MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité

Trésor-Éco

N° 310 • Juillet 2022

Direction générale du Trésor

Protection de la vie privée et concurrence dans le numérique

Mélanie THOINET, Léa DARDELET

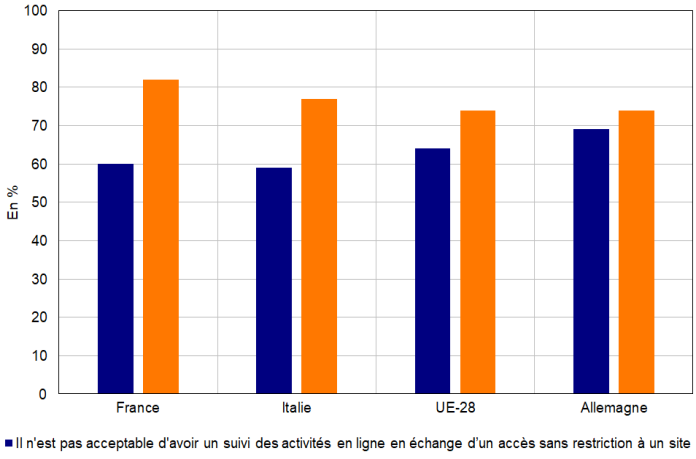
- Dans le domaine numérique, la protection de la vie privée est étroitement liée à la notion de donnée personnelle. Elle peut se définir comme la maîtrise, pour chaque citoyen, des données le concernant dont disposent d'autres acteurs.

- L'économie numérique a fait émerger des effets croisés, complexes et ambivalents entre protection de la vie privée et concurrence, brouillant les frontières entre ces deux politiques, historiquement distinctes. La préservation de la concurrence peut conduire à limiter la collecte des données personnelles par une plateforme ou à autoriser l'accès de concurrents aux données possédées par certains acteurs, ce qui renforce ou dégrade la protection de la vie privée. De manière symétrique, une protection plus stricte de la vie privée peut augmenter la concurrence en limitant l'accumulation de données, source potentielle de position dominante, ou la réduire en créant des coûts de conformité qui pèsent relativement plus sur les petits acteurs.

- Une meilleure articulation des deux types de politique est recherchée par l'Union européenne et par les autorités nationales. Au niveau européen, le *Digital Markets Act* et le *Data Governance Act* abordent ces sujets. Les autorités de concurrence donnent également une importance croissante aux enjeux liés aux données personnelles : plusieurs autorités nationales ont lancé des enquêtes sur les pratiques de plateformes, justifiées par la protection de la vie privée, pour déterminer s'il s'agissait de comportements anticoncurrentiels. Les différents régulateurs coopèrent de plus en plus pour faire face à ces questions.

- Une plus grande sensibilité des consommateurs à la valeur de leurs données réduirait les conflits d'objectifs entre politiques de concurrence et de vie privée. En effet, il existe aujourd'hui un « paradoxe de la vie privée » : bien que soucieux de la protection de leur vie privée sur Internet, les internautes dévoilent gratuitement à des acteurs leurs données, notamment parce qu'ils ne sont pas en mesure d'en connaître la valeur. En 2016, selon une enquête de la Commission européenne, 64 % des Européens interrogés trouvaient inacceptable le suivi de leur activité en ligne en échange de la gratuité d'un site web, mais 74 % d'entre eux n'accepteraient pas non plus de payer pour ne plus être suivis (*cf.* graphique). Ainsi, si les Européens sont majoritairement préoccupés par le suivi de leur activité sur Internet, très peu sont néanmoins disposés à renoncer à la gratuité de leur consultation de site web.

Préférences des Européens sur la protection de la vie privée en ligne



Source : Commission européenne, Flash Eurobarometer 443 - Report e-Privacy, 2016.

1. L'économie numérique modifie la relation entre protection de la vie privée et concurrence[1]

1.1 Protection de la vie privée et concurrence ont été longtemps abordées séparément

Traditionnellement, les politiques de protection de la vie privée et de concurrence ont des appréhensions différentes de la collecte, de l'utilisation et de la protection des données personnelles, c'est-à-dire de « toute information se rapportant à une personne physique identifiée ou identifiable »[2]. Si le droit au respect de la vie privée est inscrit dans le Code Civil[3], la séparation entre les deux types de politiques n'a pas été immédiatement remise en cause par l'émergence du numérique[4].

Le droit de la concurrence a initialement appliqué une grille de lecture « optimiste » à l'économie numérique. Dans cette lecture, l'utilisation massive de données personnelles des utilisateurs par les plateformes, mais aussi la protection de leur vie privée par ces mêmes plateformes, pouvaient améliorer la concurrence sur les marchés : elles seraient en effet un facteur de qualité du service ou produit, par l'intermédiaire duquel des acteurs se concurrenceraient. Par exemple, pour un service de navigation routière, collecter un nombre croissant de données permettrait une amélioration continue des itinéraires par rapport à ses rivaux. Symétriquement, des services se différenciant sur leur niveau de protection de la vie privée permettraient à l'utilisateur de choisir s'il est ou non utile de céder ses données en échange du service, et introduiraient ainsi de la concurrence dans la mesure où la plateforme doit livrer un service de qualité sous peine de voir l'utilisateur changer de fournisseur. Dans ce cadre d'analyse, si une entreprise conditionne le maintien de la gratuité de son produit à l'exploitation d'un volume plus important de données personnelles ou à la vente de ces données à d'autres acteurs, la moindre protection de la vie privée en découlant est assimilable à une augmentation du prix du produit ou une réduction de sa qualité (le respect de la vie privée étant un prix inobservable de l'utilisation des plateformes).

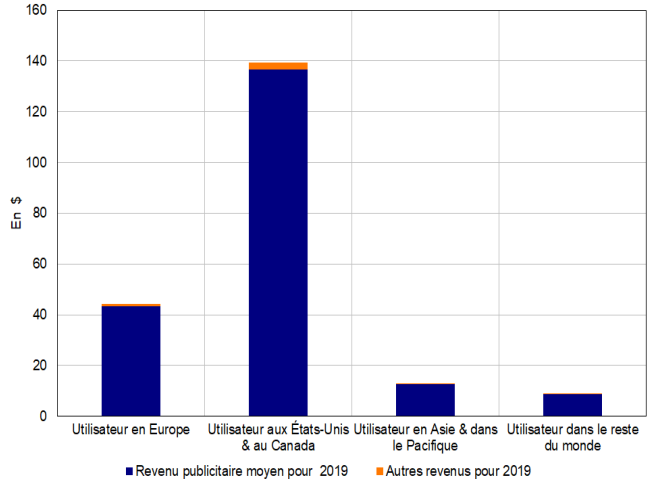
Dans le même temps, la politique de protection de la vie privée a continué d'appréhender avec précaution l'utilisation des données, en insistant particulièrement sur les risques de toute collecte de données, sans prendre en compte ses effets économiques, notamment sur la concurrence[5].

1.2 Le développement des plateformes a rendu visibles des effets croisés ambivalents entre les deux politiques

De nombreux acteurs numériques (e.g. Google, Facebook) fournissent aux utilisateurs des services en apparence gratuits. Leur modèle économique repose sur la collecte et l'exploitation de données fournies par les clients (e.g. informations de profil) ou obtenues indirectement (e.g. « cookies »). Ces données permettent aux plateformes de mieux connaître les préférences des utilisateurs, et ainsi de cibler les publicités à leur intention et donc de se financer en vendant des espaces publicitaires de plus grande valeur. Bien que difficile à estimer, la valeur des données personnelles peut être approchée grâce au « revenu publicitaire par utilisateur ». En 2019 chaque utilisateur mondial a rapporté à Facebook environ 29 $ de revenu publicitaire, 137 $ pour un utilisateur nord-américain, 13 $ pour un utilisateur asiatique et 43 $ pour un utilisateur européen (*cf.* Graphique 1).

(1) Ces questions ont fait l'objet d'un séminaire à la DG Trésor le 14 octobre 2021 (Séminaire Nasse), dont l'enregistrement est disponible en ligne : https://www.tresor.economie.gouv.fr/Evenements/2021/10/14/protection-de-la-vie-privee-et-concurrence
(2) CNIL.
(3) Article 9 du Code civil.
(4) Caffarra C., Crawford G. & Ryan J. (2021), "The antitrust orthodoxy is blind to real data harms", VoxEU ; Liguori L. (2021), "Data Privacy and Competition Protection in Europe: Convergence or Conflict?", CPI.
(5) Depuis sa création, les objectifs de la CNIL ne font pas référence au champ de l'économie.

Graphique 1 : Revenu publicitaire moyen par utilisateur pour Facebook en 2019



Source : Résultats Q4 2019 Facebook.

Le libre choix du consommateur et la protection de la vie privée comme facteurs de différenciation entre plateformes se heurtent cependant à certaines limites. L'internaute n'est souvent pas capable d'apprécier la valeur des données qu'il transmet, en raison de la complexité de leur collecte[6]. L'asymétrie d'information obère alors le choix éclairé de l'internaute et contribue au « paradoxe de la vie privée » : bien que soucieux de la protection de leur vie privée sur Internet, les internautes dévoilent gratuitement leurs données à des acteurs variés. Ainsi, selon la Commission européenne, alors que 64 % des Européens interrogés en 2016 trouvent inacceptable le suivi de leur activité en ligne, la majorité d'entre eux ne trouve pas non plus acceptable de payer pour ne plus le subir (*cf.* Graphique de 1ère page) ; de ce point de vue, une certaine cohérence est visible dans ces préférences : les pays où les consommateurs trouvent le plus acceptable d'être suivis pour ne pas payer (e.g. France et Italie) sont aussi ceux où ils sont le moins prêts à payer pour ne pas être suivis. Faute d'informations fiables sur l'usage des données ou faute d'alternatives aux services proposés par les plateformes, et en raison des effets de réseaux directs[7], il n'est pas non plus facile pour un utilisateur de changer de fournisseur de service, en particulier pour un acteur moins consommateur de données. Enfin, les interfaces biaisées (« dark patterns »[8]) entravent également la protection des données personnelles.

En outre, en raison des caractéristiques des marchés numériques (effets de réseaux directs et indirects[9]), le contrôle de données peut être source de pouvoir de marché et servir à des comportements anticoncurrentiels. Les réseaux les plus attractifs captent la majorité des revenus publicitaires découlant de l'exploitation des données et ils peuvent ainsi optimiser leurs services en investissant et innovant pour conserver cette attractivité ; ils peuvent aussi adopter des stratégies d'acquisition d'autres entreprises leur permettant de collecter un nombre croissant de données. Cela favorise les positions monopolistiques face aux petits acteurs[10], et peut être problématique lorsque cela conduit à des abus de position dominante[11].

Encadré 1 : L'exemple australien de Google

L'Autorité australienne de la Concurrence (ACCC) a estimé dans un rapport d'août 2021[a] que Google avait adopté des comportements anticoncurrentiels pour maintenir sa position dominante, par exemple en restreignant la vente de ses espaces publicitaires sur YouTube à sa propre plateforme d'enchères.

L'ACCC mettait aussi en évidence une tension entre la transmission des données aux opérateurs publicitaires et les contraintes légales de protection de la vie privée. Selon l'ACCC, Google aurait justifié par la protection des données plusieurs mises à jour aux effets potentiellement négatifs pour la concurrence sur le marché de la

a. Digital Advertising Services Inquiry – Final Report.

(6) Furman *et al.* (2019), rapport "Unlocking Digital Competition".
(7) L'attractivité de la plateforme pour un utilisateur est renforcée par la présence d'autres utilisateurs.
(8) Par exemple, un bouton d'acceptation plus visible que celui de refus, des options présélectionnées lors d'achats en ligne ; etc.
(9) L'attractivité de la plateforme dépend, pour l'utilisateur d'une face, des utilisateurs présents sur l'autre face.
(10) L'Autorité de la Concurrence et le Bundeskartellamnt (rapport « Droit de la concurrence et données », 2016) indiquent que lorsque des grandes entreprises ont une base d'informations très large, il paraît difficile à une autre entreprise de reproduire les mêmes volumes et variété de données.
(11) L'analyse de ces situations d'un point de vue concurrentiel peut être plus ardue dans la mesure où l'amélioration par la plateforme de ses revenus peut passer par la fourniture de nouveaux ou meilleurs services.

publicité. Ce serait le cas de son initiative *Privacy Sandbox* : en désactivant les cookies tiers, les informations récoltées ne pourraient plus quitter le navigateur de Google (Chrome), empêchant d'autres entreprises de les récolter directement via Chrome. En plus de contrôler toute la chaîne de valeur, Google serait ainsi le seul fournisseur de données sur les utilisateurs de Chrome. De la même façon, Google a récemment annoncé la mise en place de *Topics*, outil de ciblage par centre d'intérêt sur la base des sites visités par l'utilisateur. Google transmettra seulement trois de ces centres d'intérêt – aléatoirement choisis chaque semaine – aux acteurs qui le demandent pour diffuser leur publicité[b]. Cette *Privacy Sandbox* fait l'objet d'un débat qui reste ouvert entre les différentes autorités nationales de concurrence. Ainsi, en 2021, des enquêtes ont été lancées par la Commission européenne et l'Autorité de la concurrence britannique pour déterminer l'impact de la *Privacy Sandbox* sur la concurrence et un éventuel comportement anticoncurrentiel de Google.

b. PEReN (2022), Éclairage sur Privacy Sandbox.

La politique de concurrence peut donc contribuer[12] à renforcer la protection de la vie privée lorsqu'elle limite la concentration des données personnelles par un nombre restreint de grandes plateformes, lesquelles pourraient en faire une exploitation intrusive et ainsi réduire le bien-être des consommateurs[13]. Le maintien de la concurrence sur les marchés peut parfois promouvoir des innovations permettant une meilleure protection des données personnelles. Mais la politique de la concurrence peut aussi dégrader cette protection lorsqu'elle considère que les plateformes ne doivent pas restreindre l'accès de concurrents aux données, afin que de nouveaux acteurs – eux-mêmes plus ou moins respectueux de la vie privée des personnes – puissent entrer sur les marchés.

Symétriquement, la politique de protection de la vie privée peut contribuer à prévenir la création de positions dominantes, car elle peut soit interdire l'utilisation de certaines données de nature à octroyer un avantage concurrentiel, soit être une manière pour les acteurs de différencier leurs produits (en fonction du degré de respect de la vie privée) et donc de stimuler la concurrence. Mais elle peut également parfois accroître les positions dominantes de certains acteurs lorsque les règles protégeant les données personnelles réduisent la possibilité pour un concurrent d'innover à partir des données qu'il détient, et donc de stimuler la concurrence par une innovation disruptive, ou lorsque ces règles accroissent les coûts d'un concurrent (e.g. pour se conformer aux règles juridiques) de manière prohibitive pour un petit acteur. Cette dualité peut s'observer pour le règlement général sur la protection des données (RGPD) : il aurait à la fois des effets anticoncurrentiels en renforçant la position dominante des grandes plateformes à cause des coûts de conformité assimilables à des barrières à l'entrée pour les concurrents[14], et des effets pro-concurrentiels grâce à l'obligation de portabilité des données, qui réduit les coûts des consommateurs pour changer de fournisseur et leur donne une meilleure maîtrise de leurs données.

1.3 Des réflexions se développent pour une régulation permettant un meilleur équilibre entre concurrence et protection de la vie privée

Sans intervention des pouvoirs publics, le fonctionnement des marchés numériques ne semble pas permettre d'aboutir à un équilibre satisfaisant entre concurrence et protection de la vie privée. Le respect de la vie privée est mis en avant par certains moteurs de recherche en tant qu'avantage comparatif, mais cela ne concerne encore que des exemples limités et ce paramètre non-tarifaire ne paraît pas encore assez attractif pour modifier substantiellement les *business models* fondés sur l'exploitation des données et la publicité. Dès lors, réguler semble nécessaire pour donner un cadre permettant la libre entrée des concurrents sur les marchés numériques sans nuire à l'innovation ni à la protection de la vie privée. La question se pose particulièrement au sein de l'Union européenne, attachée à un modèle économique et social fondé sur les droits individuels et la protection des données personnelles.

(12) Manant M., Rallet A. et F. Rochelandet (2018), "Privacy et antitrust: des régulations contradictoires ou complémentaires ?", *Revue Économique* (Vol. 69).
(13) La combinaison de données personnelles peut permettre à une entreprise monopolistique de cibler les consommateurs et de les discriminer (par exemple à travers les prix, notamment dans des domaines comme la santé, les finances personnelles ou l'emploi. Les situations de monopole rendent ces préjudices plus graves, car les consommateurs n'ont pas d'autre alternative (par exemple, de tels effets ne pourraient pas être tempérés précisément en raison de l'absence de concurrence).
(14) M. Gal et O. Aviv (2020), "The Competitive Effects of the GDPR", *Journal of Competition Law and Economics*.

Des règlements ont été adoptés pour mieux réguler les plateformes numériques. Au niveau européen, le *Digital Markets Act* (DMA), approuvé en mars 2022, vise à préserver la concurrence sur les marchés numériques tout en prenant en compte les enjeux de protection de la vie privée. Par exemple, la combinaison de données personnelles pour la publicité ciblée, considérée comme source d'« *avantages potentiels […], élevant ainsi les barrières à l'entrée* », ne sera autorisée qu'avec le consentement de l'utilisateur. Le *Data Governance Act*, approuvé en novembre 2021, vise à renforcer le partage des données tout en augmentant la confiance dans les intermédiaires de données grâce à un cadre de protection (par exemple, la réutilisation des données personnelles est encadrée). Au Royaume-Uni, la *National Data Strategy* de 2019 a conduit le gouvernement à proposer une réforme du régime de protection des données pour soutenir l'innovation et la concurrence et stimuler la croissance économique tout en protégeant les données.

La définition d'un bon équilibre entre protection de la vie privée et concurrence dépend aussi des préférences des utilisateurs de plateformes. Or ces préférences sont mal identifiées par les utilisateurs eux-mêmes, comme en témoigne le « paradoxe de la vie privée ». Ce constat amène certains à préconiser un système de révélation de ces préférences à travers la monétisation des données : par exemple, au lieu de continuer à prendre la forme de paiements en données personnelles de l'utilisateur en échange de publicités ciblées, comme c'est implicitement le cas aujourd'hui, celle-ci pourrait prendre la forme de paiements monétaires par l'utilisateur pour ne plus recevoir de publicité et compenser la perte en recette publicitaire subie par la plateforme. Selon ses défenseurs, la monétisation amènerait les utilisateurs à prendre conscience de la valeur de leurs données personnelles et à adapter leurs comportements en fonction de leurs attentes en termes de protection de la vie privée. Cela promouvrait aussi la concurrence, puisque les entreprises répondant le mieux à ces attentes gagneraient des parts de marché, tout en limitant les abus possibles de position dominante : les utilisateurs, en choisissant les données qu'ils rendent accessibles à chaque plateforme, pourraient accorder des montants relativement importants aux concurrents des grandes plateformes. L'approche dite « propriétariste », c'est-à-dire où chaque internaute possèderait un « portefeuille de données personnelles » à gérer librement avec les plateformes, reste pour l'instant très prospective et incertaine, et n'est pas sans soulever des difficultés conceptuelles[15]. Elle impliquerait en effet de redéfinir la notion de données personnelles, considérées actuellement comme un droit fondamental en Europe (inaliénables au même titre que le corps d'un individu), ce qui pourrait rendre juridiquement impossible l'instauration d'un tel droit de propriété[16].

2. Les pratiques des autorités de régulation nationales et supranationales évoluent à la lumière de ces réflexions théoriques

2.1 Les différentes autorités de régulation ont d'abord fonctionné indépendamment

Les autorités de protection de la vie privée ont longtemps appréhendé les données personnelles dans le but d'éviter tout risque pour la vie privée (exemple en France de la loi « informatique et libertés » de 1978). Ainsi, en France, la Commission nationale de l'informatique et des libertés (CNIL) considère que l'utilisation des données personnelles doit être restreinte à certains acteurs identifiés.

En revanche, en matière de politique de la concurrence (e.g. contrôle des concentrations), l'utilisation des données personnelles a soit été considérée dans une logique de partage entre acteurs économiques (pour éviter les situations de position dominante qu'entraînerait le contrôle de masses de données par une seule entité), soit n'a pas été considérée du tout. Par exemple, en 2008, lors du rachat de la société DoubleClick par Google, la Commission européenne a uniquement considéré les aspects relatifs au droit de la concurrence et non ceux qui touchaient la protection de la vie privée (i.e. l'impact d'une combinaison des données des deux entreprises)[17]. De même façon, lors de l'acquisition de WhatsApp par Facebook en 2014, elle a séparé les deux enjeux (voir encadré 2).

(15) Génération Libre (2019), rapport « Aux data, citoyens ! ».
(16) Winston Maxwell, Maxime Cordier (2018), « Le tabou de la propriété des données personnelles, éléments de la personnalité et objets de commerce », Edition Multimédi@.
(17) Competition Policy Newsletter 2/2008. Rédigé par des agents ayant traité l'affaire, ce document n'engage pas la Commission.

Encadré 2 : Le rachat de WhatsApp par Facebook, 2014

En 2014, lors l'acquisition de WhatsApp par Facebook, la Commission européenne avait déclaré que les enjeux de protection de la vie privée n'entraient pas dans le cadre du droit de la concurrence[a]. Cette affaire semblait présenter peu d'enjeux relatifs à la protection de la vie privée car WhatsApp scannait des carnets d'adresses mais ne vendait pas les données personnelles récoltées aux annonceurs publicitaires. Facebook avait aussi annoncé qu'il ne serait pas en mesure de faire correspondre automatiquement ses comptes utilisateurs avec ceux de WhatsApp, information dont la Commission avait tenu compte pour autoriser l'opération. Cependant, en 2016, Facebook a modifié la politique de confidentialité de WhatsApp : les données WhatsApp ont été récoltées et utilisées pour des publicités ciblées sur les applications du groupe. En réponse, la Commission a infligé en 2016 une amende de 110 M€ à Facebook pour informations trompeuses et non-respect du fonctionnement indépendant et autonome des services de WhatsApp et Facebook. Une nouvelle amende, de 225 M€ a été infligée en 2021 à Facebook par la CNIL irlandaise au nom de la Commission européenne, pour ne pas avoir suffisamment informé les utilisateurs de WhatsApp sur l'utilisation de leurs données personnelles, comme exigé par le RGPD entré en vigueur en 2016.

a. Voir point 164 de la décision de la Commission d'octobre 2014.

2.2 Les autorités de concurrence s'intéressent désormais davantage aux effets de la protection de la vie privée

La Commission européenne s'intéresse depuis quelques années aux effets croisés des politiques de concurrence et de protection de la vie privée. En 2015, une publication de ses services sur le cas Facebook/ WhatsApp[18] indiquait ainsi que les données peuvent jouer un rôle dans l'évaluation concurrentielle des fusions, en tant que moyen d'obtenir un avantage concurrentiel, et parce que la protection de la vie privée peut être vue comme un paramètre non-tarifaire de concurrence (lorsque des produits sont offerts gratuitement aux utilisateurs car monétisés par des publicités ciblées, alors les données personnelles sont la monnaie payée par l'utilisateur ou une dimension de la « qualité » du produit). De telles considérations ont pu être prises en compte dans certaines décisions ou enquêtes : en 2016 dans la décision sur l'opération de concentration Microsoft/LinkedIn (où la protection de la vie privée a été considérée comme un moteur du choix des consommateurs et un paramètre de la concurrence[19]) et en 2020 et 2021 dans les enquêtes lancées sur les places de marché d'Amazon et Meta (où est envisagée la possibilité que les données créent des barrières à l'entrée et soient utilisées de manière anticoncurrentielle[20]). La Commission s'implique ainsi dans des pratiques liées à des enjeux de protection de la vie privée, dès lors qu'elles sont susceptibles de constituer en elles-mêmes des violations du droit de la concurrence. La mise en garde d'Apple en 2021, par la Commissaire Vestager, à propos des modifications de ses règles (changement de l'iOS14 qui oblige à afficher un pop-up demandant le consentement des utilisateurs pour suivre leurs activités) reflète cette approche : même si Apple disait avoir fait cette modification pour protéger les données personnelles, la Commissaire avait indiqué que cela ne l'exemptait pas des règles de concurrence.

Au niveau national, plusieurs autorités de concurrence se sont saisies de sujets en lien avec la protection de la vie privée. En Allemagne, le *Bundeskartellamt* a ouvert en 2016 une enquête contre Facebook sur la base d'allégations d'abus de pouvoir de marché. Il a cherché à savoir si Facebook abusait de sa position dominante pour enfreindre les règles de protection des données et étendre les conditions d'utilisation définissant le volume de données traitées. En 2019, il a imposé des restrictions au partage de données par Facebook entre ses propres plateformes et des applications tierces, affirmant que cette collecte de données sans le consentement de l'utilisateur et leur partage entre ses services représentaient un abus de position dominante. Suite aux évolutions judiciaires de cette affaire, la CJUE devra se prononcer sur ce dossier, notamment sur la compétence d'une autorité nationale de concurrence concernant le respect du RGPD par l'entreprise visée dans le cadre d'un contrôle des pratiques anticoncurrentielles.

(18) Competition merger brief 1/2015. Rédigé par des agents ayant traité l'affaire, ce document n'engage pas la Commission.
(19) Point 350 et note de bas de page 330 de la décision de la Commission du 6 décembre 2016.
(20) Discours de Margrethe Vestager lors de la conférence de l'European Data Protection Supervisor., "Data Protection and Competition: enforcement synergies and challenges", juin 2022.

En France, en 2020, l'Autorité de la concurrence a été saisie par des acteurs de la publicité en ligne qui contestaient les mêmes modifications de l'iOS14, en estimant qu'Apple abusait de sa position dominante, et risquait de réduire l'efficacité des publicités ciblées. En mars 2021, l'Autorité a considéré que ces modifications n'étaient pas une pratique anticoncurrentielle, qu'elles s'inscrivaient dans les choix d'Apple en matière de protection de la vie privée et de politique commerciale, et qu'elles seraient bénéfiques à la protection des données des utilisateurs. Elle poursuit toutefois l'instruction afin de déterminer si Apple ne favoriserait pas injustement ses propres services. En 2021, l'association France Digitale a aussi déposé plainte contre l'iOS14 auprès de la CNIL, accusant cette fois Apple de ne pas respecter le consentement des utilisateurs car la mise à jour activerait la publicité ciblée par défaut pour les applications Apple.

Enfin, aux États-Unis, la présidente de la Federal Trade Commission a annoncé en septembre 2021 qu'elle voulait faire de la protection des données personnelles une priorité de l'institution en lien avec l'application des lois antitrust, afin d'éviter des préjudices résultant des pratiques de surveillance et de l'absence de législation fédérale sur la vie privée.

2.3 Une plus grande coopération émerge entre autorités et régulateurs nationaux

En France, les coopérations multiples de l'Autorité de la concurrence avec d'autres institutions illustrent la volonté des pouvoirs publics d'appréhender les enjeux de l'économie numérique dans toutes ses dimensions. L'Autorité de la concurrence, l'Autorité des marchés financiers, l'Autorité de régulation des transports, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, la CNIL, la Commission de régulation de l'énergie et le Conseil supérieur de l'audiovisuel ont ainsi publié en 2019 une note commune sur « Les nouvelles modalités de régulation – La régulation par la donnée ». L'affaire Apple en 2020, avec l'utilisation d'un avis de la CNIL par l'Autorité de la Concurrence, est un premier exemple de cette coopération. Plusieurs collaborations se sont développées : en 2020, la DGCCRF et la CNIL ont signé un protocole de coopération pour mieux articuler droit de la consommation et respect du RGPD ; en mai 2021, l'Autorité de la concurrence et le Pôle d'Expertise de la Régulation Numérique (PEReN) ont signé une convention : le PEReN pourra analyser des données et apporter son expertise technique dans des enquêtes relatives aux plateformes numériques. Dans un récent discours[21], le président de l'Autorité de la concurrence a plaidé en faveur d'une « coopération accrue » entre les autorités de la concurrence et les autorités de protection des données personnelles, en raison notamment de l'aspect ambivalent des interactions entre l'analyse concurrentielle et les règles de protection des données personnelles.

Au Royaume-Uni, le régulateur des données (ICO) et l'Autorité de la concurrence (CMA) ont publié au printemps 2021 un protocole d'entente pour formaliser l'approfondissement de leurs interactions. Les deux instances avaient déjà pris en compte leurs objectifs respectifs au sein d'enquêtes (par exemple, l'enquête conjointe en 2021 sur la *Privacy Sandbox*). Désormais chaque autorité pourra ainsi transmettre à l'autre des informations obtenues au cours de ses enquêtes, si elles sont nécessaires à l'atteinte des objectifs de l'autre instance.

Enfin, les autorités nationales de protection des données et de la vie privée des pays du G7 ont déclaré en 2021[22] qu'il était nécessaire de renforcer la collaboration entre ces autorités et leurs homologues de la concurrence à l'échelle nationale en matière de régulation des marchés numériques. En juin 2022[23], la Commissaire Vestager a souligné l'importance de la collaboration entre les décideurs politiques dans les domaines de la concurrence, de la protection des données et de la protection des consommateurs, indiquant que l'architecture institutionnelle prévue par les différents textes européens adoptés ou en négociation devrait permettre de trouver de telles synergies.

(21) Intervention de Benoît Cœuré, président de l'Autorité de la concurrence, devant le collège de la CNIL, « Droit de la concurrence et protection des données personnelles » juin 2022.
(22) « Libre circulation des données dans la confiance » – Table ronde des autorités de protection des données et de la vie privée du G7 (CNIL.fr)
(23) Discours de Margrethe Vestager lors de la conférence de l'European Data Protection Supervisor,"Data Protection and Competition: enforcement synergies and challenges", juin 2022.

Éditeur :

Ministère de l'Économie,
des Finances
et de la Souveraineté
Industrielle et Numérique
Direction générale du Trésor
139, rue de Bercy
75575 Paris CEDEX 12

Directeur de la Publication :
Agnès Bénassy-Quéré

Rédacteur en chef :
Jean-Luc Schneider
(01 44 87 18 51)
tresor-eco@dgtresor.gouv.fr

Mise en page :
Maryse Dos Santos
ISSN 1777-8050
eISSN 2417-9620

Derniers numéros parus

Juin 2022

N° 309 Enjeu et risques des crypto-actifs
Grégoire De Warren

N° 308 L'Union européenne au défi du découplage des chaînes de valeur sino-américaines
Raphaël Beaujeu, Olivier Besson, Laure Decazes, Aymeric Lachaux

Mai 2022

N° 307 La balance des revenus en France et dans la zone euro
Alban Aubert

https://www.tresor.economie.gouv.fr/Articles/tags/Tresor-Eco

Direction générale du Trésor

@DGTresor

Pour s'abonner à *Trésor-Éco* : bit.ly/Trésor-Eco