Cette théorie pourrait également s'appliquer lorsque le comportement anticoncurrentiel d'une entreprise dominante entraîne une réduction de la concurrence et de la qualité liée à la protection de la vie privée. La division antitrust du ministère américain de la justice allègue cet effet dans une récente plainte pour monopolisation déposée contre Google, soutenant que [en restreignant la concurrence dans le domaine de la recherche, le comportement de Google a porté préjudice aux consommateurs en réduisant la qualité de la recherche (notamment sur des aspects tels que la protection de la vie privée, la protection des données et l'utilisation des données des consommateurs).] [Traduction][3]

- À l'inverse, lorsqu'une fusion ou un comportement répréhensible est susceptible d'avoir pour effet d'accroître la qualité de la protection de la vie privée par l'entremise de la concurrence, l'évaluation de la législation ou de la politique antitrust considérerait que cet effet est positif.

- **Cette théorie du « respect de la vie privée en tant que qualité » est le point de vue des organismes le plus largement exprimé sur la relation entre la confidentialité des données et le préjudice antitrust potentiel. Toutefois, ses implications et ses applications potentielles en sont encore à un stade précoce de compréhension et d'élaboration.** En théorie, la confidentialité pourrait être vue comme un élément de qualité dans de nombreux domaines de la législation antitrust. En pratique, comme l'explique le présent rapport, l'examen des fusions a été le principal contexte de l'analyse antitrust de la concurrence fondée sur la protection de la vie privée, avec une application très précoce dans les cas d'abus de position dominante.

- **Cette théorie du respect de la vie privée en tant que qualité permet à la fois d'intégrer et de limiter le rôle de la confidentialité des données dans l'analyse antitrust.**

  - **Cette théorie intègre la confidentialité des données dans des cadres analytiques antitrust établis de longue date,** lesquels reconnaissent que la

[3] Communiqué de presse, U.S. Department of Justice, *Justice Department Sues Monopolist Google for Violating Antitrust Laws* [Le ministère de la justice poursuit le monopoleur *Google* pour violation des lois antitrust] (20 octobre 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

qualité peut être à la base de la concurrence sur certains marchés. Elle le fait en interprétant le concept de « qualité » comme suffisamment large pour englober la qualité des offres en matière de confidentialité sur un marché.

- **Les organismes antitrust considèrent également que cette théorie limite leur compétence.** Lorsqu'une fusion ou un délit donne lieu à des préjudices pour le respect de la vie privée qui ne sont pas liés à la concurrence - ce que l'on pourrait désigner des préjudices « purs » pour le respect de la vie privée - de nombreuses autorités antitrust ont estimé que ces préjudices ne relevaient pas de leur compétence et qu'il était plus convenable qu'ils relèvent de la législation relative à la protection des données.

- **Bien que la théorie du respect de la vie privée en tant que qualité soit de plus en plus acceptée par les autorités antitrust, son application risque de poser des problèmes pratiques.** En particulier, il pourrait s'avérer difficile de mesurer précisément les effets de la protection de la vie privée sur la concurrence.

  - Les théories et les modèles antitrust établis sont principalement axés sur le prix. La mesure des effets non tarifaires est depuis longtemps reconnue comme un défi pour la législation antitrust - les difficultés probables de l'analyse de la qualité de la protection de la vie privée ne sont que la dernière incarnation de cette question plus large.

  - Il existe également certains facteurs spécifiques qui pourraient rendre plus difficile la mesure des effets de la protection de la vie privée sur la concurrence, notamment : les préférences souvent hétérogènes des consommateurs en matière de protection de la vie privée, la possibilité de compromis entre la protection de la vie privée et d'autres paramètres de qualité des produits dans la conception des produits et des services (par exemple, un suivi en ligne accru en échange d'une publicité comportementale mieux ciblée) et les distorsions dans le choix des consommateurs en matière de protection de la vie privée (comme les biais comportementaux).

  - La traduction des effets de la protection de la vie privée ou de la confidentialité des données en valeurs monétaires estimées ne résout pas nécessairement ces difficultés à mesurer les effets du respect de la vie privée relativement à la concurrence. Au moins une administration a décrit cette analyse d'équivalence du « prix » des données comme étant profondément incompatible avec une vision de

la confidentialité des données fondée sur les droits.

- Les affaires et enquêtes antitrust ont utilisé certains types de preuves pour déterminer si la confidentialité des données est à la base de la concurrence, et les paramètres potentiels de cette concurrence. Bien que nous en sommes à un stade précoce, ces preuves comprennent : des sondages auprès des consommateurs et des concurrents pour établir si la confidentialité des données est un moteur de la concurrence, des observations des comportements liés à la confidentialité sur le marché (par exemple, si des entreprises concurrentes modifient leurs politiques de confidentialité en réaction les unes aux autres) et des documents internes d'entreprise (par exemple, pour donner un aperçu des raisons pour lesquelles une entreprise a modifié sa politique de confidentialité). L'OCDE a également suggéré que l'analyse de la quantité et de la nature des données personnelles traitées pourrait être utile pour comprendre la concurrence liée au respect de la vie privée.

- Malgré ces nouvelles sources de preuves, certaines difficultés persistent, car il n'existe aucune approche analytique établie, ni même d'ensemble clair d'options potentielles, pour évaluer l'ampleur ou la nature spécifique des effets liés au respect de la vie privée dans l'analyse antitrust.

- **L'absence d'outils analytiques établis et fiables pour évaluer les effets de la concurrence sur la qualité de la protection de la vie privée est susceptible de constituer un obstacle à l'intégration des considérations relatives à la confidentialité dans l'analyse antitrust**.

- **Cette lacune offre également une possibilité importante de collaboration entre les autorités chargées de la protection des données et les autorités antitrust dans le but de concevoir une méthodologie et des outils fiables et bien fondés pour mesurer les effets liés à la concurrence sur la qualité du respect de la vie privée.** En particulier, l'expertise spécialisée des autorités chargées de la protection des données dans la mesure et l'évaluation de la protection de la vie privée, ainsi que les effets de la conduite du marché sur la protection de la vie privée, pourraient fournir des renseignements précieux aux autorités antitrust qui cherchent à évaluer les effets de la protection de la vie privée sur la concurrence.

A. Confidentialité, définition du marché et pouvoir du marché

- **Droit antitrust :** Le point de départ de l'analyse antitrust est souvent la définition des marchés antitrust pertinents et l'évaluation de la puissance d'une entreprise sur l'un ou l'autre de ces marchés.

- **Ni la définition du marché ni l'analyse du pouvoir de marché ne se sont concentrées expressément sur la confidentialité.** L'analyse antitrust s'est plutôt penchée sur les défis plus larges posés par les marchés numériques, notamment :

    - les divers rôles joués par les données dans la stimulation (ou la limitation) de la concurrence et du pouvoir de marché;

    - les marchés « à prix zéro », terme utilisé pour désigner les marchés où les produits ou services n'ont pas de prix monétaire, mais où les utilisateurs doivent fournir leurs données. De nombreux marchés numériques proposent des produits à prix zéro. Comme le prix ne peut constituer la base de la concurrence sur ces marchés, le respect de la vie privée et d'autres aspects de la qualité du produit peuvent jouer un rôle plus important dans la concurrence.

- **En examinant les marchés numériques, les organismes antitrust ont eu tendance à réaffirmer la résilience, la souplesse et l'applicabilité des cadres analytiques existants pour le pouvoir de marché et la définition du marché.** En même temps, les organismes reconnaissent que ces marchés numériques ont souvent des caractéristiques communes qui présentent des défis analytiques sur le plan de la législation antitrust.

- **La définition moderne du marché, notamment dans le cadre de l'examen des fusions, tend à reposer sur des méthodologies axées sur le prix.** Cette analyse axée sur le prix est mal adaptée aux produits ou aux services à prix zéro, qui ne facturent pas de prix monétaire aux consommateurs.

    - Au lieu de cela, de nombreuses administrations se sont penchées sur la question de savoir si l'analyse pourrait utiliser un test de diminution non transitoire de la qualité, faible, mais significative, pour définir les marchés antitrust pertinents. Les discussions sur cette analyse reconnaissent souvent qu'un test fondé sur la qualité sera plus difficile à mettre en œuvre que l'analyse standard basée sur le prix.

- **Les autorités antitrust ont récemment accordé une grande attention aux deux sujets particuliers suivants dans la discussion sur le pouvoir de marché numérique.**

- **La question de savoir si et quand les données peuvent conférer un pouvoir de marché ou un avantage concurrentiel.** Il s'agit notamment de déterminer si l'échelle et la portée de l'accumulation de données pourraient constituer une barrière à la concurrence sur certains marchés. Lorsqu'une entreprise accumule des données qui sont uniques et difficiles à reproduire par les concurrents en termes d'échelle ou de type, cela peut créer des barrières à l'entrée de la concurrence sur le marché et contribuer au pouvoir de marché de l'entreprise. Toutefois, sur certains marchés, les concurrents pourraient être en mesure de reproduire eux-mêmes l'ensemble de données de valeur ou il se pourrait que des facteurs autres que l'accumulation de données (tels que l'expertise dans l'analyse ou l'utilisation des données) créent un avantage concurrentiel. Le pouvoir de marché doit toujours être évalué au cas par cas dans le cadre de la législation antitrust.

- **Le rôle des effets de réseau dans le pouvoir de marché.** Les effets de réseau sont courants dans les services numériques, tels que les réseaux sociaux ou les applications de l'économie du partage (« gig »), où plus le nombre d'utilisateurs est important, plus le service a de la valeur pour les autres utilisateurs. Les autorités antitrust s'intéressent à la façon dont les effets de réseau peuvent amplifier - ou réduire - le pouvoir de marché. On a tendance à dire que les effets de réseau renforcent le pouvoir de marché des entreprises en place, mais ils peuvent aussi jouer un rôle bénéfique dans la promotion de la concurrence.

- **Les parts de marché sont souvent un facteur important dans l'analyse antitrust du pouvoir de marché.** Les mesures des revenus et des profits constituent généralement une base commune pour mesurer les parts de marché. Sur les marchés à prix zéro, cependant, des mesures différentes ou supplémentaires de la part de marché pourraient être importantes, comme le nombre d'utilisateurs ou la part des interactions pertinentes (telles que le nombre de vues, de recherches ou de transactions). En fin de compte, la mesure pertinente de la part de marché sera très spécifique au marché étudié, et souvent sujette à débat.

- **Bien que la législation antitrust soit confrontée à certains défis dans la définition des marchés à prix zéro et l'estimation du pouvoir de marché dans les contextes numériques, dans la pratique, ces défis n'ont pas été suffisamment importants pour entraver l'application de la législation antitrust.** Les organismes antitrust ont régulièrement défini les marchés et conclu que le pouvoir de marché est détenu par certaines plateformes numériques qui offrent des services à prix zéro.

B. Examen des fusions et confidentialité des données

- **Droit antitrust :** Partout dans le monde, les organismes responsables de la concurrence sont habilités à examiner et à contester les fusions (et autres transactions d'entreprises) qui sont susceptibles d'avoir des effets négatifs importants sur la concurrence.

- **Les organismes antitrust ont davantage tenu compte de la pertinence de la concurrence fondée sur la protection de la vie privée dans l'examen des fusions que dans d'autres domaines de la législation antitrust, bien que l'interaction en soit encore à ses débuts en théorie et en pratique.** Dès 2006-2007, les autorités antitrust américaines et européennes ont commencé à envisager publiquement la pertinence potentielle de la concurrence fondée sur la protection de la vie privée dans l'examen des fusions. Par exemple, lors de l'acquisition très médiatisée de Doubleclick par Google en 2007, la Commission fédérale du commerce des États-Unis a examiné, mais a largement écarté, les préoccupations relatives aux effets sur la confidentialité de la mise en commun par les parties à la fusion de leurs ensembles respectifs de données publicitaires.

- **Les organismes antitrust commencent à s'accorder sur le fait que la confidentialité des données peut être considérée comme un élément de la concurrence fondée sur la qualité dans l'examen des fusions.** Il y a maintenant eu une poignée de fusions, principalement dans l'UE et aux États-Unis, où les organismes responsables de la concurrence ont examiné les théories relatives aux effets de la concurrence sur la protection de la vie privée. Ces fusions concernaient les marchés de l'intermédiation publicitaire en ligne, des applications de messagerie grand public et des services de réseaux sociaux professionnels. Même dans les territoires de compétence qui n'ont pas encore examiné de fusion soulevant ce type de question, il existe souvent un soutien théorique à la notion que la confidentialité pourrait être un paramètre de la concurrence sur certains marchés.

- **Cependant, depuis la fusion de Google et de Doubleclick jusqu'à aujourd'hui, les organismes antitrust de l'UE et des États-Unis ont clairement indiqué qu'ils considéraient que les problèmes de protection de la vie privée qui ne sont pas liés à la concurrence ne relèvent pas de leur compétence**.

    - À titre d'exemple, lorsque Facebook a acquis WhatsApp, un service de messagerie en ligne populaire, les défenseurs de la protection de la vie privée des consommateurs ont fait pression pour que les organismes antitrust bloquent la fusion. Ils craignaient qu'après la transaction, Facebook pourrait mettre en commun et utiliser les données des consommateurs de WhatsApp d'une façon qui

violerait les politiques de confidentialité établies par WhatsApp avant la fusion. La Commission européenne a examiné ces arguments, mais a conclu que [toutes les préoccupations liées à la confidentialité découlant de la concentration accrue de données sous le contrôle de Facebook à la suite de l'opération ne relèvent pas des règles de concurrence de l'UE, mais des règles de protection des données de l'UE][4].[Traduction] L'organisme est parvenu à des conclusions similaires en réponse aux problèmes de protection de la vie privée soulevés lors de l'acquisition par Google de FitBit, une entreprise disposant de grandes quantités de données personnelles sur la santé et la condition physique.

- **Parmi les fusions examinées par les organismes antitrust, seule une petite proportion soulève des théories relatives aux effets liés à la confidentialité sur la concurrence. Parmi ces fusions, encore moins d'examens ont abouti à des conclusions selon lesquelles de tels effets liés à la confidentialité sont susceptibles de se produire.** Cela met en évidence une distinction importante entre les fusions ayant des effets liés aux données, que les autorités antitrust examinent régulièrement, et les fusions ayant des effets liés à la confidentialité, qui sont plus récentes et relativement rares. Les données concernées par les fusions ne sont souvent pas de nature personnelle, et les effets concurrentiels sont souvent sans rapport avec la confidentialité. Les intérêts antitrust sont les effets concurrentiels potentiels qui découlent de la fusion, que les données concernées soient de nature personnelle ou non.

    - Toutefois, les autorités européennes de la concurrence ont constaté que la qualité de protection de la vie privée était susceptible de diminuer dans au moins une opération : l'acquisition par Microsoft de LinkedIn, une société de réseaux sociaux professionnels. Les effets sur la concurrence fondée sur la protection de la vie privée étaient susceptibles de se produire en raison de l'éviction des services de réseaux sociaux professionnels concurrents. Les services concurrents offraient aux utilisateurs une meilleure protection de la vie privée que les parties à la fusion et, après la fusion, Microsoft aurait la motivation et la capacité d'exclure ces concurrents du marché. En tant que condition à l'approbation de la fusion, les autorités européennes de la concurrence ont exigé de Microsoft qu'elle accepte un certain nombre de conditions destinées à garantir le maintien de la concurrence dans les services de réseautage social professionnel.

[4] Commission européenne, *Facebook-WhatsApp*, Affaire n° COMP/M.7217 C (2014) 7239, ¶ p. 164 (3 octobre 2014).

- **Les autorités antitrust évaluent souvent les effets des fusions liés aux données qui ne sont pas spécifiques aux données personnelles ou à la confidentialité.** Cela inclut la prise en compte des éléments suivants.

    - L'accumulation ou la mise en commun de données résultant d'une fusion procure-t-elle un avantage concurrentiel, tel que la création de barrières à l'entrée ou à l'expansion des concurrents sur le marché, un pouvoir de marché accru ou un potentiel accru d'inconduite coordonnée de l'entreprise?

    - Les données sont-elles un intrant nécessaire à la concurrence et, dans l'affirmative, les parties à la fusion auraient-elles l'incitation et la capacité de limiter ou de verrouiller l'accès d'un rival à ces données après la fusion?

    - Au moment d'évaluer la probabilité de tels effets liés aux données sur la concurrence, il est souvent important de se demander si les données en question sont uniques et si les parties à la fusion en ont le contrôle exclusif. Lorsque les données peuvent être reproduites à partir d'autres sources, plusieurs décisions d'examen des fusions ont conclu qu'il était peu probable que des effets négatifs sur la concurrence en matière de données se produisent.

- **La poursuite de la coopération entre les organismes antitrust et les organismes de protection de la vie privée sera importante dans le cadre de l'examen de certaines fusions et de l'élaboration de solides théories générales relatives aux effets des fusions sur la confidentialité.** En tant qu'organismes de réglementation disposant de l'expertise la plus approfondie en matière de protection de la vie privée, il est important que les organismes de protection de la vie privée continuent de contribuer à l'élaboration de solides théories sur les effets des fusions. Les récentes fusions démontrent que les organismes de protection de la vie privée peuvent offrir un aperçu précieux dans certains cas spécifiques concernant les effets probables des fusions sur la concurrence fondée sur la protection de la vie privée et dans l'élaboration de recours qui sont positifs pour la protection des données.

- **Bien que relativement peu de fusions aient une incidence sur la concurrence fondée sur la protection de la vie privée, il est possible que de telles fusions deviennent plus courantes à l'avenir, pour plusieurs raisons.** La demande des consommateurs pour des produits et des services assurant la confidentialité augmente, faisant de la confidentialité un paramètre plus important de la concurrence sur certains marchés. Les autorités antitrust continuent de se concentrer sur les transactions et les effets liés aux données dans l'économie numérique. Enfin, certains pays libéralisent leurs lois sur l'examen des

fusions afin de faciliter la contestation des fusions, en particulier dans l'économie numérique. Cette évolution est susceptible d'augmenter le nombre d'examens de fusions mettant en cause des données personnelles et des questions de confidentialité.

C. Abus de position dominante et confidentialité des données

- **Droit antitrust :** La plupart des pays dans le monde interdisent l'abus de position dominante ou la « monopolisation » dans leurs lois sur la concurrence. Ces lois varient d'un pays à l'autre, mais leur objectif principal est d'empêcher les entreprises disposant d'un pouvoir de marché de s'engager dans des types de comportements unilatéraux et anticoncurrentiels.

- **Les relations entre la monopolisation, la concurrence et la confidentialité des données ne sont pas encore bien établies ou comprises de façon concrète.** Bon nombre d'affaires, d'enquêtes et de points de vue politiques commencent à affirmer l'existence d'un lien entre les deux, mais il est trop tôt pour dégager une pensée consensuelle.

    - Lorsque les organismes antitrust font référence au lien entre la monopolisation et la protection de la vie privée, la tendance est de présenter le pouvoir du marché, ou le manque de concurrence, comme une cause probable de la faible qualité des mesures de protection de la vie privée ou des choix pour les consommateurs.

    - Il a également été suggéré, moins souvent, qu'une législation onéreuse en matière de protection de la vie privée pourrait contribuer à l'enracinement des monopoles existants, en rendant plus difficile l'entrée de nouveaux concurrents sur le marché.

    - La recherche effectuée pour produire ce rapport n'a trouvé que peu de preuves empiriques dans les documents des organismes qui soutiendraient l'un ou l'autre point de vue, ou tout autre point de vue potentiel, sur la relation entre la monopolisation, la concurrence et la confidentialité.

- **L'application de la législation antitrust à l'échelle mondiale est axée sur la prévention de l'abus de position dominante dans l'économie numérique.** Les résultats d'un sondage mené par le Réseau international de la concurrence (RIC) en 2020 révèlent que 30 des 39 pays interrogés avaient ouvert des enquêtes sur l'abus de position dominante sur les marchés numériques, et qu'au moins 17 d'entre eux prenaient des

mesures d'application de la loi.[5]

- Les théories d'exclusion des concurrents sont de loin les plus fréquentes. Cependant, on constate également une augmentation récente des théories qui allèguent l'exploitation des consommateurs ou des concurrents, y compris une affaire très médiatisée intentée par l'autorité de la concurrence allemande qui allègue l'exploitation de la confidentialité. Ces deux types d'abus sont examinés dans le présent rapport.

- Les autorités antitrust ont engagé un petit nombre d'affaires préliminaires dans lesquelles il est allégué que la position dominante a été utilisée pour dégrader les protections de la vie privée et les options disponibles pour les utilisateurs de réseaux sociaux et de recherche en ligne.

- Cependant, la plupart des affaires d'exclusion antitrust concernent des effets plus larges, liés aux données, sur la concurrence, plutôt que des théories spécifiques à la confidentialité. Voici quelques-unes des théories d'exclusion liées aux données.

    - L'exclusion des rivaux de l'accès aux données importantes sur le plan concurrentiel, ou des moyens de collecte de données, par l'entremise d'ententes d'exclusivité, ou de services groupés ou liés.

    - L'utilisation des données pour faire passer un monopole d'un marché à un autre.

    - Les données en tant que fonction essentielle, à laquelle les rivaux doivent avoir accès pour concurrencer efficacement.

- **Dans une nouvelle variation des théories antitrust traditionnelles sur l'évincement de la concurrence, plusieurs organismes antitrust ont exprimé leur inquiétude quant à « l'auto-préférence » des plateformes numériques.** Ce terme technique est utilisé pour décrire le comportement d'une plateforme dominante qui utilise son double rôle d'exploitante d'un site où s'exerce la concurrence en ligne pour avantager ses propres offres intégrées verticalement par rapport aux produits ou services de tiers proposés sur le

[5] Réseau international de la concurrence (RIC), *Report on the Results of the ICN Survey on Dominance/Substantial Market Power in Digital Markets* [Rapport sur les résultats de l'enquête du RIC sur la position dominante/le pouvoir de marché important sur les marchés numériques] (Juillet 2020), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/07/UCWG-Report-on-dominance-in-digital-markets.pdf .

même site. Par exemple, le détaillant en ligne Amazon a été accusé d'exclure la concurrence de son marché en ligne, en mettant de l'avant ses propres produits par rapport à ceux des vendeurs tiers qui dépendent de ce marché pour concurrencer les produits d'Amazon.

  - L'autopréférence n'est pas interdite par la plupart des lois sur la concurrence, qui n'imposent pas aux entreprises dominantes une obligation générale d'aider leurs rivaux. Cependant, les organismes antitrust observent qu'un tel comportement pourrait violer les interdictions d'abus de position dominante ou de monopolisation lorsqu'il constitue une forme établie de comportement d'exclusion par une entreprise dominante, avec des effets anticoncurrentiels.

  - Les organismes expriment également des préoccupations générales et comparables en matière de politiques concernant le pouvoir et le contrôle exercés par les grandes plateformes numériques sur la protection de la vie privée et la concurrence dans l'écosystème numérique.

  - Une grande partie de la discussion sur l'autopréférence ne concerne pas spécifiquement la confidentialité. Toutefois, les autorités antitrust du Royaume-Uni se sont demandé si les plateformes avaient l'incitation et le pouvoir de s'engager dans ce que l'on pourrait appeler l'autopréférence « en matière de confidentialité », en surinterprétant les obligations de confidentialité des données imposées aux autres acteurs du marché, tout en permettant aux produits ou aux services des plateformes, intégrés verticalement, de se conformer à des exigences de confidentialité plus laxistes.

- **Les organismes antitrust et les organismes de protection de la vie privée suivent de près la mise en œuvre par Google de son projet de blocage des témoins tiers dans son navigateur Internet Chrome.** Les autorités chargées de la protection de la vie privée examinent de près ce changement, ainsi que la technologie de rechange que Google mettra en œuvre, pour évaluer leur incidence potentielle sur la confidentialité des données. Les procureurs généraux des États américains ont déposé une plainte conjointe dans laquelle ils affirment, entre autres, que le changement de politique de Google constitue un exercice illégal du pouvoir monopolistique qui exclut les éditeurs et les annonceurs concurrents. Les autorités antitrust du Royaume-Uni étudient des théories similaires.

  - L'attention portée par les deux régimes soulève de nouvelles questions quant à savoir si et quand des pratiques susceptibles d'améliorer la protection de la vie

privée pourraient également violer la législation antitrust et, le cas échéant, de quelle façon doit-on aborder ce conflit entre les deux domaines de droit.

- **L'autorité allemande de la concurrence poursuit une affaire d'exploitation abusive qui combine de manière particulière la législation antitrust et la législation sur la confidentialité des données.** L'agence allemande de surveillance de la concurrence allègue que Facebook a utilisé son pouvoir de marché dans les services de réseaux sociaux pour imposer aux utilisateurs des conditions de service qui les obligent à divulguer des données personnelles de façon « excessive », c'est-à-dire au-delà de ce qui aurait été consenti en l'absence de pouvoir de marché. Selon le cas présenté, Facebook aurait violé les lois sur la protection de la vie privée en n'obtenant pas un consentement adéquat pour la collecte et la mise en commun des données des utilisateurs de Facebook i) dans l'ensemble de la famille de services de médias sociaux de l'entreprise Facebook, et ii) avec des renseignements recueillis sur des sites web tiers. L'affaire est unique parce qu'elle fusionne les deux domaines du droit, faisant d'une violation des lois sur la protection de la vie privée un acte anticoncurrentiel dans le cadre de la législation antitrust. L'affaire est en cours et a été portée devant la Cour de justice des Communautés européennes.

    - D'autres juridictions n'ont pas emboîté le pas avec des affaires similaires, mais beaucoup ont suivi avec intérêt l'évolution de ce litige allemand. L'affaire a fait écho à des préoccupations politiques plus larges concernant le déséquilibre de pouvoir entre certaines entreprises numériques et les consommateurs. En particulier, les organismes antitrust et de protection de la vie privée s'intéressent aux entreprises dominantes qui imposent des conditions de service « à prendre ou à laisser », en vertu desquelles les utilisateurs doivent consentir au traitement de leurs données pour pouvoir utiliser le service.

- **Bien que rares et à un stade précoce, les affaires antitrust et les discussions politiques ont également commencé à examiner si les efforts d'une entreprise dominante pour protéger la confidentialité des données des consommateurs pouvaient justifier son comportement anticoncurrentiel.**

    - Il s'agit de l'une des interactions les plus nouvelles à l'horizon entre les deux domaines du droit. Le droit antitrust n'a pas encore déterminé si la protection de la confidentialité des données pouvait constituer une justification pro concurrentielle d'un comportement qui violerait autrement les interdictions d'abus de position dominante.

- Toutefois, le Tribunal de la concurrence du Canada a, dans une certaine mesure, examiné cette question dans l'affaire *La commissaire de la concurrence c. Toronto Real Estate Board*, une affaire d'abus de position dominante de 2016 contre une chambre immobilière dominante.

    - La chambre était accusée par l'autorité responsable de la concurrence du Canada d'exclure illégalement les agents immobiliers en ligne de certaines données d'inscription de maisons. En réponse, la chambre a fait valoir que ses politiques d'exclusion étaient mises en œuvre dans le but de protéger la confidentialité des données des personnes qui mettaient leur maison en vente.

    - Le Tribunal a conclu que les préoccupations relatives à la protection de la vie privée étaient un prétexte, soulevé après coup dans le cadre d'un litige, plutôt qu'une raison principale de la conduite d'exclusion de la commission. Malgré cette conclusion sur les faits, le Tribunal a reconnu, dans un *obiter dictum*, que les considérations relatives à la confidentialité pouvaient justifier des pratiques autrement anticoncurrentielles en droit de la concurrence, si la preuve indique que la protection de la vie privée était la principale motivation de l'entreprise dominante pour sa conduite fautive.

- Les recherches effectuées dans le cadre du présent rapport n'ont pas permis de trouver d'autres affaires d'organismes antitrust qui examinent la question de savoir si la confidentialité des données constitue une justification pour un comportement anticoncurrentiel. Toutefois, des arguments similaires - à savoir que la protection de la vie privée justifie un comportement prétendument anticoncurrentiel - ont été soulevés par de grandes plateformes numériques en leur défense dans le cadre de litiges privés aux États-Unis, en réponse à des plaintes déposées auprès des autorités antitrust de l'UE et en réponse à des enquêtes du Congrès américain concernant la législation antitrust.

- Les organismes ont également soulevé des préoccupations politiques connexes, mais plus larges, quant à la possibilité que les plateformes numériques surinterprètent les obligations en matière de confidentialité en tant que moyen d'exclure les concurrents et de renforcer leur pouvoir de marché.

- **La collaboration entre les autorités antitrust et les autorités responsables de la protection de la vie privée serait précieuse pour évaluer les allégations selon**

lesquelles la confidentialité des données est une justification commerciale. L'expertise des autorités responsables de la protection de la vie privée pourrait contribuer à éclairer l'analyse factuelle visant à déterminer si les intérêts de la confidentialité sont réellement en jeu dans un cas particulier, et à garantir une compréhension précise de la portée des intérêts en matière de confidentialité des données protégées.

- **La pertinence de la confidentialité des données dans les enquêtes et les affaires d'abus de position dominante continuera probablement de s'accroître.** La confidentialité devient un facteur plus important dans la prise de décision des consommateurs sur certains marchés. L'application de la législation antitrust continue de se concentrer sur les marchés numériques où les modèles commerciaux axés sur les données sont prévalents. Nombre de ces modèles commerciaux reposent sur le traitement de données à caractère personnel, ce qui ouvre la voie à des problèmes de confidentialité dans les affaires d'abus de position dominante.

D. Cartels et confidentialité des données

- **Droit antitrust :** La législation relative aux cartels à l'échelle mondiale empêche certains accords entre concurrents visant à fixer les prix, à répartir les marchés ou à restreindre la production.

- **À ce jour, les interactions entre les cartels et la confidentialité des données n'ont fait l'objet que de peu ou pas de discussions de la part des organismes antitrust ou responsables de la confidentialité des données.**

    - Pour les organismes antitrust, le principal intérêt concernant les cartels et l'économie numérique est le potentiel des algorithmes à faciliter la collusion illégale entre concurrents. Ce sujet a été abordé dans des rapports sur la politique antitrust dans de multiples pays. Il est lié à l'intérêt stratégique plus large, partagé avec le droit relatif au respect de la vie privée, de promouvoir la transparence et la confiance dans les marchés numériques, sujet qui est abordé plus haut dans le rapport.

- Puisque l'analyse des cartels est souvent liée au prix, les défis analytiques soulevés par un cartel ayant une incidence sur la qualité de la confidentialité sont susceptibles d'être similaires à ceux discutés ci-dessus pour mesurer et quantifier les effets liés à la confidentialité sur la concurrence.

E. Recours antitrust et confidentialité des données

- **Droit antitrust :** Une fois qu'une violation de la législation antitrust est constatée, les tribunaux et les responsables de l'application de la législation antitrust imposent des recours (ou négocient des accords de règlement) destinés à rétablir ou à maintenir la concurrence. Ces recours pourraient avoir une incidence sur la confidentialité des données d'une façon distincte de la violation de la législation antitrust elle-même.

- **Les discussions sur les recours antitrust sont généralement divisées en recours « comportementaux » et « structurels »,** bien que les deux puissent être imposés dans une même affaire**.** Un recours structurel prévoit le désinvestissement ou la dissolution d'une entreprise en entités distinctes. Un recours comportemental vise à contrôler la conduite d'une entreprise, en empêchant ou en exigeant certaines mesures (ou les deux).

- **Dans l'ensemble, la compréhension de la façon dont la confidentialité des données peut être liée aux recours antitrust n'en est qu'à ses débuts.**

- **Les recours contraignants en matière d'accès aux données ou d'interopérabilité sont les plus susceptibles de porter atteinte à la confidentialité, en particulier lorsque des données personnelles sont en jeu.** Les recours comportementaux antitrust peuvent contraindre les entreprises dominantes ou les entreprises qui fusionnent à fournir à leurs rivaux un accès aux données ou à assurer l'interopérabilité, afin de rétablir ou de maintenir la concurrence.

    - Le sujet de ces recours en matière d'accès aux données ou d'interopérabilité a pris une nouvelle importance dans les discussions sur la politique numérique, où les théories connexes du préjudice se concentrent souvent sur la valeur concurrentielle des données et les effets de l'exclusion des rivaux de l'accès aux données.

    - Les retombées potentielles des recours structurels sur la confidentialité des données, le cas échéant, sont largement inexplorées dans les documents d'organismes.

- **La législation antitrust utilise de tels recours en matière d'accès forcé aux données ou d'interopérabilité avec parcimonie et modération.** La législation antitrust ne prévoit aucune obligation générale de divulguer ou de communiquer des données importantes pour la concurrence, même pour les entreprises dominantes. La crainte est

que, s'il est utilisé trop largement, l'accès forcé aux données ne compromette les incitations des entreprises axées sur les données à fournir des produits et des services novateurs qui profitent aux consommateurs.

- **Bien qu'elles soient relativement rares, un petit nombre d'affaires litigieuses et réglées par les organismes antitrust ont tenu compte de la confidentialité des données dans la détermination des recours imposés.** Ces recours antitrust sont liés à la confidentialité des données des trois façons suivantes.

    - Les recours dans une affaire de cartel aux États-Unis et dans une affaire d'abus de position dominante en France ont obligé les entreprises à divulguer certaines données personnelles détenues sur des personnes, afin de rétablir la concurrence. Ces recours ont été conçus pour inclure un mécanisme de refus de consentement, par lequel les personnes (dont les données seraient autrement soumises à la divulgation corrective) pourraient choisir de ne pas voir leurs données personnelles divulguées dans le cadre du recours, ou dans l'un des cas, de ne pas divulguer certains types de données.

    - Les recours antitrust dans le cadre de fusions et de coentreprises ont renforcé les obligations existantes en matière de respect de la législation sur la confidentialité des données. Par exemple, les autorités européennes responsables de la concurrence ont exigé de Google qu'il offre aux utilisateurs de l'UE la possibilité de choisir d'autoriser ou de refuser l'utilisation de leurs données relatives à la santé et au bien-être, en tant que condition à l'acquisition de Fitbit par la société. Des obligations similaires de respect de la législation sur la confidentialité des données ont été recommandées par l'autorité de la concurrence colombienne dans son examen d'une coentreprise entre les trois plus grandes banques colombiennes.

    - Enfin, les autorités antitrust ont imposé des recours en matière de fusion qui obligent les parties à la fusion à continuer de conserver les données séparément. Les mesures correctives européennes dans l'affaire Google-Fitbit comprenaient également ce type d'obligation de « cloisonnement des données », exigeant que les données sur la santé et la condition physique des utilisateurs de Fitbit soient stockées séparément des données que Google utilise pour la publicité en ligne. Si l'objectif antitrust de ces obligations est de limiter les effets anticoncurrentiels probables du regroupement des données, il pourrait également y avoir des avantages accessoires en matière de confidentialité lorsque ce type de recours empêche le regroupement et le traitement des données personnelles dans les entreprises qui fusionnent.

- **En fin de compte, la discussion sur les recours en matière d'accès aux données doit être spécifique à chaque cas,** en tenant compte des types et des utilisations des données par les parties concernées, ainsi que du marché antitrust particulier examiné.

- **Cette interaction au stade des recours offre une nouvelle possibilité de collaboration productive entre les autorités antitrust et les autorités responsables de la confidentialité des données.** L'expertise des autorités responsables de la confidentialité des données pourrait fournir des renseignements précieux aux autorités antitrust qui cherchent à comprendre si et quand les droits ou les intérêts en matière de confidentialité des données sont susceptibles d'être touchés par les recours antitrust. Les recours employés par les autorités responsables de la confidentialité des données pourraient contribuer à la conception de recours novateurs liés aux données dans la législation antitrust. L'OCDE a spécifiquement appelé à la coopération dans la conception des recours.

- **La pertinence de la confidentialité des données pour les recours antitrust, et la complexité de cette interaction, est susceptible d'augmenter** à mesure que l'application de la législation antitrust continue de se concentrer sur l'économie numérique.

    - À mesure que la législation sur la confidentialité des données évolue vers des formulations de plus en plus robustes du consentement - par exemple, en préférant les modèles d'adhésion aux modèles d'abstention, et un plus grand choix d'options dans les termes du consentement - les autorités antitrust pourraient avoir plus de mal à élaborer des recours efficaces et administrables axés sur le consentement des personnes.

    - Le rétablissement de la concurrence sur certains marchés pourrait nécessiter des recours antitrust qui obligent la société visée à assurer une interopérabilité ou un flux de données permanents, plutôt que les transferts de données ponctuels ou épisodiques qui ont caractérisé les recours antitrust antérieurs. Les recours antitrust qui exigent un accès permanent aux données pourraient soulever des questions plus difficiles sur la façon de tenir compte de la confidentialité des données.

Conclusion

Le moment est venu de perfectionner à la fois la théorie et la pratique à l'intersection du droit antitrust et du droit relatif à la confidentialité des données. Comme l'atteste le présent rapport, une tapisserie complexe d'interactions émerge entre ces domaines du droit. De nouveaux points de recoupement apparaissent rapidement, car la législation antitrust et la législation relative à la confidentialité des données se concentrent toutes deux sur l'économie numérique. Cette confluence d'attention promet une ère d'interaction sans précédent entre la législation antitrust et la législation relative à la confidentialité des données.

Pourtant, ce rapport révèle également que les théories dans cet espace sont souvent nouvelles et que la pratique manque souvent de clarté. Malgré des progrès positifs, la plupart des organismes antitrust et de protection des données commencent à peine à coopérer dans leurs sphères de responsabilité. Ce *statu quo* crée un risque de lacunes, de chevauchements, de tensions et même de conflits inutiles ou involontaires entre les deux domaines d'application. Dans un monde numérique en évolution rapide et dont les enjeux sont importants, de telles inefficacités réglementaires imposent des coûts et sapent les objectifs de bien-être des consommateurs que visent la législation antitrust et la législation relative à la confidentialité des données.

Le défi posé par la réglementation du numérique exige une collaboration entre les organismes. Le dialogue entre les domaines du droit antitrust et du droit relatif à la confidentialité des données est essentiel pour permettre aux organismes d'acquérir une expertise approfondie, de dégager des théories concrètes fondées sur des preuves et d'adopter des stratégies d'application cohérentes. Une collaboration efficace entre les responsables de l'application de la législation antitrust et de la législation relative à la confidentialité des données promet d'apporter des avantages durables aux consommateurs, aux entreprises et aux organismes mêmes. À cette fin, le rapport arrive à sa fin en cernant plusieurs questions de discussion pour lesquelles un dialogue et une collaboration futurs entre les tenants des diverses doctrines seraient particulièrement utiles.

Futurs sujets de discussion entre organismes sur l'intersection de la législation antitrust et de la législation relative à la confidentialité des données

1. **Compromis entre la concurrence et la confidentialité :** Existe-t-il des compromis entre la promotion de la concurrence et la protection de la confidentialité des données dans la législation, l'application de la loi ou les politiques? Si oui, quand et dans quelle mesure ces compromis sont-ils susceptibles de se produire? De quelle façon les organismes de chaque domaine pourraient-ils évaluer et comprendre ces compromis?

2. **Qualité de la confidentialité et concurrence :** Quand la qualité de la protection de la confidentialité au sein d'un marché est-elle susceptible d'être touchée par la concurrence? De quelle façon cette qualité de la protection de la confidentialité est-elle susceptible d'être touchée? Inversement, à quel moment la protection de la confidentialité des données peut-elle avoir une incidence sur la concurrence?

3. **Mesurer les effets de la concurrence sur la confidentialité :** En termes pratiques, comment les autorités antitrust pourraient-elles mesurer les effets pertinents de la concurrence sur la qualité de la confidentialité offerte sur un marché donné?

4. **Abus de position dominante :** Quelle est la relation entre la monopolisation, la concurrence et la confidentialité? De quelle façon le pouvoir de monopole, ou à l'inverse la concurrence, pourrait-il toucher les protections de la vie privée offertes aux consommateurs? Quelles données probantes existent pour étayer et comprendre les opinions sur cette relation?

5. **Justifications commerciales :** Quand, le cas échéant, la protection de la confidentialité des données justifie-t-elle un comportement par ailleurs anticoncurrentiel? De quelle façon les autorités antitrust pourraient-elles évaluer correctement les arguments selon lesquels une fusion ou un comportement répréhensible a été engagé pour protéger la confidentialité des données des personnes?

6. **Fusions :** De quelle façon la qualité de la protection de la vie privée, en ce qui concerne la concurrence, est-elle susceptible d'être touchée par des fusions ou d'autres opérations? Quelles sont les théories acceptées concernant les effets des fusions, et autres transactions d'entreprises, sur la concurrence liée à la confidentialité?

7. **Recours :** En quoi la confidentialité des données est-elle pertinente pour les divers types de recours antitrust? De quelle façon les recours antitrust peuvent-ils être conçus pour

limiter les effets inutiles ou involontaires sur la confidentialité des données, notamment lorsque les recours imposent la divulgation de données à caractère personnel ou des obligations d'interopérabilité aux entreprises qui détiennent des données à caractère personnel?

8. **Évaluation et élaboration des théories et des pratiques :** À mesure que les théories existantes sur la législation antitrust et la confidentialité des données sont mises à l'essai et perfectionnées dans le cadre de l'application de la législation et des litiges, ces théories s'avèrent-elles fondées, basées sur des données probantes et suffisamment larges pour expliquer les diverses interactions entre les deux domaines du droit? Sachant qu'il s'agit d'une intersection naissante du droit, de quelle façon les avancées en matière de confidentialité des données ou de droit antitrust (ou de politiques) pourraient-elles influer sur les interactions entre ces deux domaines?