GROUPE DE TRAVAIL DU CITOYEN ET DU CONSOMMATEUR NUMÉRIQUE DE L'ICDPPC

Rapport fait à la 40ème Conférence sur la collaboration entre les autorités chargées de la protection des données, de la protection des consommateurs et d'autres autorités pour une meilleure protection des citoyens et consommateurs dans l'économie digitale

Sommaire

Introduction

1. La 39ème *Conférence internationale des Commissaires à la protection des données et à la vie privée* ("ICDPPC") a adopté une résolution portant sur la collaboration entre les autorités de protection des données et les autorités de protections des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique.[1]

2. La résolution de l'ICDPPC a établi le *Groupe de travail du citoyen et du consommateur numérique* ("Groupe de travail"). Par cette résolution, le Groupe de travail a été chargé d'identifier des initiatives existantes s'intéressant aux entrecroisements de la protection des consommateurs, de la protection de la vie privée et de la protection des données, de tirer parti desdites initiatives ainsi que de les renforcer. Le Groupe a également été chargé d'explorer la façon dont les autorités peuvent utiliser les cadres légaux pour œuvrer en commun et garantir de meilleurs résultats en matière de protection des données pour les citoyens et les consommateurs.

3. Le Groupe de travail soumet ce rapport, qui explore l'entrecroisement entre protection des consommateurs, protection des données, protection de la vie privée, ainsi que dans d'autres champs connexes. Ce rapport se concentre principalement sur les chevauchements de droits, tant sur le plan matériel que procédural.

4. Ce rapport comporte quatre chapitres principaux : **Chapitre I**, « Pourquoi examiner l'entrecroisement entre protection de la vie privée et protection des consommateurs ? » introduit la notion d'entrecroisement des concepts de protection du consommateur, de protection des données et de concurrence. **Chapitre II,** « Identification et renforcement des initiatives de collaboration (inter)nationale », sont identifiés les forums internationaux qui permettent l'échange d'expériences et de bonnes pratiques entre agences. Ici, des exemples de coopération sont mis en évidence, à niveau national comme international, et des suggestions et mécanismes de coopération (tant à niveau national qu'international) sont proposés. **Chapitre III,** « Défis et chevauchements, du point de vue du droit matériel ».

   Ce chapitre s'intéresse aux chevauchements du point de vue du droit matériel et

[1]ICDPPC, "Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy", 26-27 septembre 2017, Hong Kong, lien.

des idéaux partagés entre domaines réglementaires, comme la loyauté, la transparence et le consentement. **Chapitre IV**, « Recommandations » présente des travaux supplémentaires pouvant être entrepris par le Groupe de travail.

CHAPITRE I

Pourquoi examiner l'entrecroisement entre protection de la vie privée et protection des consommateurs

1. Les activités quotidiennes des individus comportent de plus en plus une caractéristique communément partagée. Elles génèrent les données qui alimentent l'économie numérique. Les modèles économiques poursuivent leur rapide évolution, qui est en partie due aux algorithmes avancés, à l'intelligence artificielle et à l'analyse prédictive, éléments qui rendent possibles pour les entreprises le calcul, l'analyse, la formulation de conclusions, avec de grandes quantités de données, à grande vitesse.

2. Alors même que des quantités plus importantes de données concernant les consommateurs sont collectées (sur de plus longues durées), les habitudes et les schémas répétitifs se font plus évidents pour les entreprises. Dans ce but, les relations avec les consommateurs, dans l'économie numérique, se sont également muées en relations de collecte de données. Avec l'augmentation des capacités en matière de bases de données et d'analyse, même des entreprises relativement modestes sont en mesure d'obtenir des détails précis concernant des individus, qui incluent les achats de ces personnes, leurs comportements, leurs positionnements géographiques et leurs centres d'intérêt, sans se limiter à ces éléments.

3. Les individus sont de plus en plus conscients du rôle que jouent leurs informations personnelles dans l'économie numérique, mais ils ne se rendent toutefois pas nécessairement compte de l'ampleur totale des différentes fins auxquelles ces informations sont utilisées. De ce fait, la façon dont ces informations sont traitées et la question de savoir si ces individus peuvent exercer un contrôle plus affirmé sur les informations les concernant (ainsi que celle de l'ampleur et de la portée des informations amassées par les organisations dans l'environnement numérique) suscitent des inquiétudes.

4. Les problèmes liés à l'utilisation et à la collecte de données dans l'économie numérique constituent un domaine dont l'intérêt est croissant, non seulement pour les autorités chargées de la protection de la vie privée, mais aussi pour celles en charge de la protection des consommateurs. Des pratiques préjudiciables, mensongères ou trompeuses en matière de vie privée peuvent donner lieu à des situations suscitant des préoccupations et peuvent mener à des mesures d'application, tant dans le cadre de la législation en matière de protection de la vie privée que dans celui de la législation relative à la protection du consommateur.

5. Les défis soulevés par la fusion des relations avec les consommateurs avec des relations liées aux données ont suscité des débats quant à la nécessité, pour les autorités chargées d'appliquer la législation en matière de protection de la vie privée et de celle relative à la protection du consommateur, d'explorer les bénéfices d'un cadre régissant la collaboration et la coopération dans l'application de leurs lois. En examinant l'entrecroisement entre ces deux domaines, les organes de réglementation peuvent acquérir une meilleure compréhension des points de divergence et de convergence entre les principes, de la façon dont chaque autorité peut faire avancer les objectifs communs, atténuer les ambigüités réglementaires et développer de bonnes pratiques aboutissant à des résultats positifs, à la fois pour les citoyens et les consommateurs numériques.

6. Compte tenu de l'importance des données personnelles dans l'économie numérique et du degré croissant de mutation des relations avec les consommateurs vers des relations basées sur les données, certains organismes de régulation ont commencé à faire part de leurs interrogations vis-à-vis de l'interaction entre « antitirust », concurrence, protection des consommateurs, protection des données et vie privée. Par exemple, les autorités européennes de protection des données ont récemment fait remarquer que «*L'augmentation du phénomène de concentration dans les marchés numériques peut potentiellement faire peser une menace sur le niveau de protection des données dont bénéficient les consommateurs de services numériques*»[2]. Ces mêmes organes ont considéré comme essentielle l'évaluation des implications à plus long terme des concentrations économiques en matière de protection des données et de droit des consommateurs dans l'économie de marché numérique.[3]. Dans le présent rapport, ces questions d'ordre plus général ne sont pas examinées. L'objet principal d'analyse sera plutôt le chevauchement conceptuel et législatif entre protection des consommateurs et protection des données.

7. Si l'on prend en compte la nécessité d'une meilleure compréhension des entrecroisements entre protection de la vie privée et protection des données (en vue de favoriser une meilleure coopération entre les autorités), dans le présent document sont examinés à la fois les mécanismes formels de coopération, ainsi que les chevauchements conceptuels entre ces domaines de réglementation.

[2] EDPB, "Statement on the data protection impacts of economic concentration", 27 août 2018, lien.
[3] Ibid.

Protection du consommateur et protection des données

8. La protection du consommateur est ancrée dans le besoin de promouvoir la prise de décisions éclairées pour le consommateur, ainsi que dans la nécessité de protéger les consommateurs contre les fraudes, les pratiques déloyales et les produits dangereux qui peuvent être préjudiciables ou dommageables.[4] De tels préjudices sont souvent la conséquence d'un manque d'informations du côté du consommateur. Comme le Guide pour le développement des politiques de consommation de l'OCDE (2010) le souligne, le traitement des dysfonctionnements du marché qui ont pour origine le manque d'informations du consommateur est l'un des objectifs principaux de la législation de protection du consommateur.[5]

9. Comme le rappellent les lignes directrices de l'OCDE régissant la protection de la vie privée (2013), la législation sur la protection de la vie privée et des données introduit également des obligations de transparence vis-à-vis des personnes concernées comme moyen de demander des comptes aux organisations, au sujet de leurs opérations de traitement des données. Dans les lignes directrices est rappelé le caractère éclairant (dans le domaine de la protection de la vie privée) des questions s'intéressant à l'interdépendance entre l'efficacité des choix faits par les consommateurs et le niveau d'information qui leur est fourni.[6].

10. Dans le document intitulé : *Mégadonnées et innovation : les grands thèmes de la politique en matière de concurrence au Canada*[7], les observations que font le Bureau de la concurrence au sujet de l'entrecroisement entre protection du consommateur et celle de la vie privée indiquent un possible chevauchement des mandats dans ce domaine, tant pour le Bureau de la concurrence canadien que pour le Commissariat à la protection de la vie privée du Canada (« OPC ») :

> *Il y a un chevauchement possible des activités liées à l'application de la loi, en vertu de la Loi [sur la concurrence] et à l'application des lois en matière de protection des renseignements personnels. Le Commissariat à la protection de la vie privée du Canada a pour mandat, conformément à la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE), de protéger et de promouvoir la protection de la vie privée dans le cadre de la collecte, de l'utilisation et de la communication de renseignements personnels. Un principe prévoit que la LPRPDE « a pour objet de les empêcher [les organisations] de*

[4] OECD, "Recommendation on consumer policy decision making", 2014, lien.
[5] OECD, "Consumer Policy Kit", 2010, p. 32, lien.
[6] OCDE, "The OECD Privacy Framework", 2013, p. 99, lien.
[7] BUREAU DE LA CONCURRENCE DU CANADA, "Mégadonnées et innovation : les grands thèmes de la politique en matière de concurrence in Canada", 19 février 2018, lien.

> *tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. » De même, la Loi [sur la concurrence] condamne les indications faites au public qui sont fausses ou trompeuses sur un point important.* ***Par conséquent, le mandat du Bureau consistant à garantir la véracité des publicités peut chevaucher le mandat du Commissariat à la protection de la vie privée consistant à protéger le droit à la vie privée. Les deux mandats sont importants pour protéger les consommateurs dans l'économie numérique.*** *»*[8] (caractères gras ajoutés ici)

11. En somme, la protection du consommateur, la protection des données, la protection de la vie privée ont en commun l'objectif de protéger les individus (consommateurs ou personnes concernées) contre les préjudices, la manipulation, les abus. Par le biais de la promotion de l'honnêteté et de la transparence, les cadres régissant la protection du consommateur et la protection de la vie privée peuvent contribuer à donner aux individus un plus grand contrôle.

Explorer l'entrecroisement

12. Parmi trois exemples de chevauchement entre les domaines de la protection du consommateur et la protection de la vie privée, on trouve : *Pratiques commerciales trompeuses et Absence de Consentement*, *Conditions générales*, et *Usages préjudiciables ou inappropriés des informations personnelles* (examinés ci-après). Ces exemples attirent l'attention sur des évènements concrets au cours desquels un chevauchement entre les cadres légaux régissant la protection du consommateur, ainsi que la protection des données, peut se produire.

Pratiques commerciales trompeuses et absence de consentement

13. Le phénomène d'augmentation qui affecte les données personnelles, tant en termes de valeur que de volume, est admis par l'économie digitale et les arnaqueurs et les criminels ont bien remarqué le fait que les données personnelles sont devenues une monnaie d'échange, à tel point que l'augmentation des informations personnelles pouvant être accessibles en ligne a incité les malfaiteurs à trouver des moyens d'exploiter lesdites informations.

14. Les consommateurs connaissent les mêmes préoccupations croissantes vis-à-vis de la façon dont les informations sont utilisées. Leur vie privée est importante pour eux. En bref, vie privée et sécurité sont maintenant devenues des considérations matérielles qui peuvent éclairer les consommateurs et influencer

[8] Ibid.

leur prise de décision en matière d'achats. Pour cette raison, les entreprises commercialisent le concept de vie privée dans leurs produits ou services.

15. Par exemple, dans le cas de l'enquête internationale dont AshleyMadison.com[9] a fait l'objet, l'entreprise commercialisait la vie privée de façon mensongère. AshleyMadison.com, via la publicité, se présentait comme un « service 100 % discret » pour des personnes recherchant des aventures extra-conjugales, et revendiquait ce statut par le biais d'une icône de sécurité « Trustmark » (marque de confiance) ou un « Trusted security award » (prix de sécurité). L'enquête a révélé que la « Trustmark » était fabriquée de toutes pièces et a permis de la faire supprimer. Elle a également dévoilé que l'entreprise proposait un « full delete » (effacement total) mensonger, moyennant des frais supplémentaires. Cependant, les utilisateurs qui choisissaient cette option ne pouvaient pas savoir que les informations contenues dans leurs profils n'étaient pas effacées, mais étaient en fait gardées pendant une période pouvant aller jusqu'à un an, après avoir payé pour un « full delete ».

16. Dans la même veine, une entreprise qui menait ses activités via Internet, trouvant des emprunteurs potentiels pour des organismes de refinancement d'hypothèques, avait réglé un différend avec la « United States Federal Trade Commission » (Commission fédérale de commerce américaine – US FTC) après avoir induit les consommateurs en erreur par des publicités mensongères déclarant qu'elle pouvait assurer gratuitement le refinancement de leurs hypothèques.[10] Les consommateurs qui cliquaient sur ces publicités étaient envoyés vers une page de renvoi, où les consommateurs donnaient volontairement leurs coordonnées, informations qui étaient finalement transmises à des organismes de refinancement hypothécaire.

17. Traditionnellement, le mandat des autorités de protection des consommateurs est de faire appliquer les interdictions de pratiques commerciales trompeuses, telles que les indications fausses ou trompeuses faites au public à des fins commerciales.

Par exemple, les articles 74.01(1) et 52(1) de la Loi canadienne relative à la concurrence *Competition Act* prévoient que nul ne peut contraindre une autre personne à avoir un comportement susceptible d'examen quand une indication

[9] L'enquête a été menée conjointement par les organismes américain et australien de protection de la vie privée le Australian Office of the Information and Privacy Commissioner, US FTC, et par le Commissariat à la protection de la vie privée du Canada.
[10] FTC, "Mortgage Lead Generator Will Pay $500,000 to Settle FTC Charges That It Deceptively Advertised Mortgage Refinancing", 12 septembre 2014, lien.

faite au public est fausse ou trompeuse, sur tout aspect significatif, à des fins promotionnelles ou d'approvisionnement :

> «***Indications fausses ou trompeuses***
>
> ***52 (1)*** *Nul ne peut, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'utilisation d'un produit, soit des intérêts commerciaux quelconques, donner au public, sciemment ou sans se soucier des conséquences, des indications fausses ou trompeuses sur un point important. (disposition pénale)*
>
> ***Pratiques commerciales trompeuses***
>
> ***74.01 (1)*** *Est susceptible d'examen le comportement de quiconque donne au public, de quelque manière que ce soit, aux fins de promouvoir directement ou indirectement soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques, des indications fausses ou trompeuses sur un point important (disposition civile)»* [11].

De même, en vertu de la loi relative à la protection de la vie privée, le consentement ne peut pas être obtenu par tromperie. Pour que le consentement soit éclairé, la législation relative à la protection de la vie privée requiert des organisations qu'elles précisent les fins auxquelles lesdites informations seront utilisées, de sorte que les consommateurs soient raisonnablement à même de comprendre la façon dont leurs informations seront collectées, utilisées ou communiquées. Autrement dit, un individu ne peut pas donner son consentement éclairé vis-à-vis d'un propos mensonger.

18. Par exemple, au Canada, les principes 4.3.5 et 4.4.2 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (PIPEDA) établissent que le consentement relatif à la collecte, l'utilisation ou la communication d'informations personnelles ne doit pas être obtenu par tromperie :

> «***Principe 3 – Consentement***
>
> *4.3.5**.** Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé.* ***Le consentement ne doit pas être obtenu par un subterfuge.*** *[Caractère gras ajouté]*
>
> ***4.4 Principe 4 Limitation de la Collecte***

[11] *Competition Act*, R.S.C., 1985, c. C-34, lien.

> *L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis.* ***Cette obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.*** *[Caractère gras ajouté].»* [12]

19. Compte tenu de ce qui précède, au Canada, la Loi relative à la concurrence *tout comme* la Loi sur la concurrence et la LPRPDE pourraient être en mesure d'être employées dans le traitement de situations où, une organisation, dans le cadre de l'approvisionnement ou de la promotion d'un produit, obtient un consentement pour la collecte, l'utilisation ou la communication d'informations personnelles, mais où ledit consentement a été obtenu par des moyens faux, trompeurs ou mensongers.[13]

Conditions générales

20. Les citoyens numériques et les consommateurs qui souhaitent prendre part à l'économie numérique sont régulièrement confrontés à des conditions générales dont le contenu est présenté comme un exposé détaillé des implications qu'a la collecte de leurs informations personnelles en matière de protection de la vie privée. La protection du consommateur et celle de la vie privée sont susceptibles de s'entrecroiser dans des cas où il est demandé aux consommateurs d'accepter des conditions générales pouvant manquer de transparence, contenir des éléments matériels dissimulés, notamment pour ce qui est de l'utilisation des données, et/ou venir contredire l'impression générale qui se dégage de messages plus dominants.

21. Ce dernier point constitue un principe fondamental de la législation de protection du consommateur – des individus ne doivent pas être induits en erreur par l'impression générale que véhicule le produit. Par exemple, si un produit est présenté comme « respectueux de la vie privée » les conditions générales qui viennent contredire l'impression que ledit produit est « respectueux de la vie privée » peuvent avoir un caractère trompeur. La législation relative à la protection de la vie privée requiert des entreprises qu'elles fassent preuve de transparence en matière de vie privée et qu'elles détaillent les fins auxquelles les informations seront utilisées. Tant dans le cadre de la législation sur la protection des consommateurs que pour celle qui a trait à la protection de la vie privée, les

[12] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, lien.

[13] De plus, la législation anti-spam canadienne (Loi canadienne anti pourriels« LCAP ») est assurée par trois autorités fédérales, parmi lesquelles le Commissariat à la protection de la vie privée du Canada, le Bureau de la concurrence du Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes.

conditions générales ne doivent pas aboutir à une tromperie du consommateur quant à la collecte des informations personnelles le concernant.

22. Pour prendre un exemple concret, la FTC américaine a accusé le créateur d'une application lampe de poche populaire (pour les appareils mobiles Androïd) d'avoir trompé les consommateurs sur les modalités de partage de leurs informations de géolocalisation avec des réseaux publicitaires et d'autres tiers (le développeur de l'application est parvenu à un règlement du différend avec la FTC américaine).[14] Dans ce cas précis, la politique de protection de la vie privée de l'entreprise ne donnait pas d'informations de façon appropriée quant au fait que l'application transmettait des données de l'appareil à des tiers, y compris à des réseaux publicitaires (parmi lesquels des identifiants de géolocalisation et des identifiants permanents de l'appareil). Bien évidemment, il n'y a pas de lien significatif entre d'un côté une fonction lampe de poche et le traitement de données de localisation géographique de l'autre. Sous l'angle de la vie privée : une organisation ne procéderait à la collecte, à l'utilisation et à la communication d'informations *qu'à* des fins *légitimes* et définies, donnerait de façon appropriée des renseignements sur ladite collecte, et l'entreprise pourrait potentiellement être assujettie à des exigences réglementaires plus strictes, dans les cas où des informations précises de géolocalisation seraient en cause.

23. Le Réseau international de contrôle et de protection des consommateurs (RICPC) mène des actions sur la question des conditions générales et a lancé un appel à l'ensemble des entreprises de l'économie digitale, les enjoignant à réexaminer lesdites conditions[15]. À l'issue une action de balayage coordonnée en février 2018, les membres du RICPC participants ont identifié plusieurs sources de préoccupation vis-à-vis des conditions générales, telles qu'une longueur excessive, le fait qu'elles soient trop difficiles à comprendre, le fait qu'elles contiennent des informations dissimulées et leur non-respect des droits statutaires en matière de protection des consommateurs et de protection de la vie privée. La lettre ouverte émise par la présidence du RICPC attire l'attention sur plusieurs bonnes pratiques, dans une volonté d'encourager les entreprises à réexaminer leurs conditions générales.

Usages préjudiciables ou inappropriés des informations personnelles

24. La protection des consommateurs et la protection de la vie privée peuvent également s'entrecroiser, quand des informations personnelles sont publiées en

[14] FTC, "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers", 5 décembre 2013, lien.
[15] ICPEN, "Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers", 29 juin 2018, lien.

ligne pour des motifs inappropriés. Par exemple, des clichés identifiant des individus au cours de leurs arrestations ont été diffusés sur Internet par des entreprises, sans que l'individu photographié n'en ait eu connaissance ou n'y ait consenti.[16] En outre, ces clichés étaient facilement accessibles par le biais de moteurs de recherche populaires. Certains sites Web hébergeant ces informations personnelles mettent en œuvre des opérations d' « effacement moyennant finance » – escroquerie dans le cadre de laquelle un site Web publie, ou facilite la publication d'informations à caractère diffamatoire, provoquant ou embarrassant, de façon à extorquer des personnes, qui sont incitées à payer pour que cette information disparaisse.[17]

25. Un stratagème similaire a été récemment contrecarré aux États-Unis. Quatre individus ont été accusés d'extorsion, de blanchiment d'argent et d'usurpation d'identité pour la gestion présumée du site Web Mugshots.com.[18] . Ces allégations visent notamment l'utilisation d'informations personnelles (noms, photographies d'arrestations par la police, accusations à l'encontre des individus) aux fins de faire payer des « frais de suppression » pour que le contenu soit effacé. Le « State of California Department of Justice » a déclaré :

> « *Ce site Web exploite des données provenant des sites Web des services de police et du shérif pour collecter les noms d'individus, des photos d'arrestation ou des accusations, puis publie à nouveau l'information en ligne, sans que l'individu n'en ait connaissance ou n'y ait consenti. Une fois que ce dernier a formulé sa demande pour que les photos soient enlevées, il est redirigé vers un site web secondaire nommé Unpublisharrest.com et doit payer des « frais de suppression » pour que le contenu soit effacé. Tant qu'une personne n'a pas effectué le paiement, Mugshot.com ne procède pas à l'effacement des informations relatives au casier judiciaire. C'est le cas, même dans l'éventualité où les accusations à l'encontre de l'individu n'ont pas été retenues, dans des cas d'erreur sur la personne, d'erreur d'application de la loi. Les personnes qui ne sont pas en mesure de payer peuvent par la suite se voir refuser un logement, un emploi ou d'autres opportunités, étant donné que la photographie de leur arrestation est facilement disponible sur Internet.* »[19]

26. Dans un autre exemple, dans le cadre d'une enquête menée par le CPC sur globe 24.com (« globe 24 »), les pratiques de l'entreprise consistant à recommuniquer

[16] PEW, "Fight against mugshot sites brings little success", 11 décembre 2017, lien.
[17] Souvent, dans des escroqueries de ce type, la partie « effacement de l'information » de l'arrangement n'est pas respectée, mais au lieu de cela, ceux qui paient sont vus comme des proies faciles pour que l'escroquerie se poursuive.
[18] STATE *OF* CALIFORNIA DEPARTMENT *OF* JUSTICE, "Attorney General Becerra Announces Criminal Charges Against Four Individuals Behind Cyber Exploitation Website", Press release, 16 mai 2018, lien.
[19] Ibid.

les décisions de justice ont été examinées. Par le biais de ces pratiques, ces décisions de justice étaient rendues accessibles en tapant le nom d'un individu dans un moteur de recherche populaire.[20] Par exemple, si un individu se trouvait impliqué dans une procédure de faillite, dans des questions de garde ou dans des questions de relations professionnelles et qu'une personne tapait son nom dans un moteur de recherche, la décision de justice concernant cet individu était consultable sur Globe24 dans les résultats de recherche. Pour qu'un individu puisse obtenir la suppression du lien, Globe24 demandait un paiement de sa part. Le CPC a découvert que Globe24 avait mis en œuvre une fraude « d'effacement moyennant finance », le CPC en a conclu que Globe24 procédait à la collecte, à l'utilisation et à la diffusion d'informations personnelles à des fins inappropriées, et a déposé une requête auprès de la Cour fédérale pour faire exécuter sa décision. La Cour fédérale canadienne a déclaré que les informations personnelles étaient utilisées à des fins inappropriées et a ordonné à l'exploitant du site que toutes les décisions rendues par la Cour, les tribunaux canadiens soient retirés et a également ordonné que soient prises des dispositions pour que lesdites décisions contenant des informations personnelles soient effacées des caches des moteurs de recherche. Des dommages et intérêts d'un montant de 5000 $ ont été versés au plaignant.[21]

27. Un autre exemple d'entrecroisement entre protection de la vie privée et protection du consommateur est illustré par la récente mesure d'application de la réglementation prise par le FTC américain à l'encontre du courtier en données Leaplab.[22] Le FTC américain soupçonnait Leaplab d'avoir acheté des demandes de prêt sur salaire et d'avoir ensuite revendu les informations ainsi découvertes à des négociants. Leaplab savait que ces derniers n'avaient pas un besoin légitime desdites informations. Parmi ces négociants, au moins l'un d'entre eux était présumé avoir utilisé ces informations dans le but de retirer des millions de dollars provenant de comptes de consommateurs, sans l'autorisation de ces derniers. Dans cet exemple, la divulgation non autorisée par le courtier de ces informations, sans besoin légitime, à une personne était une étape cruciale dans la conduite de cette manœuvre frauduleuse.

Protection de la vie privée et concurrence

[20] OPC, "Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA", 5 juin 2015, lien.
[21] FEDERAL COURT (Canada), *AT v. Globe24h.com and Sebastian Radulescu*, 30 janvier 2017, lien.
[22] FTC, "FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts", 23 décembre 2014, lien.

28. Compte tenu du fait que les informations personnelles forment une part grandissante des modèles économiques et des transactions commerciales, les implications des informations personnelles et de la vie privée commencent à faire l'objet d'une analyse de la part des autorités chargées de l'application du droit de la consommation, dans le contexte de leurs cadres d'analyse.

29. Par exemple, les autorités de concurrences française et allemande ont produit un rapport conjoint sur le rôle des données dans les relations économiques, ainsi que sur l'application du droit de la concurrence à de tels échanges. Quelques entrecroisements entre protection des données et droit de la concurrence ont été identifiés :

> *« En effet, même si les règles en matière de protection des données et de concurrence poursuivent des objectifs différents, les politiques de confidentialité des entreprises ne peuvent, par leur seule nature, échapper à un examen au regard du droit de la concurrence. Les décisions prises par une entreprise relativement à la collecte et à l'utilisation des données personnelles peuvent en effet avoir, en parallèle des implications sur la vie privée, des implications économiques et concurrentielles. Par conséquent, les politiques de confidentialité pourraient être envisagées du point de vue du droit de la concurrence dès lors qu'elles sont susceptibles d'affecter la concurrence, notamment lorsqu'elles sont mises en œuvre par une entreprise dominante pour laquelle les données servent d'intrant principal pour ses produits ou ses services. . Un lien étroit entre la dominance de l'entreprise, ses processus de collecte de données et la concurrence qui prévaut sur les marchés concernés peut alors être établi, justifiant ainsi la prise en considération des politiques et des règles de confidentialité dans des procédures de concurrence ».*[23]

30. D'autres autorités de la concurrence reconnaissent le fait que la vie privée peut constituer, en matière de concurrence, un élément autre que le prix. Par exemple le Bureau canadien de la concurrence prend la vie privée comme une « qualité du produit » pouvant constituer, en matière de concurrence, un élément autre que le prix :

> «*« Le Bureau n'a connaissance d'aucune preuve solide permettant d'exclure catégoriquement la confidentialité comme facteur susceptible d'avoir une incidence sur la perception des clients quant à la qualité d'un service qui emploie des mégadonnées et représenterait ainsi une dimension concurrentielle pertinente entre deux entreprises*».[24]

[23] AUTORITE DE LA CONCURRENCE & BUNDESKARTELLAMT, "Competition law and data", 10 mai 2016, 24, lien.
[24] BUREAU DE LA CONCURRENCE DU CANADA, "Mégadonnées et innovation : les grands de la politique en matière de concurrence au Canada", 19 février 2018, 8, lien.

31. De plus, Terrell McSweeny, ancien commissaire à la Commission fédérale du commerce américaine, admet que «*la vie privée du consommateur peut, en matière de concurrence être un élément autre que le prix.*»[25]

32. Plusieurs décisions récemment rendues[26] indiquent l'intérêt que peut avoir l'examen de problèmes liés à la vie privée, examinée sous l'angle de la concurrence, mais dans le même temps, les objectifs de la politique européenne en matière de concurrence peuvent différer de ceux des autorités de protection des données, ce qui est un point délicat. Par exemple, la Cour de justice européenne s'est montrée quelque peu réticente quant à la prise en compte de considérations liées à législation relative à la protection des données, dans le cadre de l'analyse du droit de la concurrence, comme lorsqu'elle déclare : «*Les éventuelles questions relatives à l'aspect sensible des données à caractère personnel ne relevant pas, en tant que telles, du droit de la concurrence, elles peuvent être résolues sur le fondement des dispositions pertinentes en matière de protection de données.*»[27]

33. Bien que certains recours puissent s'avérer utiles dans la résolution de problèmes en matière de concurrence, ces mêmes recours peuvent, dans un même temps, soulever ou créer des problèmes en matière de vie privée et une collaboration entre autorités est requise, en vue d'alléger cette tension. Ce fait trouve son illustration dans la décision de l'autorité de concurrence française d'imposer des mesures intérimaires à GDF Suez, lui ordonnant de permettre à d'autres acteurs du marché d'accéder à des informations concernant les clients, telles que des noms, des adresses, des numéros de téléphone et des profils de consommation.[28] Après consultation auprès de l'autorité française de protection des données, chacun des consommateurs affectés s'est vu offrir la possibilité de se soustraire à ce mécanisme de partage. En l'absence d'opposition sous 30 jours, les données du consommateur devenaient obligatoirement accessibles à d'autres fournisseurs potentiels.

34. La législation portant sur la vie privée peut potentiellement faire intervenir des considérations relatives à la concurrence. Par exemple, une exigence de protection des données pour le consentement quant à certaines utilisations d'informations pourrait, en théorie, donner un avantage concurrentiel des entreprises déjà en relation avec un consommateur, pouvant de ce fait lui donner la possibilité de

[25] T. MCSWEENY, "Competition Law: Keeping pace in a digital age", 15 avril 2016, pg. 8, lien.
[26] Se référer, par exemple, aux décisions mentionnées dans les paragraphes 90 à 94 de ce rapport.
[27] CJEU, *Asnef-Equifax*, C-238/05, para 63.
[28] AUTORITE DE LA CONCURRENCE, Décision n° 14-MC-02 du 9 septembre 2014, lien; I. DE GRAEF, "Data as essential facility", *Phd-thesis at KU Leuven* 2016, 310-315, lien.

communiquer plus facilement en vue d'obtenir ledit consentement (ce qui aboutit, dans les faits, à une augmentation des coûts de transfert, ainsi qu'à une entrave à la concurrence).

35. Comme le démontrent les exemples détaillés ci-dessus, l'entrecroisement de la vie privée et de la protection du consommateur et de la concurrence ne relève plus de l'hypothèse, mais constitue bien un problème d'une actualité immédiate. Ce rapport va maintenant être consacré à l'examen d'approches collaboratives, d'évaluations et d'autres outils, qui seraient à même de permettre aux organismes de réglementation, dans l'ensemble des domaines de réglementation, de mieux identifier, comprendre et répondre aux défis inhérents à la protection des droits des individus, dans l'ensemble des sphères de réglementation.

CHAPITRE 2

Identification et renforcement des initiatives de collaboration (inter)nationales

36. Ce chapitre a pour objet les initiatives et cadres (tant à niveau national qu'international) pouvant faciliter la collaboration entre autorités de la vie privée, de protection du consommateur, ainsi qu'avec d'autres organismes de réglementation. Le rôle crucial des données personnelles dans l'économie numérique a créé des défis à surmonter, du point de vue la surveillance et de la protection, pour l'ensemble de ces organismes. Une coordination adéquate dans le traitement des dossiers, ainsi qu'un dialogue intersectoriel entre lesdits organismes, joue un rôle important dans l'identification des bonnes pratiques, en vue de s'assurer du respect des droits relatifs à la vie privée pour les consommateurs, tout en préservant le potentiel d'innovation de l'économie numérique.

Initiatives de collaboration nationales

37. Selon de récentes statistiques publiées dans un document de l'OCDE portant sur l'application de la législation relative à la protection du consommateur dans le marché mondial, 87 % des membres de l'OCDE disposent d'une forme de cadres légaux, ou d'arrangements d'un autre genre, en vue de coopérer avec d'autres autorités nationales, dans l'application de la législation de protection du consommateur.[29] Certains de ces accords de collaboration interagence portent notamment sur des problèmes de protection des données.

38. Les agences s'intéressent de près à l'identification concrète d'exemples de coopération interagence à un niveau national, ainsi qu'à l'élaboration d'une vue d'ensemble de certains facteurs et points fondamentaux à prendre en compte lors de telles démarches d'identification. Par exemple, dans des cas spécifiques, la vie privée sera abordée comme facteur de qualité, et les données seront abordées comme un facteur concurrentiel dans des questions de droit de la concurrence. Dans de tels cas, les autorités de protection des données relevant d'une même juridiction souhaiteront peut-être formuler des conseils ou des observations sur la façon dont ces questions de vie privée ou de protection des données sont abordées Des chevauchements existent en matière de tromperie (en lien avec le consentement ou l'identification des manières dont ces informations seront

[29] OECD, "Consumer protection enforcement in a global digital marketplace", *OECD Digital Economy Papers* 2018, no. 266, lien.

utilisées), chevauchements qui peuvent justifier d'interventions *ponctuelles*, en présence de tels cas de figure. Les fraudes et escroqueries sont d'autres domaines dans lesquels une collaboration peut se révéler utile – les questions relatives à la vie privée peuvent révéler fraudes et escroqueries et *vice versa*. Des mécanismes visant à collaborer avec les autorités compétentes (de protection du consommateur ou autre) pourraient par conséquent s'avérer bénéfiques dans l'exercice de la protection du citoyen.

39. Les sections ci-dessous mettent en relief deux exemples de collaboration interagence pouvant être dignes d'intérêt pour les autorités désireuses de mettre en place des mécanismes de coopération à niveau international.

Le cas de montres intelligentes – collaboration entre les autorités de protection des données et de protection des consommateurs en Norvège

40. L'Autorité de protection des données (Datatilsynet), l'Autorité de protection des consommateurs et le Conseil de la consommation de Norvège ont fait l'expérience de l'importance d'un travail commun pour le renforcement du droit des consommateurs dans l'économie numérique. Les autorités ont développé une étroite collaboration vis-à-vis des questions de politique et d'application de la législation. Ces organismes de protection des consommateurs et de protection des données ont défini un cadre commun, qui a servi de point de départ, pour évaluer les modalités de résolution de ces problèmes liés aux données des consommateurs et aux modèles économiques basés sur les données, en conformité avec la législation de protection des données et celle relative aux droits des consommateurs.

41. Ces dernières années, le Conseil de la consommation a analysé les conditions générales de produits dits « intelligents », telles que des dispositifs de suivi de la forme physique, des jouets, des applications en lien avec la santé et des montres équipées de GPS. L'analyse de ces organismes démontre que des défis majeurs se présentent vis-à-vis de la sécurité des données, en ce qui concerne les dispositifs de « l'Internet des objets ». En 2017, le Conseil de la consommation a mené une enquête sur la sécurité de plusieurs types de montres GPS commercialisées à l'intention des enfants. L'enquête a révélé que des personnes non autorisées avaient la capacité d'extraire des informations de la montre, et également de lire et de modifier les données de localisation de l'objet. Il était aussi possible de relier la montre à un nouveau compte, sans que le consommateur n'en ait connaissance. Ces défauts constituent plusieurs violations des législations européennes en matière de protection des données et du consommateur.

42. Suite à ces constatations, le Conseil de la consommation a déposé une plainte auprès de l'autorité de protection des données, ainsi qu'auprès de celle chargée de la protection du consommateur, au sujet de trois montres GPS. Ces deux autorités ont traité cette affaire conjointement. Les gestionnaires du dossier provenant des deux autorités ont travaillé ensemble, dans le but de procéder à des évaluations préliminaires du dossier et de préciser la nature des principaux motifs de préoccupation, en conformité avec les cadres légaux des autorités respectives.

43. Au cours de l'évaluation, respectivement des politiques de confidentialité, puis des conditions générales, les autorités ont procédé à la comparaison des exigences en matière de langage clair et compréhensible, en conformité avec les autorités de protection des données et celles de protection des consommateurs. Cela garantissait l'application de critères similaires vis-à-vis des documents et a rendu possible une approche uniformisée.

44. Dans le cas des problèmes de sécurité, les deux autorités ont convenu que l'approche raisonnable consistait en une première évaluation des affaires, sous l'angle de la protection des données, par l'autorité en charge de ces questions, qui prend ensuite des mesures d'application, en conséquence. L'issue des évaluations et le travail d'application de la loi influe sur la manière d'examiner l'affaire, en conformité avec la législation en matière de protection des données.

45. Dès l'abord, les autorités ont identifié trois résultats. Premièrement, en cas de non-respect de la législation relative à la protection des données par les responsables du traitement des données, poursuivre la commercialisation et la vente des dispositifs devient plus difficile, en conformité avec la législation de protection du consommateur. Deuxièmement, si la législation relative à la protection des données s'avère ne pas être capable de couvrir toutes les préoccupations en raison de problèmes d'ordre juridictionnel, la législation relative à la protection du consommateur pourrait être employée pour imposer des obligations d'information aux responsables de traitement des données, pour informer les consommateurs vis-à-vis d'opérations de traitement (surprenantes) et quant aux risques concernant la protection des données. Troisièmement, si les responsables du traitement des données respectaient la législation en matière de vie privée, des exigences additionnelles en matière d'information ne seraient pas imposées aux responsables de traitement des données par la législation de protection du consommateur, dès lors que le traitement de ces données ne revêt pas, pour les consommateurs, un caractère surprenant ou une nature différente

de celle des attentes raisonnables de ces derniers (sur la base des caractéristiques et de la commercialisation du produit).

46. Après examen des dossiers, l'autorité de protections des données a pris la décision d'ordonner aux autres responsables en charge du contrôle de mettre fin à tout traitement de données en lien avec les montres GPS, en raison d'un niveau de sécurité insuffisant dans les opérations de traitement. Suite à cette décision, l'un des trois responsables de traitement des données a décidé de ne pas renouveler ses services. Dans les deux cas de figure restants, l'autorité de protection des consommateurs mène maintenant ses propres évaluations, qui, cependant, ne sont pas en lien direct avec l'entrecroisement de la protection du consommateur et de la protection des données.

Accord de collaboration entre les autorités de protection des données et l'autorité de protection du consommateur aux Pays-Bas.

47. L'autorité néerlandaise protection des données (Autoriteit Persoonsgegevens) et l'autorité de protection du consommateur et de la concurrence des Pays-Bas (Autoriteit Consument en Markt) ont conclu un accord de collaboration en 2016, pour clarifier les procédures à suivre dans l'éventualité d'un chevauchement ou de l'entrecroisement de leurs compétences.[30] L'accord de collaboration prescrit explicitement que la conclusion d'une telle entente a le double avantage d'éviter les accords *ad hoc* pour chaque affaire prise séparément, et également celui de permettre l'établissement d'un cadre de coopération qui est transparent vis-à-vis de l'ensemble des parties prenantes.

48. L'accord de collaboration officialise certains mécanismes, que la réunion annuelle portant sur la poursuite de leurs efforts de coopération, la désignation d'un interlocuteur spécifique au sein de chaque autorité, ainsi que, tous les trois ans, l'évaluation desdits mécanismes. De plus, l'accord prévoit des échanges d'informations et un travail de collaboration, dans l'éventualité où des cas de compétences parallèles se présentent. Les dispositions relatives à l'échange d'informations stipulent que les deux autorités peuvent, et le cas échéant ont l'obligation, de procéder au partage d'informations nécessaires à l'accomplissement de leurs missions légales respectives. Les organismes se tiendront également mutuellement informés, en présence d'une violation relevant exclusivement du domaine de compétence de l'autre autorité. En cas de compétences parallèles, les deux autorités doivent dialoguer afin de déterminer à

[30] ACM & AP, "Samenwerkingsprotocol tussen Autoriteit Consument en Market en Autoriteit Persoonsgegevens", *Staatscourant* 3 novembre 2016, lien.

qui va incomber la gestion de différents aspects de l'affaire. Les autorités ont également la possibilité de faire le choix de créer des équipes conjointes, dans la gestion du dossier. L'accord de collaboration contient également des dispositions relatives à la compétence d'application de dispositions spécifiques, par exemple, pour les cookies et le marketing direct.

49. Les deux autorités ont mis en place une relation de travail à long terme, sur la base de l'accord de collaboration et ont mené par le passé des actions sur plusieurs problèmes liés à la protection de la vie privée des consommateurs. Des problèmes comme la génération de leads, l'inspection en profondeur de paquets, ou la collecte de données personnelles sensibles de consommateurs pendant les périodes d'élections[31].

Initiatives internationales de collaboration

50. En parallèle aux collaborations interagence à un niveau national, l'économie numérique nécessite un cadre homogène de coopération et d'application de la loi. Les sections ci-dessous fournissent un résumé de certaines initiatives visant à améliorer la coopération internationale en matière d'application de la loi, ainsi qu'à encourager un meilleur dialogue entre les différents organismes.

L'initiative « Networks of Networks » du réseau mondial d'application des lois de protection de la vie privée (GPEN)

51. L'initiative « Networks of Networks » (« NoN ») du réseau mondial d'application des lois de protection de la vie privée (« GPEN ») vise à améliorer la coopération internationale en matière d'application de la loi, en encourageant la mise en place d'un meilleur dialogue avec les organismes d'application de la loi œuvrant dans d'autres secteurs. Ce second aspect est particulièrement pertinent vis-à-vis de l'action du groupe de travail. En participant à des échanges avec des autorités de protection du consommateur membres du GPEN NoN, les organismes de protection de la vie privée peuvent découvrir des opportunités de coopération internationale plus adaptées.

52. Le Réseau international d'organismes d'application des lois en matière de communications non sollicitées et de pourriels (UCENET, auparavant nommé « London Action Plan ») et le Réseau international de contrôle et de protection des consommateurs (« RICPC ») participent tous deux à l'initiative GPEN NoN. L'UCENET a été fondé en 2004 dans le but de promouvoir la coopération en

[31] ACM, "ACM and the Dutch DPA take action against Stemwijzer.nl", 8 février 2017, lien.

matière d'application internationale des lois relatives aux pourriels. Depuis sa création, l'UCENET a élargi son mandat pour inclure des menaces supplémentaires en ligne sur mobile, les logiciels malveillants, les spams SMS et les numéros de téléphone à exclure (« Do not call »). L'UCENET compte parmi ses membres des représentants de services gouvernementaux de réglementation et d'application de la loi, ainsi que des industriels qui s'intéressent à ces questions.

53. Le RICPC œuvre pour promouvoir et faciliter l'application de la législation relative à la protection du consommateur, tant par le biais de l'échange d'informations concernant les évolutions du marché et les bonnes pratiques en matière de réglementation, que par la coordination et la coopération dans la résolution de problèmes que rencontre le marché. Ces dernières années, il est de plus en plus évident que, lors de ces échanges, l'accent est mis sur la coopération interagence dans le cadre de projets liés à l'application de la réglementation en matière de protection du consommateur. Le RICPC gère également econsumer.gov, un site Web via lequel les consommateurs du monde entier peuvent signaler des fraudes internationales. Des agences de protection du consommateur de 36 pays participent à econsumer.gov. Le projet comporte deux volets principaux : un site Web publique multilingue, qui permet aux consommateurs de transmettre des plaintes transfrontalières pour fraude, et un site sécurisé econsumer.gov, qui permet aux autorités répressives mondiales de partager et d'accéder à des données relatives aux plaintes provenant des consommateurs (ainsi qu'à d'autres informations relatives aux enquêtes en provenance d'autres juridictions).

54. L'initiative NoN permet essentiellement au GPEN de comprendre les modalités de coopération d'autres secteurs, pour l'amélioration des modèles de collaboration propres aux GPEN. Un avantage supplémentaire réside dans la possibilité de dialogue sur des problèmes communs, pour le développement de la coopération entre les réseaux. Les membres du GPEN ont été invités à prendre part à la conférence de l'ICPEN en tant qu'organisation ayant le statut d'observateur. Ces relations permettent au GPEN d'affiner sa compréhension de l'importance (et de la prévalence croissante) des questions d'application de législation en matière de protection de la vie privée et de protection du consommateur dans le cadre desquelles ces deux législations s'entrecroisent. Plus spécifiquement, la présence du GPEN au RICPC donne l'opportunité aux réseaux respectifs de pouvoir bénéficier de connaissances et expérience pertinentes en matière d'application de la loi. Par exemple, en échangeant sur les bonnes pratiques, en abordant des

questions d'intérêt commun, ainsi qu'en développant des relations bilatérales et multilatérales pour faciliter le développement de la coopération intersectorielle.[32]

L'événement du GPEN à destination des professionnels (« GPEN Practitioners' Event »)

55. En 2017, l'OCDE a émis une recommandation[33] incluant certains éléments susceptibles de faciliter la collaboration entre les organismes de protection de la vie privée et ceux protégeant les consommateurs. Centrée sur les « lois protégeant la vie privée » (c'est-à-dire « le droit ou les réglementations internationaux dont l'application a pour effet de protéger les données personnelles, en conformité avec les lignes directrices de l'OCDE en matière de vie privée »), cette recommandation préconise que les pays « améliorent leurs cadres nationaux d'application de la réglementation relative à la vie privée, pour mieux permettre à leurs autorités de coopérer avec des organismes étrangers ». L'OCDE recommande tout particulièrement que : les autorités de protection des données de protection de la vie privée soient dotées de mécanismes de partage d'informations pertinentes avec des autorités étrangères (compte tenu des possibles violations de leurs lois de protection de la vie privée) en vue d'obtenir : des informations de la part d'individus, des documents ou dossiers, la localisation ou l'identification d'organisations ou d'individus impliqués.

56. Une autre recommandation générale concerne la mise en œuvre d'actions appropriées pour « engager les parties prenantes pertinentes dans des discussions et des activités destinées à renforcer la coopération dans l'application des lois protégeant la vie privée ». Bien que ces éléments puissent aussi concerner des organismes de protection des consommateurs, les exemples spécifiques donnés par la suite incluent : des autorités pénales, des responsables de la protection de la vie privée, des groupes de surveillance du secteur privé, des groupes de la société civile et des groupes commerciaux. L'esprit qui sous-tend la recommandation générale pourrait certainement s'étendre aux autorités de

[32] Dans une lettre ouverte de 2018, destinée aux entreprises de l'économie numérique, des membres du RICPC ont cerné les préoccupations liées aux pratiques pouvant « porter préjudice aux consommateurs et qui peuvent ne pas être en conformité avec les droits nationaux de la consommation. » La lettre contient, dans son estimation desdits préjudices, des éléments faisant référence à la vie privée, tels que le fait d'éviter les conditions générales trop longues, qui peuvent décourager les individus et les amener à se désintéresser d'importantes informations au sujet de leur vie privée et des droits qui s'y rattachent. ICPEN (RICPC), "Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers", 29 juin 2018, lien.

[33] OECD, "Recommendation on cross-border co-operation in the enforcement of laws protecting privacy", 2007, lien.

protection du consommateur. Néanmoins, les exemples spécifiques viennent indirectement appuyer le point de vue selon lequel la recommandation dans son entier, en se référant à des « lois ayant pour effet de protéger les données personnelles » inclut la législation relative à la protection du consommateur.

L'événement du GPEN à destination des professionnels (« GPEN Practitioners' Event »)

En 2018, le GPEN a organisé la seconde édition de son « GPEN Practitioners' Event ». Cette manifestation était l'opportunité pour les membres du GPEN d'engager des débats au niveau du personnel, autrement dit du côté des « professionnels ». Ceux-ci portaient principalement sur les aspects pratiques de la conduite d'enquêtes, de la mise en œuvre de mesures d'application de la loi, ainsi que de sur la période qui suit la mise en œuvre de ces mesures, dans la gestion d'une affaire. L'évènement avait pour but : l'échange d'expériences pratiques, de compétences et stratégies pertinentes, dans le contexte de pratiques en ligne, tant dans les limites des frontières nationales qu'en dehors de celles-ci. L'objectif était également de développer des contacts au niveau opérationnel pouvant servir de socle à des collaborations ultérieures.

57. Cette année, l'évènement était ouvert aux participants à l'initiative NoN du GPEN, y compris à l'UCENET et du RICPC. La présence et la participation active des autorités de protection du consommateur encourage le développement de la collaboration entre autorités de protection de la vie privée du consommateur et facilite le transfert de compétences et d'expérience dans les différentes sphères de réglementation.

La Chambre de compensation numérique (« Digital Clearing House »)

58. La Chambre de compensation numérique a pour but de réunir des organismes de réglementation œuvrant dans différents domaines du droit, comme la protection des consommateurs et l'application de la réglementation en matière du droit de la concurrence, dans l'optique de solutionner des motifs communs de préoccupations et d'entretenir un dialogue ouvert quant aux problèmes soulevés par l'entrecroisement de plusieurs réglementations. La Chambre de compensation numérique fonctionne sur la base de l'idée selon laquelle, alors même que l'économie numérique exerce des pressions sans précédent, une réponse cohérente et « sans cloisonnements » est nécessaire, et ce, de la part de l'ensemble des organismes de réglementation ayant la responsabilité de

l'écosystème numérique. Le réseau a été lancé à l'initiative du CEPD[34]. Le réseau a eu l'appui du Parlement européen[35] et le soutien de la 39e ICDPPC.[36]

59. Les organismes de réglementation se sont rencontrés à deux reprises en 2017, une troisième rencontre s'est tenue en juin 2018. Les questions liées à l'entrecroisement de législations, ainsi qu'à des préoccupations communes ont été explorées, y compris : les disparités entre individus et prestataires de services, les marchés de l'attention et l'opacité des algorithmes qui collectent et utilisent des données personnelles, la prise en compte de la vie privée dès la conception et les failles de sécurité des objets connectés, ainsi que la tarification personnalisée et la collusion sur les prix, les conditions générales de services gratuits en ligne, le micro-ciblage, la manipulation des votants et la loyauté des politiques de confidentialité, ainsi que la pertinence des données personnelles dans l'évaluation des législations en matière de concurrence et de protection du consommateur.

60. Les mécanismes de coopération transfrontaliers ont également fait l'objet de discussions. Par exemple, le soutien des autorités de concurrence dans les fusions–acquisition numériques et les efforts communs entre agences de protection des données et celle des consommateurs, ont fait partie des thèmes abordés.

Mécanismes de collaboration

61. Le reste de ce chapitre fournit une vue d'ensemble des mécanismes de collaboration, tant formels qu'informels, qui peuvent inspirer divers organismes actifs dans l'application de la loi dans l'écosystème numérique, dans l'optique d'un renforcement de la collaboration.

Détachements/ Échange de personnel/Bourses

62. Les détachements, échanges de personnel, bourse dans la coopération et les échanges d'informations entre les agences. Un agent détaché peut assister l'agence d'accueil dans la compréhension des éléments liés à l'organisme d'origine. Inversement, l'agent détaché, à son retour, fait part à l'organisme d'origine de ses observations sur le fonctionnement de l'agence d'accueil. Enfin, le

[34] EDPS, "Opinion 8/2016 on Coherent enforcement of fundamental rights in the age of Big Data", 23 septembre 2016, lien.
[35] PARLEMENT EUROPÉEN, "Resolution on Fundamental rights implication of Big Data", 20 février 2017, lien.
[36] ICDPPC, "Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy", 26 et 27 septembre 2017, Hong Kong, lien.

détachement permet de construire une connaissance de l'autre, au niveau du personnel, des liens et une confiance qui sont souvent des éléments cruciaux pour une collaboration efficace. Les agents détachés peuvent devenir des points de contact essentiels, dans des efforts en communs ultérieurs. Plusieurs initiatives existent pour encourager les détachements :

- La convention de détachement de l'APPA[37] Le Forum des Autorités de protection de la vie privée de l'Asie-Pacifique (APPA) ("APPA") a publié en décembre 2014 une convention de détachement. Ce cadre donne des conseils relatifs à la mise en place d'un détachement réussi, y compris des propositions de modalités d'organisation, une liste chronologique d'éléments à vérifier, ainsi que d'autres ressources destinées à l'agent détaché, au responsable de l'organisme d'origine, ainsi qu'à son homologue de l'organisme d'accueil.

- La liste d'opportunités du GPEN. Le forum du site Web du GPEN héberge un tableau d'opportunités, où les agences peuvent poster des offres de détachement ou d'emploi.

- Détachements de l'EPDB. Les experts nationaux détachés (« END ») sont parfois détachés vers le Secrétariat du Comité européen de protection des données (« EDPB ») pour une durée déterminée, en provenance d'organismes nationaux du secteur public dans des états membres de l'UE. Les END gagnent de l'expérience à un niveau européen et permettent à l'EDPB de pouvoir bénéficier de leurs compétences et expériences professionnelles. Quand une disponibilité s'ouvre, pour un END, l'EDPB contacte les autorités nationales de protection des données, pour les informer d'un appel à candidatures. Ce processus se fait par le biais de l'employeur de membres du personnel de ces autorités. Ce même employeur continue de verser un salaire à son employé pendant la durée du détachement.[38]

63. Le Groupe de travail remarque le potentiel qui réside dans les détachements et les missions entre les autorités de protection des données, de concurrence et de protection des consommateurs, au sein d'une même juridiction. Cela peut constituer un mécanisme utile à l'élargissement des perspectives d'une agence. De plus, les échanges interagence peuvent contribuer à forger une expertise dans plusieurs domaines multidisciplinaires relevant de l'application de la loi, ainsi que

[37] http://www.appaforum.org/resources/secondments/.
[38] https://edpb.europa.eu/about-edpb/career-opportunities_en

dans le développement de réseaux informels de contacts, au niveau du personnel, pour garantir l'efficacité d'une collaboration, quand celle-ci est maintenue.

Les saisines

64. Les saisines entre juridictions peuvent aider une agence dans l'accomplissement de sa mission, en tirant parti du travail déjà accompli par une autre agence. Cela peut se produire dans différentes circonstances, comme dans les cas où l'agence a déjà mené une action, dans la mesure où l'étendue de ses pouvoirs le lui permettent, ou lorsqu'elle rencontre des obstacles, de nature juridictionnelle ou autre, à la poursuite de mesures de mise en application. Concrètement, ces limites ne sont pas souvent fixes, mais sont un problème de ressources. Une question de compétence extraterritoriale peut être soulevée et résolue, mais cela nécessitera des ressources supplémentaires en quantité significative, ce qui réduit l'ampleur des ressources disponibles dans d'autres contextes. Dans de telles situations, les saisines peuvent être des moyens appropriés de tirer parti d'un travail précédemment accompli, pour que l'évolution de l'affaire concernée se poursuive, en cohérence avec la mission de l'agence.

65. Typiquement, les éléments de preuve (ou d'autres informations dans le cadre du travail sur une affaire), sont organisés, partagés, expliqués, si besoin est, à une autre agence. Le personnel de l'agence à l'origine de la saisine reste disponible pour répondre aux questions ou effectuer une identification. La forme que peuvent prendre les échanges dans le cadre d'une saisine peut varier. L'agence à qui est destinée la saisine peut ou non être obligée d'agir dans le cadre de l'affaire en question. . De même, l'agence à l'origine de la saisine peut ou non être en droit d'attendre une réponse, ou un résumé récent de la situation, de la part de l'agence à qui la saisine est destinée.

66. Parmi les exemples de programmes relatifs aux saisines, on compte :

- La cellule de liaison pénale de la FTC américaine. (« CLU »).[39] La FTC américaine dispose d'une unité dédiée à la mise en relation avec les procureurs généraux et à la saisine de ces derniers. Une agence de protection de la vie privée pourrait travailler dans un sens similaire, dans le cadre de saisines entre agences de protection du consommateur. Les affaires de fraude gérées par la FTC peuvent révéler des éléments de preuve, qui viennent informer le dossier des poursuites pénales, tels que des témoignages de victimes, des achats faits dans le cadre d'une infiltration, des documents

[39] http://www.appaforum.org/resources/secondments/

commerciaux et des témoignages internes. L'équipe de la CLU aide les procureurs généraux à comprendre les éléments de preuve, y compris le fonctionnement d'une fraude complexe, et peut aussi renvoyer à des procédures pénales déjà portées devant les tribunaux par la FTC. De ce fait, les procureurs sont plus susceptibles de prononcer des actes d'accusation pénale, étant donné qu'on leur remet un dossier d'affaire plus solide.

- L'alerte du GPEN. Le mécanisme d'alerte du GPEN a lancé un système de saisine simplifiée. Les organismes participants peuvent, en toute confidentialité, faire part de leur intérêt quant à une affaire ou une enquête donnée, dans une recherche d'opportunités de collaboration.

Mécanismes de collaboration à l'échelle régionale (exemple concernant l'UE)

67. En plus de mécanismes internationaux de coopération, il existe des cadres régionaux institutionnalisés de coopération. Les deux mécanismes détaillés ci-dessous impliquent une coopération au sein de l'UE, dans les domaines de la protection du consommateur et de la protection des données. Les mécanismes qu'ils introduisent peuvent également être une source d'inspiration, pour une coopération dans les différents axes des législations relatives à la protection du consommateur, à la protection de la vie privée et à la concurrence, tant à un niveau national qu'international.

- Le Réseau de coopération de l'UE en matière de protection des consommateurs (« Réseau CPC »). Ce réseau permet aux organismes de protection du consommateur d'entreprendre des actions conjointes de mise en application de la loi, dès lors que les violations des règles de protection des consommateurs se produisent dans différentes juridictions de l'espace économique européen.[40] Dans le cadre du réseau CPC, tout organisme au sein d'un pays où les droits du consommateur subissent une atteinte peut demander à son homologue du pays où se situe l'entreprise concernée de prendre des mesures. Le Règlement sur la coopération en matière de protection des consommateurs établit une liste des pouvoirs minimums que chaque organisation doit détenir pour garantir une collaboration. Ces pouvoirs incluent l'obtention d'informations et d'éléments de preuve pour lutter contre les infractions au sein de l'UE, pouvoir mener des inspections sur site, demander de faire cesser ou d'interdire les infractions commises au sein de l'UE, et d'obtenir les engagements et paiements des entreprises au Trésor public. Le CPC donne accès à une plate-forme via laquelle

[40] COMMISSION EUROPÉENNE, "Single Market Scoreboard – Consumer Protection Cooperation Network", Reporting period January – décembre 2017, lien.

les organismes de protection des consommateurs peuvent s'alerter mutuellement vis-à-vis des malversations pouvant s'étendre à d'autres pays. De plus, cette plate-forme leur permet de coordonner leurs approches vis-à-vis de l'application de la législation de protection du consommateur, dans la lutte contre les infractions courantes.

Récemment, un nouveau règlement du CPC a été adopté : le Règlement CPC (UE) 2017/2394. Le nouveau règlement sera applicable à partir du 17 janvier 2020, et vise à améliorer l'actuel cadre du CPC, en renforçant le mécanisme d'assistance mutuelle (en imposant des délais plus courts), en procédant à l'extension des pouvoirs minimums accordés aux autorités nationales de protection du consommateur, ainsi qu'en mettant en place un meilleur mécanisme de coordination, pour les infractions courantes susceptibles de porter atteinte aux intérêts collectifs des consommateurs résidants dans plusieurs États membres de l'UE.

- Le Règlement général de l'UE sur la protection des données (« RGPD ») a introduit une obligation similaire imposée aux autorités de protection des données, quant à l'échange mutuel d'informations pertinentes, ainsi qu'à l'assistance mutuelle pour l'application et la mise en œuvre cohérente du RGPD. L'assistance mutuelle comprend les demandes d'information et les mesures de surveillance, telles que les demandes préalables d'autorisation et de consultation, de contrôles et d'enquêtes. Chaque organisme de protection des données doit répondre à la demande d'une autre autorité de surveillance sans retard excessif, et pas plus tard que dans une période d'un mois après réception de la demande. De telles mesures peuvent comporter, plus spécifiquement, la transmission d'informations pertinentes relatives au déroulement d'une enquête. Les demandes d'assistance doivent inclure l'ensemble des informations nécessaires, y compris l'objectif de la demande, ainsi que les raisons qui en sont à l'origine. Les informations échangées ne seront utilisées qu'aux fins qui ont motivé la demande.

68. Le RGPD ouvre également la voie à un cadre formel pour les opérations conjointes, y compris pour les mesures d'enquête et d'application qui impliquent du personnel de plusieurs organismes de surveillance d'États membres. Si le titulaire ou responsable compte des établissements dans plusieurs États membres, ou dans les cas où un nombre significatif de personnes concernées, dans plus d'un État membre, sont susceptibles d'être fortement affectées par des opérations de traitement de données, un organisme de surveillance de chacun de ces États membres est autorisé à prendre part à des opérations conjointes de ce type.

69. Malgré ces exemples d'initiatives de coopération, tant à l'échelle nationale qu'internationale, le groupe de travail remarque qu'il subsiste un fort potentiel de renforcement de la coopération informelle, ce qui est également vrai pour la promotion d'exemples sains de cadre formel bien établis et qui fonctionnent bien. Le Groupe de travail a suggéré de s'intéresser à la possibilité d'organiser des ateliers, des séminaires, des téléséminaires, dans le traitement des questions de collaboration interagence et de la création d'une présence plus affirmée du Groupe de travail dans des forums internationaux tels que l'ICPD, le GPEN et la Chambre de compensation numérique.

Les cadres formels et informels permettant la diffusion d'alertes pourraient être pertinents pour d'autres autorités et devraient faire l'objet d'une attention toute particulière : l'échange interagence d'informations (confidentielles), les possibilités de mener des actions conjointes de mise en application, ainsi que l'échange de bonnes pratiques et leçons tirées de cas de figure spécifiques.

CHAPITRE 3

Défis et chevauchements du point de vue du droit matériel

70. Comme souligné dans l'ensemble de ce rapport, les législations relatives à la protection des données, à la protection du consommateur et à la concurrence donnent accès à plusieurs recours pour traiter les pratiques commerciales qui exploitent les données à des fins inappropriées. Dans certains cas, ces législations offrent des possibilités de recours qui se recoupent. Dans certains cas de figure, les objectifs sous-jacents que poursuivent ces différents domaines du droit font surgir des tensions, compte tenu du fait que les solutions proposées par l'une de ces législations peuvent entrer en conflit avec d'autres législations.

71. Ce chapitre détaille un choix de principes matériels clés que la protection de la vie privée, la protection des données et celle des consommateurs ont en commun. La législation relative à la concurrence comporte également, jusqu'à un certain point, certains principes de droit matériel en commun, tels que la loyauté et le consentement.

La loyauté

72. La loyauté est un principe communément partagé entre la protection de la vie privée, celle des données et celle du consommateur. Bien que le concept de loyauté connaisse des interprétations variables dans ces différents domaines du droit, les réalités de l'économie numérique actuelle peuvent permettre d'aboutir à des interprétations plus convergentes.

73. Dans la législation de l'UE relative à la protection des données, la notion de loyauté est inscrite à l'article 5.1.a) du GRPD, ainsi libellé :

« Les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (« licéité, loyauté et transparence ») »

74. D'une manière générale, la loyauté est intimement liée au niveau d'information donné aux personnes concernées, pour autant qu'une personne concernée qui, ayant reçu une quantité insuffisante d'informations, ne soit pas en position de prendre de décision autonome vis-à-vis de ses données personnelles.[41] La Raison

[41] W. MAXWELL, "The Notion of 'Fair Processing' in Data Privacy" in *Quelle protection des données personnelles en Europe ?*, CÉLINE CASTETS-RENARD (ed.), Université de Toulouse, 2015, lien.

39 du RGPD confirme cette approche « *Tout traitement de données à caractère personnel devrait être licite et loyal. Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées.* »[42]

75. En vertu de la législation de protection des données de l'UE, il est clair qu'un manque d'information donne lieu à un traitement déloyal. Néanmoins, la nature des pratiques qui entrent dans le champ d'application du principe de loyauté et de son critère. Dans cette optique de clarification, une affaire récente du Tribunal belge de Première instance apparaît comme étant capable d'élargir le critère de loyauté[43].

76. Le procès est basé sur une enquête menée par l'autorité belge de protection des données vis-à-vis de Facebook, qui a révélé que le réseau social collecte des informations concernant chaque utilisateur d'Internet quand ces derniers surfent sur le Web, non seulement sur la plate-forme de Facebook, mais également des informations en provenance de plus de 10 000 sites Web différents. Pour y parvenir, Facebook utilise plusieurs moyens technologiques, tels que les « cookies », les « modules de réseaux sociaux » (par exemple, les boutons « j'aime » ou « partager »), ainsi que des « pixels » (qui sont des images invisibles utilisées pour surveiller les habitudes de navigation en ligne), de sorte que, même si un individu n'a jamais navigué sur le domaine Facebook, ses habitudes de consommation font tout de même l'objet d'une surveillance discrète en arrière-plan par Facebook.

77. Dans cette décision, le Tribunal belge de Première instance a déclaré :

> « *Pour qu'un traitement soit loyal (sic) il faut que les données soient obtenues en toute transparence, qu'elles ne soient pas conservées plus longtemps que nécessaire et que le traitement ultérieur ne soit pas contraire aux prévisions raisonnables de la personne concernée. […] les informations défaillantes entravent non seulement le consentement valable, mais aussi le traitement loyal des données à caractère personnel.* »[44] (soulignement ajouté ici)

[42] Se référer également à la raison 60 du RGPD : « Le principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. »

[43] Cet élément de la décision du Tribunal de première instance belge a été rendu sur la base de l'Article 4, alinéa 1 de la Loi belge relative à la vie privée du 8 décembre 1992, qui transposait l'article 6.1.a) de la Directive européenne 95/46/CE relative à la protection des données, abrogée et remplacée par le RGPD le 25 mai 2018. Bien que la formulation du nouvel article 5.1.a) du RGPD soit légèrement différente, l'essence de cette disposition demeure inchangée.

[44] TRIBUNAL DE PREMIERE INSTANCE DE BRUXELLES, jugement du 16 février 2018, 66, lien.

78. La citation ci-dessus démontre le lien fait par le Tribunal entre consentement éclairé et traitement licite et loyal des données, remarquant qu'un manque d'information constitue un obstacle à l'obtention d'un consentement valable *et* au traitement loyal des données personnelles. Du point de vue du droit matériel, cette décision évoque l'idée de loyauté dans le contexte de la protection des données, ainsi que dans le domaine de la protection du consommateur, en introduisant les attentes raisonnables du consommateur comme l'un des critères d'estimation de la loyauté dans des opérations de traitement.

79. Pareillement, dans un récent engagement proposé à WhatsApp par le Commissariat à l'information du Royaume-Uni («UK ICO») confirme que la loyauté demeure lié à l'exigence du fait de fournir une quantité suffisante d'informations, l'engagement énonçant notamment : «*le consentement présumé n'a pas été loyalement obtenu. Vis-à-vis des utilisateurs existants, le processus ne les informait pas assez clairement du partage dont leurs données personnelles allaient faire l'objet, avec Facebook, à aucune des fins prévues. Le Premier avocat de l'avis n'a pas du tout mentionné Facebook. […]*"[45]

80. Du point de vue de la protection du consommateur, la loyauté constitue un objectif crucial. Au sein de l'UE par exemple, l'instrument le plus important en lien avec la loyauté est la Directive relative aux pratiques commerciales déloyales (DPCD).[46] Plus particulièrement, l'article 5(4) de la DCPD énonce deux catégories spécifiques de pratiques déloyales : les pratiques commerciales trompeuses et les pratiques commerciales agressives[47]. La DCPD définit comme suit ces deux catégories :

« ***Art. 6 – Pratiques trompeuses***

Une pratique commerciale est réputée trompeuse si elle contient des informations fausses, et qu'elle est donc mensongère ou que, d'une manière quelconque, y compris par sa présentation générale, elle induit ou est susceptible d'induire en erreur le consommateur moyen, même si les informations présentées sont factuellement correctes, en ce qui

[45] INFORMATION COMMISSIONER'S OFFICE, Letter to WhatsApp concerning the sharing personal data between WhatsApp Inc. ("WhatsApp") and the Facebook family companies, 16 février 2018, 6, lien.

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

[47] La disposition générale de l'article 5(2) de la DCPD et les deux catégories de pratiques commerciales déloyales, complémentée par une liste noire en annexe de la DCPD. La disposition générale de l'article 5(2) de la DCPD peut être employée en tant que « filet de sécurité » vis-à-vis de pratiques qui ne sont pas couvertes dans la liste noire, ou vis-à-vis de dispositions plus spécifiques relatives aux pratiques agressives et trompeuses.

concerne un ou plusieurs des aspects ci-après et que, dans un cas comme dans l'autre, elle l'amène ou est susceptible de l'amener à prendre une décision commerciale qu'il n'aurait pas prise autrement: […]

Art. 8 – Pratiques commerciales agressives

Une pratique commerciale est réputée agressive si, dans son contexte factuel, compte tenu de toutes ses caractéristiques et des circonstances, elle altère ou est susceptible d'altérer de manière significative, du fait du harcèlement, de la contrainte, y compris le recours à la force physique, ou d'une influence injustifiée, la liberté de choix ou de conduite du consommateur moyen à l'égard d'un produit, et, par conséquent, l'amène ou est susceptible de l'amener à prendre une décision commerciale qu'il n'aurait pas prise autrement. »

81. La question de savoir si un problème en lien avec la vie privée sera nécessairement considéré comme une violation de la législation de protection du consommateur est prise en compte dans les lignes directrices communes de l'Union européenne relatives à la DCPD :

> « *La violation, par un professionnel, de la directive sur la protection des données ou de la directive sur la vie privée et les communications électroniques n'impliquera pas toujours en soi que la pratique elle-même viole également la DPCD. Toutefois, de telles violations de la protection des données devraient être prises en considération dans l'appréciation du caractère déloyal général des pratiques commerciales au regard de la DPCD, notamment lorsque le professionnel traite des données des consommateurs en violation des exigences de protection des données, par exemple à des fins de prospection directe ou à toutes autres fins commerciales telles qu'établissement de profils, prix personnalisés ou applications de mégadonnées.* »[48]

82. De ce fait, le manque de transparence vis-à-vis des données personnelles devrait être pris en compte dans l'évaluation de la loyauté d'une pratique commerciale. Plusieurs affaires récentes illustrent l'entrecroisement entre la DCPD et les principes de protection des données.

83. Par exemple, le 16 juillet 2018, la Cour d'appel de Berlin a déclaré que plusieurs dispositions de la politique de confidentialité de Facebook étaient inégales.[49] La Cour a constaté que Facebook était en violation de la législation allemande de protection des données, ainsi qu'avec celles portant sur les paramètres par défaut

[48] EUROPEAN COMMISSION, "Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices", SWD(2016) 163final, 25 mai 2016, lien.
[49] Voir Communiqué de presse du demandeur ; TRIBUNAL DE PREMIERE INSTANCE DE BERLIN, jugement du 24 janvier 2018, lien.

de confidentialité de Facebook, de même que vis-à-vis de certaines conditions générales de Facebook. La Cour a constaté que les utilisateurs n'avaient pas donné leur consentement concernant certains réglages préalablement cochés, tels que le partage de données de positionnement géographique avec d'autres utilisateurs lors de discussions en ligne, et le fait de pouvoir accéder à la « timeline » (ligne chronologique) d'un utilisateur via un moteur de recherche en ligne. De plus la Cour a constaté que les conditions générales de Facebook étaient invalides, comme elles étaient définies en des termes trop larges, pour inclure « *des déclarations de consentement rédigées sous forme de contrat d'adhésion, qui permettaient à Facebook d'utiliser Facebook pour du contenu commercial sponsorisé, ou des contenus similaires.* »[50]

84. D'un côté, la Cour a utilisé la législation en matière de protection des données pour traiter la question des paramètres par défaut de l'application Facebook, en estimant que l'application ne recueillait pas le consentement éclairé. D'un autre côté, la Cour a annulé plusieurs clauses des conditions générales de Facebook au motif qu'elles contrevenaient à la DCPD. Même si la cour a utilisé la législation de protection du consommateur pour invalider les clauses controversées, l'analyse (du point de vue du droit matériel) du critère de loyauté s'appuyait lourdement sur la législation en matière de protection des données (tout particulièrement sur les dispositions relatives au consentement éclairé.) Cette décision constitue une excellente illustration de l'interaction entre la législation relative à la protection des données et la législation de protection des consommateurs.

85. Plus récemment, en avril 2018, l'autorité italienne d'antitrust et de protection du consommateur (« AGCM ») a démarré une enquête sur Facebook, portant sur des pratiques commerciales déloyales présumées.[51] Cette enquête visait à évaluer la question de savoir si Facebook avait procédé à l'information adéquate et immédiate de ses utilisateurs au cours de l'activation du compte, quant à la collecte de l'utilisation de donnés utilisateurs, et si ce comportement constitue une pratique commerciale déloyale, en infraction du Code italien de la consommation (qui transpose la DCPD dans le droit national italien). Cette affaire peut potentiellement être une bonne illustration de l'interaction entre protection de la vie privée, protection des données, et protection du consommateur, dans le contexte de l'application des cadres de protection du consommateur, pour contrer des pratiques qui entrent typiquement dans le champ d'application de la législation en matière de protection des données.

[50] Ibid.
[51] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, "Misleading information for collection and use of data, investigation launched against Facebook", 6 avril 2018, lien communiqué de presse.

86. Bien que l'application de la loi vis-à-vis de problèmes en lien avec la vie privée et d'une relative nouveauté dans l'Union européenne c'est, pour la FTC américaine, une approche très bien connue, inscrite dans son double mandat.[52] Par exemple, la disposition 5, de la Loi américaine sur la FTC interdit « *des pratiques ou actes commerciaux déloyaux ou mensongers.* ». La déloyauté est définie de manière plus précise dans la législation :

> « *La Commission n'aura aucune autorité que ce soit , en vertu du présent article ou de l'article 57a du présent titre, pour déclarer l'illégalité d'un acte ou d'une pratique, au motif qu'un tel acte ou pratique est illégal, excepté si l'acte ou la pratique cause un préjudice important aux consommateurs, préjudice que lesdits consommateurs ne peuvent eux-mêmes raisonnablement éviter, et qui n'est pas atténué par des avantages compensatoires pour les consommateurs ou la concurrence* »[53]

87. Pour qu'une pratique soit considérée comme déloyale, la FTC américaine doit établir que la pratique cause un préjudice important, que les consommateurs ne peuvent pas raisonnablement éviter, et que ce préjudice n'est pas raisonnablement atténué par des avantages compensatoires. Contrairement à la DCPD, où les pratiques trompeuses sont une sous-catégorie des pratiques déloyale, la FTC américaine a, dans le contexte de l'évaluation du caractère trompeur d'une pratique, une analyse différente. Pour qu'une pratique soit trompeuse, il doit y avoir une représentation, omission ou pratique susceptible d'induire le consommateur en erreur, le consommateur ayant fait preuve d'un comportement raisonnable en la circonstance. La représentation, l'omission ou la pratique doivent être « significatives ».[54]

88. Le Groupe de travail remarque, dans certains cas de figure, qu'il existe une tendance à régler les questions de vie privée en employant la législation relative à la protection du consommateur. Néanmoins, même dans les cas d'application par le biais de la législation de protection du consommateur, la protection des données et les questions de vie privée restent un critère clé dans l'évaluation de fond sur le caractère de loyauté et l'inégalité des conditions générales et d'autres pratiques commerciales, ce qui a pour conséquence un chevauchement étroit de ces deux domaines du droit.

---

[52] W. MAXWELL, "The Notion of 'Fair Processing' in Data Privacy" in *Quelle protection des données personnelles en Europe ?*, CÉLINE CASTETS-RENARD (ed.), Université de Toulouse, 2015, lien.
[53] 15 U.S.C. §45(n)
[54] FTC, "Policy Statement on Deception", 1983, lien.

Le consentement en tant que problème récurrent

89. Comme détaillé ci-dessus, parmi les pratiques d'un contrôleur de gestion ou d'un responsable de données, on peut trouver les conditions générales complexes et trompeuses, à tel point que le consentement du consommateur et des personnes concernées est peu fiable et que leur liberté de choix est amoindrie lors de l'acceptation de clauses de confidentialité. La capacité de faire des choix efficaces est cruciale dans la législation relative à la protection du consommateur, dans la législation de protection des données, ainsi que dans celle relative à la concurrence. Par exemple, le consentement est prépondérant dans les décisions prises par l'autorité italienne d'antitrust et de protection du consommateur. C'est également le cas dans l'évaluation préliminaire de l'autorité allemande de concurrence dans le cadre des poursuites contre Facebook.

90. Le 11 mai 2017, l'AGCM a adopté deux décisions découlant de deux enquêtes menées à l'encontre de WhatsApp vis-à-vis de l'exigence d'acceptation par les utilisateurs de ces conditions générales, ainsi que sur la modification quasi unilatérale de ses conditions générales.[55] La première enquête a révélé que la façon dont WhatsApp a cherché à extorquer leur consentement quant au transfert à Facebook de données relatives aux consommateurs constituait une pratique agressive vis-à-vis du code de la consommation d'Italie (qui applique les dispositions de la DCPD).[56] L'organisme a également déterminé que le fait d'imposer l'acceptation pleine et entière de conditions générales révisées, comme condition d'utilisation de l'application (y compris le partage de données avec Facebook) amenait les utilisateurs à croire que, dans le cas contraire, ils perdraient l'accès à WhatsApp. Cela constituait une pratique commerciale agressive. Compte tenu du fait que la possibilité de décliner le partage des données n'était pas présentée sur la page principale, la pratique commerciale limitait la liberté de choix des utilisateurs, ce qui les conduisait à prendre une décision qu'ils n'auraient peut-être pas prise dans d'autres circonstances.[57]

---

[55] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, Décision du 11 mai 2017, lien communiqué de presse, lien PS10601, lien CV154; N. ZINGALES, "Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law", *Computer law & security review* 2017, Vol(3), 553-558.

[56] L'autorité a remarqué que le comportement en question ne faisait pas, en tant que tel, l'objet d'une interdiction en vertu de législation italienne en matière de protection des données, mais a constaté que ce comportement constituait une violation du droit italien de la consommation. AUTORITA GARANTE DELLA CONCORRENZA E DEL MERCATO, Décision 11 mai 2017, p. 13, lien.

[57] L'utilisateur n'aurait réalisé qu'une alternative se présentait à lui qu'à l'issue d'une étape postérieure, après avoir accepté les conditions générales révisées et en accédant à la politique de confidentialité. De plus, ce choix, dont la nature n'était pas évidente, était défini comme une option de désengagement. En somme, les utilisateurs étaient amenés à donner un consentement d'une portée plus grande que nécessaire, pour continuer à utiliser l'application.

91. De plus, il a été constaté que les pratiques de WhatsApp étaient en infraction vis-à-vis de l'article 8 de la DCPD, qui interdit les pratiques agressives, y compris l'influence injustifiée en tant que pratique commerciale déloyale. Tout particulièrement « l'influence injustifiée » vis-à-vis de ses utilisateurs, amenant ces derniers à donner un consentement plus étendu que nécessaire pour continuer à utiliser le service. De plus, l'AGCM a découvert que le constat d'influence injustifiée se trouvait aggravé, eu égard à la situation de dominance du marché, tant dans le cas de WhatsApp que de Facebook. La pratique a été considérée comme étant en violation vis-à-vis de la diligence professionnelle qu'un utilisateur est en droit d'attendre d'un leader parmi les prestataires de services de communication à destination des consommateurs.[58]

92. Comme énoncé dans le sous-titre « loyauté » ci-dessus, une récente enquête (2018) de l'AGCM concernant Facebook[59] examine l'utilisation de la présélection pour rendre possible les échanges de données personnelles, à la fois en provenance et à destination de tiers, à chaque connexion ou utilisation de sites Web d'application tiers par l'utilisateur, en ne proposant qu'une option de désengagement. Facebook est soupçonné d'exercer une influence injustifiée sur les utilisateurs inscrits, qui, en échange de l'utilisation de Facebook, consentent à la collecte et à l'utilisation de toutes les informations les concernant : informations provenant de leurs profils Facebook personnels, des informations découlant de l'utilisation de Facebook, ainsi que de leurs propres expériences sur des sites et applications tierces.

93. On trouve un raisonnement similaire dans l'évaluation préliminaire de l'Autorité allemande de concurrence (Bundeskartellamt), dans le cadre de son enquête portant sur les conditions générales de Facebook. Selon l'évaluation préliminaire de la Bundeskartellamt, Facebook impose à ses utilisateurs des conditions générales déloyales en vertu du droit allemand, en les poussant à un choix de type « tout ou rien » vis-à-vis de l'expérience Facebook. Après avoir énoncé les raisons pour lesquelles Facebook est considéré comme occupant une position dominante, la Bundeskartellamt a rédigé utilisation abusive en ces termes :

> « *Si une entreprise occupant une position dominante impose à l'utilisateur son accord comme condition d'utilisation de ses services, cela peut relever, pour l'autorité de concurrence, d'un cas de conditions commerciales abusives. […] Un tel abus peut prendre la forme de tarifs excessifs (prix abusifs) ou de conditions commerciales déloyales (conditions commerciales abusives) ».*".

[58] *Ibid.*

[59] L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, "Misleading information for collection and use of data, investigation launched against Facebook", 6 avril 2018, lien communiqué de presse.

La Bundeskartellamt poursuit :

> « *[…] Les principes du droit civil peuvent également être appliqués en vue de déterminer si les conditions commerciales sont abusives ou non. Par principe, tout principe, toute règle de droit visant à protéger un cocontractant en situation de déséquilibre peut être appliqué, aux dites fins de protection. En suivant l'approche de la Cour fédérale de justice [allemande], la (Bundeskartellamt) applique également les principes relatifs à la protection des données dans son évaluation des conditions générales de Facebook.* […] *La législation relative à la protection des données vise à garantir que les utilisateurs puissent décider librement et sans contrainte quant à l'utilisation qui est faite de leurs données personnelles.*»

94. Il faut signaler que le raisonnement de la Bundeskartellamt est ancré dans le droit et la jurisprudence nationaux, point qui permet à l'organisme l'utilisation des dispositions relatives à la protection des données comme preuve du caractère abusif. Une autre disposition inscrite dans le droit national en matière de droit de la concurrence considère l'accès à des données personnelles comme critère de puissance sur le marché. Néanmoins, cette affaire pose bel et bien la question de savoir dans quelle mesure et à quelles conditions une infraction à la législation de la protection des données peut mener à des infractions vis-à-vis du droit de la consommation[60].

95. Ces cas de figure ne sont que quelques exemples de chevauchements en matière d'application de législations relatives à la protection des données à celle de la vie privée et à la protection du consommateur. À mesure que se poursuivra la croissance de l'économie numérique, la fréquence d'incidents de ce type, qui posent des problèmes juridictionnels, augmentera elle aussi, tout comme le besoin du maintien d'une coopération dans l'ensemble des disciplines en matière de réglementation.

[60] See in this respect: G. COLANGELO & M. MARIATERESA, "Data accumulation and the privacy-antitrust interface: Insights from the Facebook case for the EU and the US", *TTLF Working Papers* 2018, n° 31.

CHAPITRE 4

Travaux supplémentaires pouvant être entrepris par le Groupe de travail

96. Eu égard aux considérations qui précèdent, il est clairement nécessaire de continuer à explorer cet important entrecroisement. Dans cet objectif, le groupe de travail a soumis à l'ICDPPC un projet de résolution pour examen et adoption par l'ICDPPC.

97. Le projet de résolution charge au Groupe de travail d'effectuer ce qui suit :

i. S'adresser à davantage d'autorités compétentes dans l'application de mesures de protection de la vie privée, des données et de la concurrence, dans un effort d'analyse et de cartographie des cas d'applications de la loi et des jurisprudences intéressants, qui affectent la vie privée des consommateurs numériques, en vue de fournir des outils supplémentaires pour enrichir la prise de décision, ainsi que l'identification des opportunités de collaboration, à mesure qu'elles se présentent.

ii. Établir une présence forte dans les forums internationaux tels que le RICPC, le GPEN, la Chambre de compensation numérique et le Réseau de coopération en matière de protection des consommateurs, dans l'optique de soutenir le rayonnement du Groupe de travail au sein de ces réseaux. De promouvoir la prise en compte des questions relatives à la protection de la vie privée dans les forums de protection des consommateurs et de faciliter la poursuite de la démarche de sensibilisation interagence et de coopération à niveau international.

iii. Et prendre en compte le développement d'une série d'ateliers ou de webinaires ayant pour thème la coopération interagence, afin d'identifier des cadres et bonnes pratiques concernant la conclusion d'accords interagence, l'échange d'informations et les actions communes d'application de la loi. Cela peut, par exemple se concrétiser dans l'organisation d'un atelier et par l'invitation de réseaux explorant l'entrecroisement (tels les réseaux cités dans la tâche 2), ainsi qu'en tirant parti des travaux d'autres Groupes de travail, tels que le Groupe de travail d'application de la loi (« Enforcement Working Group »), tant dans une optique d'identification des efforts collaboratifs fructueux, que dans l'identification des défis et des opportunités.