Conclusions

de la mission de réflexion portant sur l'articulation entre protection des données et concurrence

confiée par Marie-Laure Denis, Présidente de la CNIL

à Bruno Lasserre, Président de la CADA et membre du collège de la CNIL

avec le concours de

la Mission d'analyse économique de la CNIL

28 novembre 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

1. Introduction générale

Cinq ans après la première tentative du Bundeskartellamt d'articuler concurrence et protection des données, trois ans après le *Joint statement* des deux autorités britanniques, plus d'un an après l'arrêt *Meta platform c/ Bundeskartellamt* de la CJUE de juillet 2023 qui crée un régime de coopération entre autorités, l'objectif d'articuler « protection des données » et « concurrence » est devenu une évidence. Evidence pour le politique, qui souhaite considérer la régulation du numérique notamment, comme un tout. Evidence pour les autorités, qui approfondissent leur coopération par tous les moyens. Evidence pour les entreprises, enfin, qui appellent une telle cohérence de leurs vœux. De plus en plus rares sont ceux qui, parmi les institutions ou les chercheurs, défendent une parfaite indépendance des deux régulations.

En effet, la réalité économique des marchés du numérique et des acteurs dominants qui y sont actifs accroît les situations d'interdépendance entre les deux régulations. Ainsi, dans ces situations, ce qui se passe dans l'un des cadres a des effets sur l'autre et réciproquement[1]. Les deux cadres juridiques sont souvent décrits comme ayant des objectifs distincts, ce qui est exact, mais ont aussi des objectifs communs, parmi lesquels la protection du bien-être individuel, de la liberté de choix des personnes, la loyauté, la transparence qui rend l'information plus symétrique ainsi que la réduction des asymétries de pouvoir (Majcher, 2023).

Il convient, pour autant, de bien définir ce que l'on entend par une meilleure articulation des deux cadres. En la matière, un certain nombre de questions se posent : le lien entre les deux domaines doit-il être à sens unique, ou est-il réciproque, c'est-à-dire que la protection des données peut-elle et doit-elle intégrer des éléments d'analyse concurrentielle ? La question de l'articulation ne doit-elle se poser qu'en cas de conflit de normes, ou doit-elle reposer sur une vision plus intégrée ou un dialogue des deux cadres de régulation, de leurs concepts et de leurs outils ? L'articulation ne doit-elle concerner que la protection des données et la concurrence, ou doit-elle s'étendre à la protection du consommateur qui est le domaine où l'intersection avec les deux autres est la plus patente, ou même encore à la régulation des communications électroniques et des médias et demain de l'IA ?

Si la première interrogation est désormais réglée par la jurisprudence *Meta platforms c/ Bundeskartellamt*, c'est la question de l'articulation qui fait l'objet du présent rapport. Elle repose sur une approche équilibrée de la question : se gardant tant de la fiction d'une parfaite indépendance des régulations, que de l'illusion d'une intégration des deux cadres en l'état actuel du droit positif, le présent rapport propose une approche équilibrée fondée sur la convergence des régulations et le dialogue des concepts et des outils (cf. Figure 1).

Ces notions sont déjà exposées et développées dans la récente Déclaration conjointe « *Concurrence et données personnelles : une ambition commune* » entre l'Autorité de la concurrence et la CNIL, publiée le 12 décembre 2023. Le présent rapport vise à approfondir la convergence entre les deux cadres de régulation, en se plaçant dans la perspective de la protection des données, qui est la perspective la moins développée actuellement. Il fait 15 propositions pour approfondir convergence dialogue et coopération. Ce faisant, il ne s'interdit pas de formuler des pistes de réflexion à destination de l'Autorité de la concurrence.

Les objectifs de la démarche sont les mêmes que ceux de la Déclaration conjointe : réduire les tensions ; mettre en avant les synergies de régulation qui la rendent plus efficace et plus prévisible ; illustrer la conviction qu'il existe plus de synergies que de tensions, faire dialoguer les concepts et les outils, au besoin en les adaptant, pour permettre leur prise en compte à titre d'inspiration mutuelle dans l'appréciation des pratiques mais aussi dans l'analyse juridique ; rendre plus fluide et rapide la coopération entre les deux autorités sur les concepts, la doctrine et les cas ; renforcer la sécurité juridique pour les entreprises ; enfin agir au bénéfice de tous les citoyens, consommateurs, personnes concernées par la protection de leurs droits.

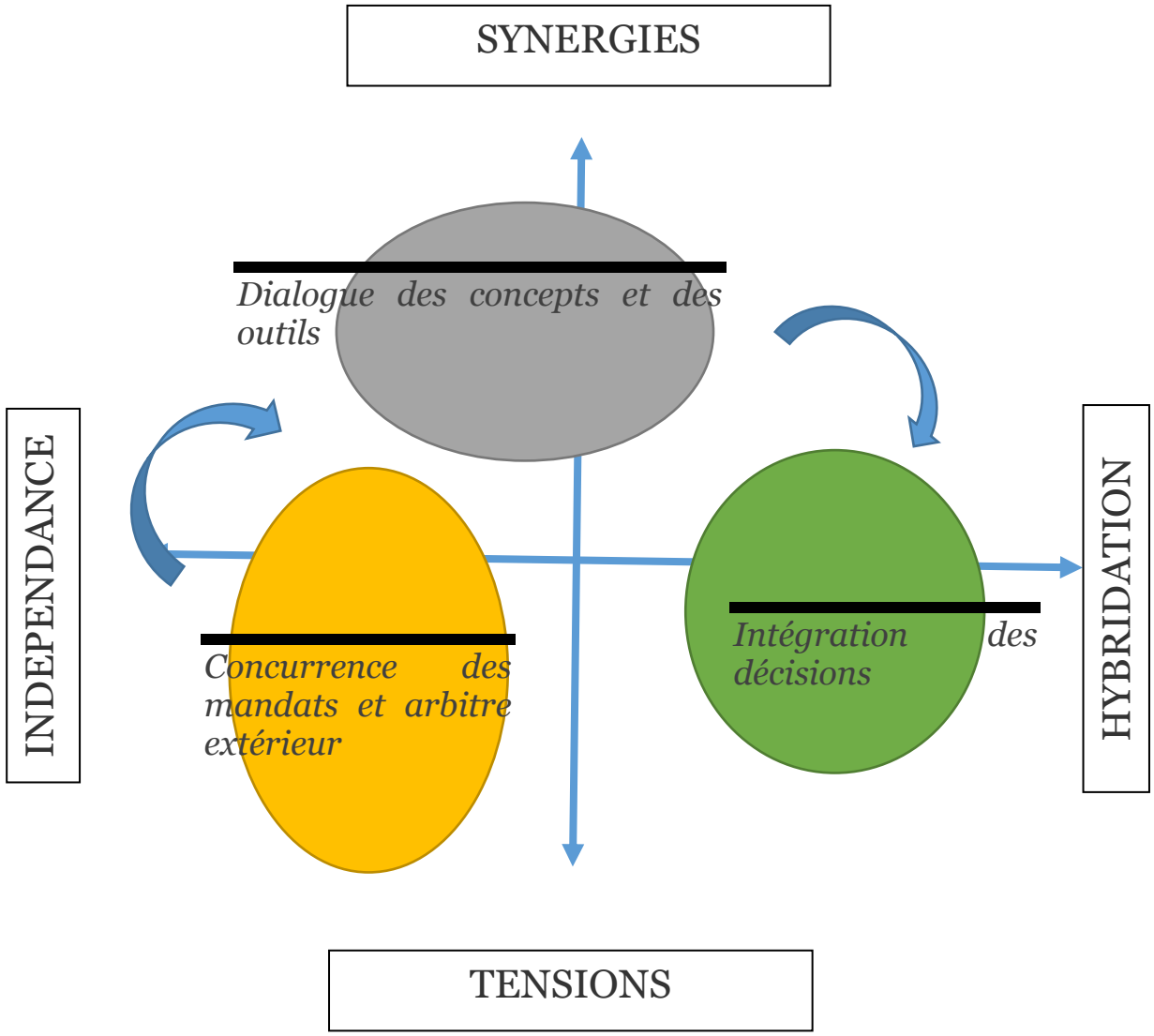
Cette approche se veut également évolutive et convergente: au fur et à mesure des progrès de la prise en compte de la protection des données en concurrence et de la concurrence en protection des données, dans les pratiques et les doctrines respectives des deux institutions, au fur et à mesure des progrès du dialogue des concepts et des outils, dont le présent rapport propose la montée en puissance, au fur et à mesure des éléments de convergence

[1] Cf. l'audition de Marie-Laure Denis devant le collège de l'Autorité de la concurrence en novembre 2022 : https://www.cnil.fr/fr/protection-des-donnees-et-droit-de-la-concurrence-marie-laure-denis-intervient-devant-le-college-de.

rendus publics par les deux autorités. L'hybridation des deux régulations sera ainsi en mesure de progresser, sans jamais aller bien sûr jusqu'à la fusion des cadres juridiques et des mandats des deux autorités.

Enfin, le présent rapport ne traite pas de l'articulation avec la protection du consommateur, qui devrait faire l'objet d'une approche intégrée avec les deux autres domaines, ni de la régulation du numérique en général, visant à mettre en place une coopération entre de multiples autorités qui excède l'objet du présent rapport.

Fig.1 : Différents modes d'articulation entre protection des données et concurrence



Légende : ***« articuler » deux cadres juridiques suppose de s'interroger selon deux axes : d'une part,*** *met-on l'accent sur les tensions (objectifs opposés) ou les synergies (objectifs convergents) et d'autre part, veut-on favoriser des régulations en silos (pas d'influence mutuelle) ou leur hybridation (objectifs, concepts, qualifications juridiques qui s'intègrent).*

S'agissant du sujet qui nous occupe, nous avons déjà quitté un régime d'entière indépendance mettant l'accent sur les tensions (quadrant sud-ouest qui représente le degré zéro de la coopération) mais ne sommes pas non plus dans un régime où les deux législations s'intègrent (ce qui se passerait en généralisant le cas Meta c/ Bundeskartellamt).

Nous sommes plutôt dans une situation plus équilibrée où nous cherchons à construire un dialogue des concepts et des outils pour tirer parti des synergies (l'inspiration mutuelle plutôt que la reconnaissance mutuelle) et promouvoir les convergences de régulation.

Encadré 1 : L'arrêt Meta de la CJUE

La possibilité de constater une violation du RGPD pour une autorité nationale de concurrence

L'arrêt Meta de la CJUE du 4 juillet 2023[2] **consacre la possibilité, pour une autorité de concurrence nationale, de constater à titre incident une violation du RGPD dans le cadre de l'examen d'un abus de position dominante, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus** (p. 36). Selon la Cour, aucune disposition du RGPD n'interdit aux autorités nationales de concurrence de constater, dans le cadre de l'exercice de leurs fonctions, la non-conformité au RGPD d'un traitement de données personnelles effectué par une entreprise en position dominante et susceptible de constituer un abus de cette position (pt 41).

La consécration de cette possibilité permet tout d'abord de conclure au soutien de la Cour à la prise en compte de la protection des données personnelles dans le champ de l'analyse concurrentielle, comme le rappelle la déclaration conjointe entre l'Autorité de la concurrence et la CNIL[3].

Réciproquement, la Cour ouvre la possibilité pour les autorités de protection des données nationales de prendre en compte les concepts du droit de la concurrence au soutien de leurs propres analyses. Ainsi, la Cour juge que la position dominante de l'opérateur d'un service ne fait pas obstacle, en tant que telle, à ce que ses utilisateurs puissent valablement consentir au traitement de leurs données personnelles effectué par cet opérateur. Cependant, elle juge qu'il s'agit d'un élément important pour déterminer si le consentement été donné librement (pt. 39).

Il peut en être déduit que les notions et concepts d'autres droits peuvent utilement être mobilisés au soutien de l'analyse menée par une autorité de protection des données. L'intégration de l'analyse concurrentielle dans les travaux de la CNIL apparaît dans ce cadre indispensable afin d'identifier les situations dans lesquelles le recours aux concepts du droit de la concurrence pourrait être favorisé. Cela permettra également de mieux déterminer la nécessité de faire appel à l'Autorité de la concurrence et sous quelle forme.

La préservation de l'autonomie des autorités compétentes

La Cour souligne néanmoins que lorsque l'autorité de la concurrence nationale relève une violation du RGPD, elle ne se substitue pas aux autorités de contrôle mises en place par ce règlement (pt 49). En effet, **l'appréciation du respect du RGPD doit se limiter aux seules fins de constater un abus de position dominante et d'imposer des mesures visant à cesser cet abus selon les règles du droit de la concurrence**.

Des enseignements peuvent en être tirés sur la manière adéquate pour les autorités d'utiliser les notions et concepts d'autres droits. Ainsi, **l'utilisation de notions et concepts d'autres droits par une autorité compétente doit strictement se limiter aux seules fins de mener à bien ses propres missions**. Ces dernières, prévues par les textes dans un Etat de droit, demeurent inchangées.

Une coopération institutionnelle renforcée

Dans ce cadre, la Cour affirme la nécessité d'une coopération institutionnelle renforcée entre les autorités nationales, en vertu du principe de coopération loyale posé par les traités européens. La Cour précise ainsi que les autorités nationales de concurrence doivent **se concerter et coopérer loyalement avec les autorités veillant au respect du RGPD** pour limiter les risques de divergence d'interprétation.

La Cour apporte des précisions utiles sur la manière dont cette coopération renforcée doit s'effectuer. A cet égard, les autorités doivent s'assister, **ne pas compromettre leurs objectifs respectifs et éviter les divergences**. Ainsi, la Cour indique que l'autorité nationale de concurrence doit notamment vérifier si le comportement en cause a déjà fait l'objet d'une décision par l'autorité de contrôle nationale compétente ou chef de file ou par la CJUE, et ne pourra le cas échéant s'en écarter. En cas de doute, l'autorité nationale de concurrence doit consulter ces autorités pour avis et solliciter leur coopération, autorités qui doivent de leur côté répondre dans un délai raisonnable (pts 54 et suiv.).

La **coopération existante entre la CNIL et l'Autorité de la concurrence a donc vocation à s'intensifier** par des consultations plus fréquentes dès lors que l'application de leurs règlementations se

[2] CJUE, aff. C-252/21, 4 juill. 2023, Meta Platforms Inc. e.a. contre Bundeskartellamt.
[3] Autorité de la concurrence et Commission nationale de l'informatique et des libertés, 2023, Concurrence et données personnelles : une ambition commune, p.8.

croisent. L'arrêt de la Cour fait d'ailleurs d'une telle coopération **non plus une faculté, mais une obligation juridique** pour les Etats membres et ces autorités.

2. L'articulation entre protection des données et concurrence

La coopération entre autorités de concurrence et de protection des données est devenue un impératif, en raison des évolutions du contexte tant économique que réglementaire et normatif. La numérisation de l'économie et l'omniprésence des grands acteurs du Net, mettant au centre de leurs modèles d'affaires la collecte et l'utilisation des données personnelles (2.1) explique l'acuité de cet enjeu. La protection des données personnelles en tant que droit fondamental et la protection de la concurrence comme élément du bon fonctionnement de l'économie et des marchés, peuvent en effet être articulés pour atteindre des objectifs communs (2.2). Il est donc nécessaire, comme l'illustre l'arrêt *Meta Platforms* de la CJUE (cf. encadré 1), pour la CNIL de prendre en compte l'analyse concurrentielle dans le cadre de ses travaux afin d'accroître la cohérence de son action conjointe avec l'autre autorité (2.3).

2.1 Les données personnelles au cœur des modèles d'affaires

2.1.1 La numérisation de l'économie

Impulsée par l'essor des technologies de l'information, une transformation économique et sociale profonde de la société française est à l'œuvre depuis plusieurs décennies. Parmi ces changements, l'importance prise par le numérique a modifié les logiques économiques et sociales préexistantes[4].

Ce monde numérique implique pour les entreprises de reconsidérer leurs modèles d'affaires en intégrant de nouvelles dynamique d'innovation. Face à la nécessité de développer régulièrement des produits et services innovants et aux possibilités offertes par le numérique, une logique d'industrialisation de l'innovation s'est installée dans l'économie. Le numérique a augmenté la proximité qui pouvait exister entre les consommateurs et les entreprises[5] : les modèles d'affaires de la fin des années 2000 considérant l'utilisateur comme un simple acheteur final ont peu à peu basculé vers des modèles d'affaires impliquant davantage le consommateur comme le moteur du cycle de vie du produit ou service. À titre d'exemple, les plateformes numériques ont intégré dans leurs modèles d'affaires l'utilisateur comme destinataire (utilisation de la plateforme) et moteur (collecte et utilisation de données personnelles aux fins d'optimisation et de financement) du service.

Pour les entreprises, ces transformations ont notamment eu pour conséquence de diversifier et de complexifier les modes de production. En effet, si les possibilités offertes par le numérique ouvrent un large champ des possibles, le modèle d'affaires peut rapidement être remis en question par une innovation plus récente. Pour les utilisateurs, les technologies du numérique se sont diffusées dans tous les pans de la société. Par conséquent, il devient de plus en plus facile d'utiliser le numérique au quotidien et certains usages deviennent plus difficilement accessibles ou moins avantageux lorsqu'ils ne sont pas totalement numérisés. De plus, la généralisation des outils du numérique a modifié le rapport du consommateur au produit ou service proposé par les entreprises.

En réalité, l'adaptation des entreprises à la transformation numérique est passée par une intégration de l'utilisateur dans les modèles d'affaires. En fonction du secteur, du produit, du service et des besoins de l'entreprise, cette prise en compte peut prendre des formes variées. Néanmoins, l'élément central de cette transformation reste la collecte et l'utilisation massive de données, et surtout de données personnelles. Cet usage intensif soulève des questions puisqu'il peut amener à des comportements non conformes à la réglementation : RGPD, mais aussi droit de la concurrence et droit de la consommation.

De fait, l'évolution des modèles d'affaires qui vient d'être rapidement décrite a contribué à augmenter le rapport de dépendance des entreprises vis-à-vis des outils du numérique en renforçant la place d'acteurs devenus dominants dans les secteurs fondés sur les technologies du numérique. Cette numérisation s'accompagne donc d'enjeux concurrentiels forts, soulignés en France par la création d'un service de l'économie numérique par

[4] P. Lemoine, 2014, « La nouvelle grammaire du succès : la transformation numérique de l'économie française », Rapport au gouvernement.
[5] Direction générale du Trésor, novembre 2020, « Numérisation des entreprises françaises », *Trésor-Eco*, n°271.

l'Autorité de la concurrence en 2020, mais aussi par l'Union européenne avec la mise en place du paquet numérique européen (DSA[6], DMA[7], *Data Act*[8]).

En particulier, c'est la collecte et l'utilisation de données au sens large qui cristallise l'essentiels des enjeux concurrentiels de la transformation numérique, avec pour de nombreuses entreprises un intérêt pour des données personnelles. Dès lors, comme le montre la déclaration conjointe entre la CNIL et l'Autorité de la concurrence, une protection conjointe des données personnelles et de la concurrence est nécessaire pour répondre de manière adaptée aux enjeux de la numérisation de l'économie.

2.1.2 L'essor des bases de données massives et de l'IA

La transformation des modèles d'affaires a modifié le rapport des entreprises aux données. La collecte et l'utilisation des données, notamment personnelles, sont devenues centrales.

L'accroissement de la quantité de données utilisées par les entreprises a contribué à généraliser la création de base de données massives aussi appelées *big data*. Elles correspondent à l'ensemble des données disponibles sur un sujet précis (santé, immobilier, assurance, etc.). Les données collectées peuvent être recueillies auprès de diverses sources, directement ou indirectement. Elles sont ensuite exploitées pour obtenir une meilleure connaissance du secteur, optimiser la production, accroître les ventes, améliorer le ciblage des utilisateurs, etc. Dès lors que la collecte de données est importante, la probabilité de collecte de données personnelles augmente mécaniquement.

L'accroissement de la formation et l'utilisation des bases de données massives ont été favorisés par les progrès technologiques constatés au cours des dernières décennies. Le développement d'outils plus rapides, plus intelligents et dotés de capacité de stockage plus importantes ont révolutionné les usages et contribué à la démocratisation des données massives. Ce faisant, leur agrégation et leur extraction se sont simplifiées, rendant l'analyse des données massives d'autant plus attrayante pour les entreprises. Ces données permettent d'accroître les connaissances de l'entreprise et d'effectuer des prédictions soit par l'application de modèles statistiques, soit par des modèles d'apprentissage automatique.

Les données massives représentent une source d'opportunités économiques importante pour les entreprises. En effet, tout en améliorant la performance globale de l'entreprise, elles peuvent contribuer à faciliter l'innovation. C'est d'ailleurs à partir de l'exploitation de ces données massives que les grandes entreprises du numérique se sont développées (Zuboff, 2019)[9]. En particulier, la collecte et l'utilisation de données personnelles ont été déterminantes afin de développer des avantages concurrentiels sur des marchés dynamiques. Ces pratiques, qui pour certaines étaient contraires au RGPD, ont contribué à la mise en place de positions dominantes qui soulèvent de nombreuses problématiques concurrentielles.

Exacerbée dans le domaine du numérique, l'utilisation des données massives s'est généralisée à l'ensemble de la société et de l'économie. Dorénavant, il est commun de trouver dans une entreprise, une collectivité ou une administration, une ou plusieurs fonctions dédiées à la collecte et l'exploitation de données.

Cette généralisation des données massives dans l'économie a également permis de construire une économie de l'attention « *dans laquelle les entreprises profitent des données pour capter de plus en plus finement l'attention des utilisateurs, les exposer à plus de publicité et, de façon circulaire, collecter encore plus d'informations* »[10]. La construction et le maintien de cette économie de l'attention constituent pour certains modèles d'affaires un des enjeux prioritaires. Dans l'économie du numérique, les plateformes dites « structurantes »[11] sont tout

---

[6] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) noté ici « DSA » pour *Digital Service Act*.

[7] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques) noté ici « DMA » pour *Digital Market Act*.

[8] Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) noté ici *Data Act*.

[9] Zuboff, S. (2019). *The age of Surveillance Capitalism*, London, England: Profile Books.

[10] Rapport d'information n°768 sur l'exposition des données, Les Notes Scientifiques de l'Office – Note n° 36 – Face à l'explosion des données, janvier 2023.

[11] Bourreau, M. et Perrot, A. (2020). « Plateformes numériques : réguler avant qu'il ne soit trop tard ». *Notes du conseil d'analyse économique*, (6), p. 1-12.

particulièrement concernées[12]. Face à la recrudescence de pratiques intrusives, se pose la question de la protection des utilisateurs contre de telles défaillances de marché, c'est-à-dire des situations où le marché ne permet pas d'atteindre par lui-même une allocation efficace des ressources.

En ce sens, le RGPD peut être « *un instrument puissant de consolidation de l'écosystème numérique européen* »[13] ; néanmoins la protection de la concurrence apparaît comme indissociable afin de ne pas reproduire des structures de marché dominées par quelques acteurs et rendre la concurrence plus effective.

Le secteur de l'intelligence artificielle (IA) est également un bon exemple des enjeux économiques associés à une prise en compte conjointe de la protection des données et de la concurrence. Le développement économique du secteur doit s'accompagner d'une intégration dès la conception (« *by design* ») de la protection des données personnelles.

Pour le moment, les modèles d'intelligence artificielle nécessitent de collecter et d'exploiter des quantités massives de données. Il y a donc, en parallèle d'une course à l'innovation, un développement des stratégies de production et consolidation de base de données adaptées à l'intelligence artificielle. Dans ce contexte, les grands acteurs du numérique, qui bénéficient de gisements de données personnelles importants, sont d'ores et déjà présents sur l'ensemble de la chaîne de valeur de l'IA[14]. Cette situation peut conduire à la construction de positions qui pourraient devenir dominantes dans ce domaine également.

2.2 Les questions d'orientation des marchés

2.2.1 Les mécanismes d'incitation des acteurs économiques

Le libre jeu de la concurrence incite les entreprises à se différencier en proposant des offres qui se démarquent de celles de leurs compétiteurs. La protection de la vie privée et des données personnelles des utilisateurs peut, à cet égard, faire partie d'une stratégie de différenciation pour les entreprises.

Néanmoins, les données personnelles peuvent dans certains cas être utilisées pour désavantager les entreprises concurrentes. Cette situation a été mise en avant dans l'affaire Apple/Shazam, où « *la Commission avait examiné si, grâce à l'acquisition du contrôle de l'application Shazam et de la base de données Shazam, Apple pouvait avoir accès à certaines données sur ses concurrents* » [15]. Les informations sur les clients rendues ainsi accessibles ont été vues par la Commission européenne comme des informations commercialement sensibles, en prenant en compte les obligations règlementaires relatives à la protection des données personnelles. L'affaire Microsoft/LinkedIn a aussi permis de mettre en exergue le rôle déterminant des données personnelles dans les stratégies des entreprises. Dans sa décision, la Commission européenne a notamment conclu que les règles du RGPD permettaient de limiter la capacité de ces deux entreprises à combiner et traiter ces données.

Réciproquement, les nombreuses sanctions de la CNIL montrent que libre jeu de la concurrence seul n'est pas suffisant pour permettre une orientation des entreprises vers des comportements plus respectueux de la vie privée et des données personnelles. L'action des institutions, ainsi qu'une bonne coopération entre elles, sont indispensables. En ce sens, le RGPD permet de mettre en place un cadre normatif incitatif favorisant la protection des utilisateurs.

En effet, les choix des entreprises peuvent être orientée par des mécanismes d'incitation, qui peuvent prendre des formes variées. Les incitations monétaires, telles que les sanctions pécuniaires par exemple, sont un des moyens d'internaliser les conséquences économiques sur les tiers des choix des entreprises en matière de vie privée dans leurs stratégies. Elles sont complétées par des incitations non monétaires, telles que les mises en demeure ou la publication des décisions, qui ont un effet sur le comportement des entreprises en augmentant le risque d'une sanction pécuniaire ou d'une dégradation de la réputation de l'entreprise.

La collecte et l'utilisation des données personnelles, ainsi que la protection de la vie privée, sont donc des facteurs d'orientation des choix des entreprises.

Le RGPD peut aussi permettre d'orienter les utilisateurs. Par la promotion d'une plus grande transparence, et donc d'une meilleure information des personnes, la règlementation en matière de protection des données

---

[12] Conseil national du numérique, « Votre attention, s'il vous plaît ! Quels leviers face à l'économie de l'attention ? », juillet 2022.
[13] Rapport Villani, Donner un sens à l'intelligence artificielle, 2018.
[14] Autorité de la concurrence, Avis 24-A-05 du 28 juin 2024 relatif au fonctionnement concurrentiel du secteur de l'intelligence artificielle générative.
[15] Commission européenne, avril 2024, Competion *policy brief*, Issue 1, p.15.

personnelles permet à la fois de faciliter un choix éclairé des utilisateurs et une orientation vers des offres plus respectueuses de la vie privée et des données personnelles. Enfin, une plus grande prise en compte de la vie privée dans le choix des utilisateurs incite à son tour les entreprises à développer et améliorer leurs offres en la matière.

2.2.2 La vie privée comme paramètre concurrentiel

La CNIL intervient dans une « *économie de marché fondée sur les principes de liberté de choix du consommateur et de liberté d'entreprendre* »[16]. Comme le rappelle la déclaration conjointe « *une concurrence libre et non faussée permet d'éviter les comportements de rente préjudiciables au consommateur* »[17]. Or, le consommateur est également un individu ou une « personne concernée » au sens du RGPD.

Avec le développement de modèles d'affaires utilisant davantage de données personnelles, la protection de ces données s'est peu à peu affirmée comme un paramètre de concurrence à prendre en compte dans les décisions des autorités de concurrence. En effet, les marchés numériques se caractérisent par la présence d'acteurs au pouvoir de marché important et une tendance à la concentration. Les pouvoirs structurants de ces acteurs et la difficile contestabilité de leurs positions conduisent à maintenir des structures de marché concentrées.

En particulier, les plateformes numériques, par l'utilisation de modèles d'affaires fondés sur l'accumulation et la combinaison des données, sont propices au développement d'avantages concurrentiels centrés sur l'accumulation de données. Ces avantages sont ensuite amplifiés et consolidés par les effets de réseau propres au numérique, qui peuvent alors « *favoriser le verrouillage de positions dominantes, et risquer de dégrader la concurrence et de favoriser dans le même temps une exploitation abusive des données personnelles* »[18]. Un cercle vicieux de la surexploitation et de la non-conformité se met alors en place dans les deux domaines à la fois.

En outre, la capacité limitée des utilisateurs à exercer un pouvoir de négociation face aux acteurs dominants ne permet pas toujours, même s'ils le souhaitent, de choisir une offre plus respectueuse de leur vie privée. De plus, leurs comportements peuvent être influencés par une forte asymétrie d'information entre eux et les entreprises, ainsi que par la mise en place de stratégies biaisant le consentement (« *dark-patterns* », présélection de choix, etc.). Il convient également de prendre en compte les externalités positives et négatives consécutives à la collecte et au traitement de données personnelles que peuvent produire les entreprises compte tenu de leurs effets sur les utilisateurs.

Indéniablement, les données personnelles sont devenues un moteur de croissance et un avantage commercial dans certains domaines, notamment celui du numérique et de la technologie. À titre d'exemple, dans le cadre d'une opération de concentration (fusion ou acquisition), la protection des données personnelles « *peut être un élément important de la qualité d'un produit ou d'un service offert et donc un paramètre de la concurrence entre les parties à la concentration et leurs rivaux et un élément de différenciation* »[19]. La Commission peut alors examiner le projet en prenant en compte le RGPD, aux fins de considérer les limites qui incomberaient aux entreprises en ce qui concerne la combinaison d'ensembles de données ou les règles relatives à la collecte, au traitement, au stockage et à l'utilisation des données par exemple.

Du point de vue de la protection de la concurrence, le niveau de protection correspond à un paramètre de qualité et donc de choix pour l'utilisateur. Un marché concurrentiel peut permettre par l'innovation et une pression concurrentielle suffisante de promouvoir une meilleure prise en compte de la vie privée des utilisateurs et la protection de leurs données. Aussi, la prise en compte par la CNIL des mécanismes concurrentiels à l'œuvre sur les marchés est-elle cruciale afin de favoriser la création de services et produits favorisant une plus grande maîtrise des données par l'utilisateur. Continuer à favoriser la mise en place de meilleures conditions de choix des utilisateurs en améliorant un exercice libre de leurs choix sur le marché passe donc par une meilleure compréhension du rôle de la protection des données personnelles comme paramètre concurrentiel.

2.2.3 Contribuer à l'innovation

L'intégration de l'analyse concurrentielle dans les travaux et décisions relatifs à la protection des données personnelles permet également de participer au débat concernant la contribution du RGPD à l'innovation. La

---

[16] Autorité de la concurrence et Commission nationale de l'informatique et des libertés, 2023, « Concurrence et données personnelles : une ambition commune », p.3.
[17] Ibid.
[18] Ibid., p.6.
[19] Commission européenne, avril 2024, Competion *policy brief*, Issue 1, p.5.

littérature économique ne permet pas de conclure définitivement à l'existence d'un effet global du RGPD sur l'innovation (CNIL, 2023)[20]. Néanmoins, la prise en considération des enjeux concurrentiels spécifiques de chaque marché dans l'analyse économique permet de mieux prendre en compte l'évolution de la dynamique d'innovation des secteurs centrés sur la collecte et l'exploitation des données personnelles. La concurrence est en effet le moteur principal de l'innovation, soit qu'on souhaite y échapper, soit qu'on souhaite contester des positions existantes.

Prendre en compte la concurrence permet de mieux comprendre comment et pourquoi les entreprises ont été contraintes de mettre à jour leurs outils informatiques, leurs modes de fonctionnement et la gestion de leurs données afin d'innover pour leur mise en conformité RGPD ou d'aller plus loin que la simple conformité pour faire de la protection de la vie privée un élément de différenciation. Ces ajustements ont certes nécessité des ressources qui n'ont plus été disponibles pour investir dans d'autres activités de recherche et d'innovation, néanmoins « *ils peuvent favoriser l'innovation progressive au sein du portefeuille de produits et de services existant* »[21]. De plus, cet investissement pourrait réduire leurs coûts liés à la mise en œuvre du RGPD et ainsi améliorer l'efficacité des processus internes de l'entreprise, qui seraient alors une occasion d'améliorer les revenus de l'entreprise par des économies de coûts ou des innovations incrémentales (Blind, Niebel et Rammer, 2024).

À titre d'exemple, dans le domaine de l'IA, l'innovation se fonde sur les données. La prise en compte des spécificités concurrentielles permet une vue plus complète des enjeux du secteur tout en intégrant la protection de la vie privée et des données personnelles comme un des paramètres importants dès la conception des outils. Dans la pratique, *« les régulateurs et les professionnels de la protection de la vie privée dans les organisations, travaillent activement au déploiement de solutions pour mettre en œuvre une IA respectueuse de la vie privée et même à utiliser l'IA au service de la protection de la vie privée* »[22]. Les autorités de protection des données ont donc un rôle dans la clarification quant à la collecte et l'utilisation responsables et conformes au RGPD des données personnelles, dans le but de contribuer à favoriser l'innovation en matière d'IA.

En résumé, une meilleure articulation entre la concurrence et la protection des données permet de garantir un environnement favorable à l'innovation respectueuse de la vie privée et des données personnelles.

D'ailleurs, continuer à développer une pleine compréhension de ces enjeux économiques comme le fait la CNIL est nécessaire pour intégrer davantage la protection de la vie privée et des données personnelles au cœur des préoccupations des entreprises lorsqu'elles innovent. Certes, la réglementation peut être un moteur d'innovation en incitant « *les acteurs à mener des activités d'innovation afin de préserver leur compétitivité sur les marchés* »[23]. Néanmoins, l'innovation dépend également de nombreuses autres éléments, tels que la taille de l'entreprise, le modèle d'affaires, les économies d'échelles, les effets de réseaux ou encore l'accès aux financements. Inciter les entreprises à innover en matière de protection de la vie privée nécessite de comprendre davantage les dynamiques d'innovation et concurrentielle des entreprises.

2.3 Une culture minimale de la concurrence

2.3.1 Comprendre et se faire comprendre

Pour la CNIL, se faire comprendre par les autres autorités, et notamment l'Autorité de la concurrence, est une nécessité. Cela permet également de diffuser le plus largement possible les pratiques et comportements les plus vertueux pour la vie privée et les données personnelles. En effet, si l'intégration des analyses concurrentielles dans les travaux de la CNIL permet d'améliorer sa capacité à orienter les acteurs du marché vers une meilleure protection des personnes, il demeure nécessaire de pouvoir de développer une faculté à pouvoir communiquer avec les autres autorités dans un langage commun.

Le développement de ce langage commun peut s'appuyer utilement sur le vocabulaire économique. En particulier, il nécessite de comprendre le vocabulaire relatif à la concurrence pour mieux déterminer quels sont les points de tension et de convergence. Cette meilleure compréhension contribue aussi à accroître la capacité

---

[20] https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres.

[21] Blind, K., Niebel, C. et Rammer, C. (2024). The impact of the EU General data protection regulation on product innovation. *Industry and Innovation*, *31*(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858.

[22] OECD.AI Policy Observatory (2024). A new expert group at the OECD for policy synergies in AI, data, and privacy. Disponible ici : https://oecd.ai/en/wonk/expert-group-data-privacy.

[23] OCDE (2023). Concurrence et innovation, Partie I : Cadre théorique - Note de référence, DAF/COMP(2023)2, p. 30. Disponible ici : https://one.oecd.org/document/DAF/COMP(2023)2/fr/pdf.

d'analyse des enjeux économiques et concurrentiels de la CNIL. Elle permet *in fine* de mieux appréhender les dossiers communs et avis en lien avec l'Autorité de la concurrence.

Une meilleure compréhension de ce qu'est la concurrence est également nécessaire afin de détecter les intersections entre protection des données et concurrence qui pourraient être d'intérêt pour la CNIL dans certains dossiers. À titre d'exemple, certaines problématiques concurrentielles sont susceptibles de prime abord de ne pas soulever de question relative à la protection des données. Néanmoins, la protection des données personnelles peut s'avérer dans certains cas un paramètre important pour la concurrence. Dans cette situation, dans la perspective d'une intensification de la coopération entre la CNIL et l'Autorité de la concurrence, l'expertise de la CNIL pourrait être utile pour compléter l'analyse de l'Autorité. Réciproquement, l'expertise de l'Autorité de la concurrence pourrait permettre d'éviter une incohérence des décisions futures des deux autorités.

La construction d'un langage commun par un développement des méthodes et analyses respectives concourrait ainsi à renforcer la capacité d'identification des sujets sur lesquels chaque Autorité pourrait contribuer utilement.

La connaissance du vocabulaire de la concurrence et la prise en compte de ses problématiques peut également contribuer à une meilleure compréhension, de la part des professionnels, des acteurs des décisions de la CNIL. En effet, comme tout champ du droit, celui de la protection des données personnelles possède son propre vocabulaire. Développer une capacité à ancrer les travaux et décisions de la CNIL dans un cadre économique plus large peut permettre de les rendre « faciles à lire et à comprendre » pour un plus grand nombre. Cela peut aussi favoriser l'adhésion des acteurs économiques aux recommandations et avis rendus. La prise en compte des dynamiques concurrentielles permet de simplifier l'intégration dans les modèles d'affaires des entreprises en diminuant le risque que ces recommandations ou avis ne génère des effets économiques négatifs non anticipés pour l'entreprise.

2.3.2 Mieux identifier les conséquences économiques et concurrentielles

Prendre en compte les enjeux concurrentiels dans les travaux de la CNIL passe par une identification en amont des principales problématiques afin de garantir une pleine efficacité des décisions.

Les missions de la CNIL ne peuvent être assurées sans prendre en compte les conséquences économiques et concurrentielles qui pourraient résulter de ses décisions, avis ou recommandations. À titre d'exemple, la CNIL doit veiller à prendre en compte « *dans tous les domaines de son action, la situation des personnes dépourvues de compétences numériques, et les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises* » (art. 8.I.2.c de la loi « Informatique et libertés »). Une telle prise en compte ne saurait intervenir sans une identification des problématiques économiques et concurrentielles de ces acteurs.

En sus d'un accompagnement adapté, mieux identifier les problématiques économiques et concurrentielles permet d'anticiper les évolutions technologiques et stratégiques des entreprises. Cela permet de renforcer la capacité de la CNIL à orienter les transformations économiques vers une plus grande protection de la vie privée et apporter des éclairages sur les enjeux économiques et concurrentiels en lien avec la protection des données personnelles. La CNIL avait, par exemple, en 2021 publié un nouveau Livre blanc sur les données et moyens de paiement permettant d'« *éclairer, d'accompagner les professionnels et anticiper les transformations à venir* »[24].

Accélérer l'identification des conséquences économiques et concurrentielles a également pour objectif d'accroître la sécurité juridique pour les entreprises. D'ailleurs la CNIL élabore régulièrement des cadres de références (lignes directrices, référentiels, recommandation, etc.) en concertation avec les acteurs ou secteurs concernés. Ils permettent de guider ces organismes dans la mise en conformité de leur traitements[25]. La prise en compte des réalités économiques et des modèles d'affaires des entreprises accroît la pertinence, la portée et l'applicabilité de ces cadres de référence sur le terrain. En particulier, dans le cadre des recommandations, les entreprises seront d'autant plus enclines à mettre en place des propositions plus protectrices des données personnelles si elles ont été pensées et proposées en cohérence avec leurs enjeux économiques et concurrentiels.

---

[24] CNIL, 2021, QUAND LA CONFIANCE PAIE : Les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données, Collection livre blanc, n°2. Disponible ici : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_livre_blanc_2-paiement.pdf.

[25] https://www.cnil.fr/fr/les-decisions-de-la-cnil/les-cadres-de-reference.

En outre, « *l'informatique doit être au service de chaque citoyen* »[26] et ne doit pas fonctionner au détriment du respect de la vie privée des utilisateurs. La protection des données étant un droit fondamental, en cas de survenance d'un conflit entre protection des données et concurrence il est possible que le juge, saisi de ce conflit, donne la priorité à la protection des données, mais à l'issue d'une période plus ou moins longue d'insécurité juridique. Mieux identifier ces problématiques permet donc d'anticiper et d'éviter ces effets en garantissant une application proportionnée de la règlementation en matière de protection des données personnelles.

2.3.3 Maîtriser les effets sur la concurrence

Comme le rappelle la déclaration conjointe du 12 décembre 2023[27], alors que la mission confiée à la CNIL vise à « *protéger les utilisateurs contre toute collecte et exploitation préjudiciables de leurs données, notamment lorsqu'ils utilisent des biens ou des services marchands* », la politique de concurrence a pour objectif de garantir « *les conditions d'une concurrence libre et non faussée entre les entreprises sur les marchés, dans l'intérêt des consommateurs, en favorisant l'innovation, la diversité de l'offre et des prix attractifs* ». Les deux visions convergent donc dans leur mise en œuvre et dans certains de leurs objectifs, puisqu'elles ont vocation à servir l'utilisateur, qu'il soit entreprise ou consommateur individuel.

Toutefois, afin de mieux maîtriser les effets des normes de protection sur la concurrence, la CNIL devrait les appréhender dès le stade de leur élaboration. À titre d'exemple, le coût de la protection des données personnelles est proportionnellement « moins onéreux » pour une grande entreprise. Les incidences économiques sur les plus petites entreprises sont donc différentes. Ces disparités, parfois très importantes, nécessitent une prise en compte plus asymétrique du principe de responsabilité afin de ne pas favoriser l'émergence de barrières à l'entrée néfastes pour la concurrence et les utilisateurs.

De plus, le développement des modèles d'affaires reposant sur la collecte et l'exploitation de données renforce la place des données personnelles dans les dynamiques concurrentielles des marchés. La protection de la vie privée en tant que paramètre concurrentiel a des effets directs sur les choix proposés aux utilisateurs, mais également sur les stratégies déployées par les entreprises. En particulier, « *le contrôle de données peut être source de pouvoir de marché et servir à des comportements anticoncurrentiels* »[28]. Dès lors, il convient de mieux appréhender les incidences des décisions de la CNIL sur la concurrence, puisqu'elles peuvent – dans certains cas et indirectement – avoir un effet sur les conditions de concurrence.

Maîtriser davantage les effets sur la concurrence permet aussi de développer un équilibre entre la concurrence et la protection de la vie privée des utilisateurs. Si l'orientation des acteurs vers des modèles d'affaires plus protecteurs de la vie privée est importante, l'attractivité de ces modèles est nécessaire pour atteindre cet objectif. Comprendre, anticiper et maîtriser les effets des décisions sur la concurrence permet de les adapter au mieux et d'associer les acteurs (entreprises et/ou autorités de concurrence) aux démarches de réflexion de la CNIL. C'est le cas notamment lorsque des enjeux concurrentiels apparaissent lors de l'élaboration de documents de droit souple tels que des recommandations ou des codes de conduite. Il peut alors être opportun, pour la CNIL, de consulter pour avis l'Autorité de la concurrence afin de disposer de la meilleure analyse possible des enjeux concurrentiels du marché.

Anticiper le futur rôle des données pour les entreprises nécessite également d'appréhender pleinement les effets sur la concurrence. En effet, les décisions de la CNIL peuvent avoir pour effet d'orienter les choix des acteurs qui pourraient alors en réponse modifier leurs modèles d'affaires dans une logique à la fois de conformité et de stratégie concurrentielle. Aussi, la dynamique concurrentielle du marché peut-elle jouer un rôle déterminant dans les modalités de la mise en conformité des entreprises.

Proposition n°1 : prendre en compte les questions concurrentielles en amont dans les travaux de la CNIL. *Développer une meilleure vision des effets des décisions de la CNIL sur la concurrence permet de promouvoir une cohérence générale de l'application de la concurrence et de la protection des données. L'accroissement de cette cohérence contribue à faciliter la valorisation de comportements vertueux à la fois pour le respect de la concurrence et la protection de la vie privée et des données personnelles. Il concourt également à renforcer la prévisibilité des actions de régulation et par conséquent la sécurité juridique des entreprises.*

---

[26] Article 1er de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[27] Autorité de la concurrence et Commission nationale de l'informatique et des libertés, 2023, Concurrence et données personnelles : une ambition commune, p.6.
[28] Direction générale du Trésor, juillet 2022, Trésor-Eco, n°310, p.3.

3. Le dialogue des concepts et des outils

Une coopération entre la CNIL et l'Autorité de la concurrence, ne se bornant pas à atténuer les tensions qui peuvent exister entre deux régulations distinctes mais recherchant réellement les convergences, en développant les synergies - dans les limites du cadre juridique définissant les compétences et les pouvoirs propres des services de chacune de ces institutions - doit promouvoir un dialogue des concepts (mais aussi des outils). Un tel dialogue permet de tirer parti d'une certaine communauté des objectifs et de favoriser l'inspiration mutuelle entre les deux cadres de régulation. Après l'arrêt *Meta Platforms*, cet exercice dont la Cour elle-même a donné l'exemple est devenu indispensable. Toutefois, dans bien des cas, les concepts et les outils ne peuvent être transposés automatiquement d'un cadre à l'autre, et doivent être adaptés.

Le droit de la concurrence et la jurisprudence ont permis de construire de nombreux outils et concepts qui, du point de vue de la protection de données personnelles, peuvent contribuer à améliorer la prise en compte des enjeux concurrentiels dans les décisions de la CNIL (3.1). Réciproquement, le RGPD et la jurisprudence associée permettent à l'analyse concurrentielle de mieux appréhender les pratiques des acteurs en matière de données dans la pratique de l'Autorité de la concurrence (3.2). Cette prise en compte croisée des données personnelles et de la concurrence permet également de faire progresser une approche par les risques, afin de mieux approcher les effets potentiels sur les personnes et sur les marchés (3.3). *In fine*, ce dialogue des concepts et des outils entre la CNIL et l'Autorité de la concurrence doit se décliner dans la coopération existante notamment en ce qui concerne la mise en œuvre (3.4).

3.1 Développer la prise en compte de la concurrence en protection des données

3.1.1 La dominance

Sans être définie par les textes, la notion de dominance a été précisée par la jurisprudence comme concernant « *une position de puissance économique détenue par une entreprise qui lui donne le pouvoir de faire obstacle au maintien d'une concurrence effective sur le marché en cause en lui fournissant la possibilité de comportements indépendants dans une mesure appréciable vis-à-vis de ses concurrents, de ses clients et, finalement, des consommateurs* »[29]. D'ailleurs, la CJUE indique également qu'« *une telle position, à la différence d'une situation de monopole ou de quasi-monopole, n'exclut pas l'existence d'une certaine concurrence mais met la firme qui en bénéficie en mesure sinon de décider, tout au moins d'influencer notablement les conditions dans lesquelles cette concurrence se développera et, en tout cas, de se comporter dans une large mesure sans devoir en tenir compte et sans pour autant que cette attitude lui porte préjudice* »[30].

La position dominante n'est pas illicite en soi : seul son abus est prohibé. Mais, pour deux ces concepts, avec le développement des modèles d'affaires utilisant massivement les données personnelles, la vie privée et les comportements des entreprises en matière de protection des données personnelles sont devenus des déterminants importants dans l'analyse de la dominance et des abus associés d'une entreprise.

Si le rôle de la protection des données dans la qualification d'abus de dominance semble voué à s'accroître, le rôle de la dominance (et de l'abus de position dominante) dans la protection des données personnelles, bien qu'existant, reste peu développé. À titre d'exemple, lorsqu'un abus de position dominante prend la forme de ventes liées, une analyse de la segmentation du marché[31] en matière de vie privée peut améliorer l'analyse concurrentielle. Réciproquement, cette notion d'abus pourrait être utile pour identifier les conditions contractuelles existantes lorsqu'une entreprise met en place un modèle d'affaires proposant un service alternatif payant sans publicité ciblée et une version gratuite rémunérée par de la publicité ciblée.

Dans sa décision C-252/21, en s'appuyant sur le considérant 43 du RGPD qui dispose que « *lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement* », le consentement ne peut constituer une base légale valable, la CJUE a mis en évidence le rôle important de la position dominante sur l'appréciation de la liberté du consentement[32]. Il convient de rechercher s'il existe un déséquilibre manifeste entre l'usager et le service, si le consentement est sollicité de manière suffisamment granulaire et si la collecte

[29] CJUE, aff. 27/76, 14 févr. 1978, United Brands / Commission, Rec. p. 00207, pt 65.
[30] CJUE, aff. 85/76, 13 févr. 1979, Hoffmann-La Roche / Commission, Rec. p. 00461, pt 4.
[31] Autrement dit des produits ou services avec des niveaux différents de protection de la vie privée.
[32] CJUE, aff. C-252/21, 4 juill. 2023, Meta Platforms Inc. e.a. contre Bundeskartellamt, pt 155.

de données est strictement nécessaire[33]. Par conséquent, alors même que la dominance accroît la probabilité d'un tel déséquilibre, sans emporter en elle-même invalidité du consentement, c'est malgré tout au fournisseur, dans ce cas comme dans les autres cas, d'apporter la preuve que son action ne remet pas en cause la liberté du consentement [34].

De même, en ce qui concerne le choix de la base légale, les lignes directrices du G29 sur l'intérêt légitime adoptées en 2014 prennent en compte la dominance parmi les facteurs pertinents pour la balance des intérêts entre la personne concernée et le responsable du traitement, ce dernier étant alors en meilleure position pour imposer ce qu'il considère comme étant son intérêt légitime[35].

Au-delà, plusieurs questions se posent visant à mieux comprendre le rôle que peut avoir la dominance en pratique en protection des données : (1) Comment considérer la dominance lorsque seules des alternatives non segmentées selon la vie privée sont présentes sur le marché ? (2) Quel est le rôle de la dominance lorsque des alternatives plus favorables à la vie privée existent ? (3) Quel rôle l'abus de position dominante peut-il avoir sur les conditions de la protection ? (4) L'absence de toute alternative peut-elle être expliquée par une position dominante ?

En outre, en cas de dominance, le risque pour la protection des données des personnes est supérieur car l'entité pourrait être tentée d'abuser de ses conditions contractuelles[36]. Par ailleurs, la dominance tend à réduire les choix des personnes sur le marché. Dès lors, la prise en compte de la dominance permet de mieux tenir compte de l'asymétrie existante entre l'entreprise et les personnes[37], ce qui permet de mieux évaluer un éventuel déséquilibre manifeste.

3.1.2 Le pouvoir de marché

En concurrence, le pouvoir de marché se définit comme « *la capacité pour les entreprises de fixer leurs prix au-delà de leurs coûts ou d'offrir des prestations de faible qualité* »[38]. En droit de la concurrence, l'existence d'un pouvoir de marché n'est pas suffisante pour qualifier un comportement d'anticoncurrentiel ou pour interdire un projet de concentration. D'ailleurs, l'acquisition d'un pouvoir de marché peut résulter du libre jeu de la concurrence. Néanmoins, sa « concentration excessive »[39] ou son utilisation aux fins de restreindre la concurrence soulève des enjeux importants.

À titre d'exemple, l'Autorité de la concurrence précise qu'une plateforme numérique pourrait être définie comme une entreprise qui détient un pouvoir de marché structurant en considérant « *l'importance de sa taille, sa capacité financière, sa communauté d'utilisateurs et/ou des données qu'elle détient* »[40]. Ce pouvoir lui permettrait de « *contrôler l'accès ou d'affecter de manière significative le fonctionnement du ou des marchés sur lesquels elle intervient* »[41]. Aussi, la capacité de l'entreprise à collecter et utiliser des données fait partie des indices potentiels permettant de déterminer l'existence d'un pouvoir de marché.

En protection des données personnelles, en généralisant l'approche du G29, le rôle du pouvoir de marché[42] peut être déterminant pour l'appréciation de la balance des intérêts lorsque le traitement est fondé sur la base légale de l'intérêt légitime. En effet, la détention d'un pouvoir de marché met l'entreprise en capacité d'avoir un effet sur le choix des usagers. Dans certains cas, cette situation peut conduire à une diminution du nombre d'offres présentes sur le marché. Le prix proposé devient alors plus élevé qu'il ne le devrait, la qualité de la protection des données dans les offres disponibles peut s'amenuiser et, *in fine*, la capacité de négociation ou de changer de fournisseur de l'usager peut s'en trouver amoindrie. Dans cet exemple, le pouvoir de marché a donc pour effet d'augmenter l'asymétrie existante entre l'entreprise et les utilisateurs. Il peut avoir aussi pour effet de biaiser

---

[33] Ibid., point 144 et 149.
[34] Ibid., point 98 et 152.
[35] G29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 avril 2014, pages 40 et 55.
[36] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), point 127.
[37] Ibid.
[38] Tirole, J. (2014). Nobel Prize Lecture, Market Failures and Public Policy.
[39] Autorité de la concurrence, 3 mars 2023, Feuille de route 2023-2024.
[40] Autorité de la concurrence, 19 février 2020, Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques, p.8.
[41] Ibid.
[42] Graef, I. et Van Berlo, S. (2021). Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility. *European Journal of Risk Regulation*, *12*(3), 674–698. https://doi.org/10.1017/err.2020.92.

les négociations contractuelles entre un acteur et d'autres partenaires ou intermédiaires lorsqu'il s'agit de traiter des données personnelles (par exemple entre un responsable de traitement et son sous-traitant).

Ainsi, à partir d'une analyse concurrentielle de la structure du marché et du comportement des acteurs, il est possible d'en tirer des conséquences plus larges en protection des données, que ce soit pour apprécier un éventuel déséquilibre manifeste ou opérer la balance des intérêts en cause par exemple. En protection des données, ce n'est pas la question des barrières à l'entrée sur le marché en tant que tel qui compte, mais celle de la préservation de l'autonomie des personnes usagers de ce marché.

Encadré 2 : un exemple d'adaptation des concepts, le « data power »

Dans le domaine du numérique, où la donnée est au cœur de la construction de l'avantage concurrentiel, l'obtention ou le renforcement d'un pouvoir de marché provient dans certains cas de la maîtrise des données personnelles, notamment lorsqu'il s'agit d'une plateforme numérique. Ce phénomène apparaît comme problématique du point de vue de la CNIL, car les principes de la protection des données veulent que les données personnelles soient sous le contrôle des personnes, et non des responsables de traitement, et qu'en tout cas, ces derniers ne puissent imposer aux personnes leurs choix en la matière.

Alors qu'en concurrence, le pouvoir de marché désigne l'influence d'un acteur sur la manière dont les échanges sont organisés sur l'offre (les concurrents) et la demande (les consommateurs), en protection des données, on s'intéresse aux effets de cette influence sur les personnes via les conséquences de cette position dans l'exercice de leur droit fondamental à la protection des données personnelles. A ce titre, le pouvoir sur les données ressemble plus au déséquilibre entre le consommateur et le professionnel en droit de la consommation. Il peut donc être intéressant d'adapter les concepts au lieu d'en faire une réutilisation impropre.

Du point de vue de la CNIL, on peut donc définir le « pouvoir sur les données », qui peut se manifester de plusieurs manières dans la réalité empirique objective, comme une entrave à l'autonomie informationnelle de la personne, provenant d'un déséquilibre économique entre elle et le responsable de traitement, se traduisant par une asymétrie d'information ou d'autres biais de la rationalité individuelle, et se mesurant par un risque pour la protection des données de cette personne ou sa vie privée.

Le « pouvoir sur les données » (*data power*), « *une forme multiforme de puissance disponible pour les plateformes numériques, découlant de leur contrôle des flux de données* »[43], pourrait être particulièrement pertinent pour mieux appréhender les capacités de ces entreprises à agir sur les données. En effet, l'omniprésence d'une plateforme peut lui permettre d'avoir accès à de grands volumes de données, de pouvoir les accumuler et les combiner, et bien que le traitement puisse – s'il respecte le RGPD – ne pas être problématique, le pouvoir découlant du volume, de la variété des données, ainsi que de l'asymétrie entre les entreprises et les consommateurs peut l'être[44] pour des raisons que ce concept permet d'expliciter.

L'existence d'un pouvoir sur les données pourrait par exemple permettre de mieux comprendre les effets des comportements d'une entreprise sur la capacité d'exercice du choix du consommateur étant donné les offres alternatives existantes. En particulier, sa prise en compte pourrait concourir à améliorer l'analyse de la capacité de l'entreprise à affecter le consentement de l'utilisateur. À titre d'exemple, l'utilisation de « *dark patterns* » par les grandes plateformes pourrait révéler dans certains cas un indice de l'existence d'un pouvoir sur les données. Dans le cadre des modèles « consentir ou payer », par exemple, « *conformément au principe de loyauté, l'équilibre des pouvoirs devrait être un élément clé de la relation entre le responsable du traitement et la personne concernée. Les déséquilibres de pouvoir doivent être évités ou, lorsque cela n'est pas possible, ils doivent être reconnus et pris en compte par des contre-mesures appropriées. Ceci afin de s'assurer que la personne concernée puisse s'engager dans un choix véritablement libre lorsqu'elle consent au traitement de ses données personnelles* »[45].

---

[43] Lynskey, O. (2019). Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*, *20*(1), 189-220. https://doi.org/10.1515/til-2019-0007.

[44] Karjalainen, T. (2022). The battle of power: Enforcing data protection law against companies holding data power, *Computer Law & Security Review*, 47(105742), https://doi.org/10.1016/j.clsr.2022.105742

[45] EDPB, 17 avril 2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Opinion of the Board (Art. 64).

Initialement promu par Orla Lynskey, ce concept a été repris par Majcher (2023)[46] et certains régulateurs comme l'EDPS (Colaps et D'Cunha, 2024[47]). Ces auteurs soulignent son adaptation en matière d'intégrité de l'autonomie informationnelle des personnes concernées et via la notion de « déséquilibre manifeste » du considérant 43 du RGPD, qui joue un rôle important dans les analyses. D'un point de vue économique également, le « data power » décrit la capacité des responsables de traitement à extraire la valeur d'usage des données à leur profit dans la chaîne de valeur de la donnée (ex : publicité ciblée) en laissant les individus concernés aux prises avec les externalités négatives (risques, coûts de l'exploitation abusive de la donnée, personnalisation des prix, etc.).

La portée de ce concept est étendue : il permet de décrire également la capacité de négociation asymétrique des grandes plateformes en ligne avec les autres entreprises et intermédiaires ayant besoin de leurs données mais parfois soumises à des clauses léonines voire discriminatoires (la loyauté des relations contractuelles est un des sujets du Data Act), ainsi que la capacité de ces acteurs à maintenir leurs partenaires dans l'opacité des pratiques utilisées (ex : mesure d'audience et efficacité de la publicité ciblée) ou de modifier les règles de l'écosystème à leur profit (ex : rôle en matière de compliance des magasins d'applications mobiles, *Privacy sandbox* de Google). *In fine*, ce pouvoir pourrait nourrir des acquisitions prédatrices et réduire la contestabilité des marchés et l'innovation (Majcher, 2023).

Enfin, le « data power » recouvre la capacité de lobbying de ces grands acteurs, leur capacité à influer sur le « narratif » médiatique et politique et ainsi, en dernière instance, de faire évoluer la réglementation à leur profit, sans parler des ressources qu'ils peuvent consacrer à des contentieux pour se soustraire à des décisions de mise en œuvre des autorités compétentes, qu'elles soient d'ailleurs relatives à la concurrence ou à la protection des données de la même façon.

Pour Klaudia Majcher, il est possible pour une autorité de qualifier l'existence d'un pouvoir sur les données selon ces trois dimensions individuelle, économique et politique en ayant recours à une analyse à la fois structurelle et comportementale de l'acteur. Cette grille d'analyse pourrait être utilement complétée par une analyse de la situation des personnes concernées et notamment, des préjudices y compris informationnels qu'elles subissent.

Proposition n°2 : expérimenter le concept de « pouvoir sur les données » en tant qu'éclairage doctrinal, *lorsqu'il est plus adapté que les concepts concurrentiels existants (dominance ou pouvoir de marché) dans les analyses de protection des données de la CNIL, lorsqu'il s'agit d'apprécier les relations entre une personne concernée et un responsable de traitement.*

3.1.3 Mieux définir le produit ou service en cause

L'utilisation du concept de marché pertinent par les autorités de concurrence nécessite des moyens techniques et des pouvoirs d'investigations différents de ceux de la CNIL. Par ailleurs, elle exige de définir un produit ou service dans une temporalité précise afin de déterminer les effets potentiels sur le marché. La délimitation du marché pertinent est donc, en soi, une partie importante de l'analyse lors des décisions ou avis émis par l'Autorité de la concurrence. Elle pourrait difficilement être reproductible du point de vue d'une autorité de protection des données.

Néanmoins, cette approche peut être une source d'inspiration. En effet, la protection des données personnelles invite à prendre comme point de départ de l'analyse les effets des pratiques des entreprises sur les utilisateurs. Il y a donc une nécessité pour la CNIL de définir précisément le produit ou service en cause afin d'évaluer au mieux le degré de conformité des entreprises aux règles du RGPD. Ainsi, les précédents avis sectoriels ou décisions de l'Autorité de la concurrence, voire de la Commission européenne, pourraient permettre à la CNIL de confirmer le choix du produit ou service en cause.

Par ailleurs, la méthodologie de construction du marché pertinent pourrait donner des indications de bonnes pratiques pour définir les produits ou services en cause. C'est le cas de la notion de substituabilité, c'est-à-dire

---

[46] Majcher, Klaudia, 'The Big Picture', *Coherence between Data Protection and Competition Law in Digital Markets*, Oxford Data Protection & Privacy Law, Oxford, 2023, https://doi.org/10.1093/oso/9780198885610.003.0008.

[47] D'Cunha, C., Colaps, A., "A clear imbalance between the data subject and the controller : data protection and competition law", in Two decades of personal data protection, What next ? EDPS 20th Anniversary, chapitre 15, pp. 192 à 205. Luxembourg : Office des publications de l'UE, 2024.

la capacité d'un produit à remplacer un autre sans perte de valeur pour l'utilisateur. Du point de vue du RGPD, sans avoir besoin de réaliser de calcul économique, la notion d'équivalence fonctionnelle pour l'utilisateur pourrait être retenue. À titre d'exemple, dans le cadre des modèles « payer ou consentir », elle consisterait pour l'utilisateur à bénéficier d'un service ou produit présentant les mêmes fonctionnalités quelle que soit la formule proposée (payante ou gratuite).

D'autres éléments du point de vue de l'utilisateur peuvent utilement inspirer la CNIL, telle que la capacité de l'utilisateur à faire un choix libre entre la poursuite ou l'arrêt de l'utilisation d'un service. Cela dépend de la question de savoir si l'utilisateur dispose d'une « véritable alternative ». À titre d'exemple, dans le cadre des modèles « payer ou consentir », lorsqu'un utilisateur n'a d'autre choix que d'utiliser un autre service nécessitant son consentement pour maintenir un service actif, celui-ci pourrait se trouver dans une situation de contrainte où le préjudice pourrait être accentué.

3.1.4 L'exclusivité dans les conditions contractuelles

Le droit de la concurrence s'intéresse également aux accords d'exclusivité. Ces accords sont des contrats qui ont, bien évidemment, dans certaines circonstances, des effets sur la concurrence. Ils peuvent avoir pour objectif de mettre en place un engagement de l'acheteur à se fournir auprès d'un unique fabricant (exclusivité de fourniture). Des engagements peuvent aussi être définis pour que le fabricant ou commerçant ne s'approvisionne qu'auprès d'un seul distributeur (exclusivité d'approvisionnement). Un contrat peut également être rédigé afin qu'en plus des engagements sur la fourniture et/ou l'approvisionnement, des modalités de vente soient fixées (exclusivité de concession)[48].

De tels contrats peuvent conduire à des comportements anticoncurrentiels, tels que des abus de position dominante. En effet, les contrats d'exclusivité transforment les relations entre les acteurs d'un marché et donc la structure normale de la concurrence. En particulier, lorsque l'entreprise est dominante, celle-ci peut chercher à « *évincer ses concurrents en les empêchant d'acheter à des fournisseurs. La Commission considère que ce verrouillage des intrants est en principe susceptible d'entraîner une éviction anticoncurrentielle si l'obligation de fourniture exclusive ou l'incitation lient la plupart des fournisseurs efficaces d'intrants et si les entreprises en concurrence avec l'entreprise dominante sont incapables de trouver d'autres sources efficaces de fourniture des intrants* »[49].

Du point de vue de la protection des données personnelles, ces accords d'exclusivité peuvent conduire à une restriction du nombre d'alternatives équivalentes pour les utilisateurs. La doctrine sur les *cookies walls*, ou « murs de traceurs », montre que l'existence d'alternatives équivalentes doit être prise en compte dans l'appréciation de la validité du consentement. Ce critère se retrouve également comme un des éléments importants de l'évaluation de la validité du consentement dans le cadre des modèles « consentir ou payer ».

L'exclusivité peut également concerner les questions d'accès ou de mise à disposition de données. Cette question du partage asymétrique des données ne peut qu'être vue différemment du point de vue des deux autorités : alors que les autorités de la concurrence pourraient y voir une pratique anti-concurrentielle, les autorités de protection des données se demanderont si le partage était nécessaire pour réaliser la finalité du traitement et souhaiteront qu'il n'excède pas cette mesure. Toutefois, il n'existe aucune obligation d'ouverture *erga omnes* de la donnée détenue par une entreprise, dans la mesure où la donnée personnelle n'est en règle générale pas qualifiable d'« infrastructure essentielle » au sens du droit de la concurrence : non-rivale, sa collecte est libre sous réserve de respecter le cadre applicable et c'est au contraire cette ouverture qui accroîtrait la dépendance vis-à-vis des plus gros fournisseurs de données[50]. En revanche, les deux autorités se retrouveront sur la nécessité de la transparence sur ces partenariats d'accès aux données (tant envers les personnes concernées, qui bénéficient à ce sujet d'une obligation légale, qu'envers le marché).

---

[48] Reboud, L. (1968), Contrats d'exclusivité et concurrence, *L'Actualité économique*, 43(4), 617–669. https://doi.org/10.7202/1003090ar.

[49] Commission européenne, 24 février 2009, Communication de la Commission — Orientations sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes, 2009/C 45/02, point 32.

[50] Cf. Autorité de la concurrence et Bundeskartellamt, « Droit de la concurrence et données », étude publiée, 10 mai 2016 : https://www.autoritedelaconcurrence.fr/sites/default/files/Big%20Data%20Papier.pdf page 20.

3.2 Expliciter la protection des données comme paramètre concurrentiel

3.2.1 La licéité

L'article 5.1 a) du RGPD dispose que les données personnelles doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée* ». Par ailleurs, le traitement n'est licite que dans la mesure où il respecte l'une des six bases légales du RGPD[51].

L'analyse concurrentielle peut permettre d'identifier une situation dans laquelle un acteur tirerait un bénéfice de l'illicéité de son traitement. Ainsi, par la mise en œuvre d'un traitement illicite, l'entreprise pourrait être en capacité de renforcer, maintenir ou acquérir une position avantageuse sur le marché (notion de « concurrence déloyale »). Cela pourrait être également, pour une autorité de concurrence, un élément constitutif d'un pouvoir de marché et/ou d'une position dominante. Autrement dit, l'illicéité d'un traitement pourrait conduire à produire des effets néfastes sur la concurrence. La Cour de cassation juge d'ailleurs avec constance que le manquement à une réglementation confère à l'acteur qui s'en rend responsable « *un avantage concurrentiel indu, qui peut être constitutif d'une faute de concurrence déloyale* »[52].

Au demeurant, il peut être utile de prendre en compte la stratégie de l'entreprise pour mieux répondre aux différentes questions – Quelles données sont concernées ? Comment ont-elles été utilisées ? Pour quelles finalités ont-elles été exploitées ? – que se pose la CNIL. L'avantage tiré de l'illicéité du traitement pourrait être corroboré par les motifs concurrentiels identifiés lors de la phase d'analyse.

Dans le cas où le caractère manifeste de l'avantage concurrentiel ainsi obtenu ne peut être établi, notamment si aucune décision de l'Autorité de la concurrence ou de la Commission européenne ne le permet, la saisine de l'Autorité de la concurrence pour avis est nécessaire. Cet avis pourrait alors permettre de caractériser l'illicéité d'un traitement au titre du RGPD. À ce titre, l'intégration de l'analyse concurrentielle en amont des demandes d'avis permettra de mieux identifier les situations nécessitant un avis de la part de l'Autorité de la concurrence.

Proposition n°3 : développer dans la pratique de la CNIL la prise en compte des illicéités concurrentielles au titre du a) du 1 de l'article 5 du RGPD*. Les comportements de concurrence déloyale ou les pratiques anti-concurrentielles, s'ils sont jugés ou documentés par les autorités de concurrence, peuvent constituer des facteurs complémentaires aux manquements aux règles de protection des données. Dans le cas contraire, il conviendra de saisir l'Autorité de la concurrence pour avis.*

Encadré 3 : Le respect du principe non bis in idem dans la mise en œuvre du droit de la concurrence et de la protection des données

Selon le principe *non bis in idem*, principe général du droit issu de la procédure pénale et découlant tant de l'article 8 de la Déclaration des droits de l'homme et du citoyen que consacré à l'article 50 de la Charte des droits fondamentaux de l'Union européenne, nul ne peut être doublement poursuivi ou puni pénalement à raison des mêmes faits. Ce principe ne se limite pas aux poursuites et sanctions qualifiées de « pénales » mais s'étend plus généralement à toute sanction ayant le caractère de punition, y compris lorsqu'elle n'est pas prononcée par une juridiction répressive. Il s'applique donc aux manquements relevant du droit de la concurrence et de la protection des données, qui peuvent notamment donner lieu à des sanctions administratives.

A cet égard, dans l'hypothèse d'une mise en œuvre successive du droit de la concurrence et de la protection des données dans des affaires connexes, le risque d'enfreindre ce principe apparaît limité. En effet, outre que l'analyse portera dans de nombreux cas sur des faits distincts, le droit de la concurrence et la protection des données à caractère personnel ont des objets et protègent des intérêts sociétaux bien différents.

Par ailleurs, la jurisprudence du Conseil constitutionnel[53] précise qu'il n'est pas exclu que « *les mêmes faits puissent faire l'objet de poursuites différentes aux fins de sanctions de nature différente en application de corps de règles distincts* », sous réserve du respect du principe de proportionnalité des délits et des peines en cas de cumul de sanctions. Dans le même sens, s'agissant de réglementations présentant des objectifs pourtant proches, la jurisprudence de la CJUE indique que ce principe ne s'oppose pas à ce qu'une entreprise soit

[51] Article 6.1 du RGPD.
[52] v. p. ex. Cass. Comm. 27 septembre 2023, n°21-21.995.
[53] Par exemple : Cons. Const., décision n° 2021-892 QPC, 26 mars 2021, Société Akka technologies et autres, concernant la sanction de l'obstruction aux enquêtes de l'autorité de la concurrence.

sanctionnée pour une infraction au droit de la concurrence lorsqu'elle a déjà fait l'objet d'une décision définitive pour non-respect d'une réglementation sectorielle pour les mêmes faits[54].

3.2.2 La nécessité

Quelle que soit sa base légale, un traitement doit toujours être nécessaire à l'atteinte de la finalité poursuivie par le responsable de traitement. Cette finalité doit être prédéfinie.

Ce principe revêt une importance particulière au moment des fusions de bases de données lors d'opérations de concentration entre entreprises. L'existence d'un historique de concentrations lors desquelles les données personnelles ont été affectées devrait éveiller la vigilance. En effet, le responsable du traitement doit pouvoir démontrer que le traitement préalable à la concentration est toujours nécessaire en précisant, le cas échéant, les nouvelles conditions dans lesquelles le traitement sera réalisé.

Ainsi, les situations concurrentielles se traduisant par une diminution des choix à disposition des consommateurs posent la question du nombre d'alternatives réelles à une solution dominante. C'est le cas également de structures concurrentielles où peu d'acteurs représentent une véritable alternative (oligopole par exemple) déjà établie et reconnue par l'Autorité de la concurrence. Face à ces situations, il serait alors utile de déterminer à la fois le caractère moins intrusif de l'alternative et la capacité de l'utilisateur à faire ce choix.

3.2.3 Le libre consentement

Le consentement en tant que base légale à un traitement doit, pour être valide au sens du RGPD, être donné de manière libre, spécifique, éclairée et univoque par la personne concernée[55].

Pour être libre, le consentement doit résulter d'un choix réel et non contraint de la personne concernée.

Or, l'analyse de la position d'un responsable de traitement sur un marché donné peut éclairer utilement l'appréciation du caractère libre du consentement à un traitement de données à caractère personnel.

L'arrêt *Meta Platforms* donne un exemple concret dans lequel la situation concurrentielle permet d'apprécier la liberté du consentement des personnes concernées[56][57]. La position dominante du responsable du traitement sur un marché donné pourrait ainsi, sans affecter par principe la liberté du consentement, être prise en compte pour rechercher si ce critère de liberté du consentement est satisfait.

Réciproquement, la capacité du consommateur à effectuer un choix libre peut également être utilisé pour qualifier des comportements anticoncurrentiels. Dès lors, il est important pour mieux protéger la vie privée de prendre en compte d'éventuelles décisions de l'Autorité de la concurrence ou de la Commission européenne concernant le comportement concurrentiel de l'entreprise, en particulier lorsque la protection de la vie privée a été identifiée comme un des paramètres concurrentiels.

En outre, le défaut de liberté du consentement de l'utilisateur peut également être, du point de vue concurrentiel, le résultat de l'exercice abusif d'un pouvoir de marché. Dans cette situation, la liberté du consentement est un paramètre déterminant pour identifier de quelle façon l'entreprise s'y est prise pour abuser de son pouvoir de marché. Ainsi, l'absence de liberté du consentement ou la manipulation du consentement des personnes par des *dark patterns*, par exemple, peuvent-elles jouer un rôle important dans la qualification par l'Autorité de la concurrence d'abus d'exploitation.

En outre, lorsqu'un traitement est fondé sur la base légale du consentement, l'appréciation du respect du principe de nécessité tient compte des alternatives proposées à l'utilisateur (ex : en cas de traitement des données biométriques, avec la base légale du consentement, une alternative à la biométrie doit exister pour que le consentement soit valide). En particulier, la capacité du responsable à proposer un traitement identique assurant une meilleure protection de la vie privée est étudiée. Aussi, dans cette hypothèse, la présence d'alternatives moins intrusives pour la vie privée sur le marché est un élément important de l'appréciation du respect du principe de nécessité pour l'acteur en cause.

---

[54] CJUE, aff. C-117/20, 22 mars 2022, bpost SA contre Autorité belge de la concurrence, paragraphes 40-58.
[55] Art. 4.11 du RGPD.
[56] CJUE, aff. C-252/21, 4 juill. 2023, Meta Platforms Inc. e.a. contre Bundeskartellamt, p. 36.
[57] Article 7.4 du RGPD.

3.2.4 La loyauté du traitement

Aux termes du a) du 1 de l'article 5 du RGPD, les données personnelles doivent être collectées de manière licite, loyale et transparente. Le considérant 39 du RGPD précise à cet égard que le fait que des données à caractère personnel sont traitées, et selon quelles modalités, devrait être transparent pour les personnes concernées. Les informations communiquées aux personnes concernées sur les traitements qui les concernent (identité du responsable du traitement, finalités du traitement notamment) permettent d'assurer un traitement loyal et transparent à l'égard des personnes concernées.

Le respect du principe de loyauté du traitement est donc étroitement lié à la transparence dont il est fait preuve à l'égard des personnes concernées : le traitement des données doit correspondre factuellement à la description qui en est faite aux personnes concernées. Toutes les informations utiles concernant le traitement doivent être apportées aux personnes concernées, en application des articles 13 et 14 du RGPD, et de surcroît présentées de manière aisément accessible et facile à comprendre (consid. 39 du RGPD).

Le principe de loyauté a en ce sens été décrit par la littérature[58] (et par l'EDPS[59] dans son avis 8/2016[60]) comme permettant de faire le lien entre concurrence, protection des données et protection du consommateur : c'est ce principe qui met l'utilisateur en situation de décider de l'usage qui est fait de ses données en toute connaissance de cause. Le droit de la consommation prohibe ainsi les pratiques commerciales déloyales[61].

De son côté, le droit de la concurrence prohibe l'imposition de « *conditions de transaction non équitables* » (article 102 TFUE), regardées comme abusives en situation de position dominante. Sur ces points, l'atteinte à la concurrence pourrait augmenter la gravité d'un manquement au principe de loyauté d'un traitement de données, par exemple au regard de la transparence à l'égard des personnes concernées.

3.2.5 La minimisation

La situation concurrentielle peut également être prise en compte lors de l'analyse de la proportionnalité ainsi que de la nécessité de la collecte de données au regard du principe de minimisation ou de la base légale retenue[62].

L'absence ou la faible concurrence, notamment lorsque l'entreprise est en situation de dominance, pourrait être un des indices d'une possible sur-collecte lorsque le consommateur n'a pas le choix, sur le marché, entre des services impliquant des niveaux de collecte différenciés, en violation du principe de minimisation.

Dans ce contexte, au vu des biais affectant les décisions des personnes et les incitations éventuellement mises en place (qui peuvent, dans certains cas, constituer des *dark patterns*), le responsable du traitement devrait démontrer qu'il ne sur-collecte pas ou qu'il permet un choix effectif entre plusieurs niveaux de service modulant l'intensité de la collecte de données dès lors que les objectifs poursuivis par les traitements de données que ces différents niveaux de service impliquent justifient la collecte des données . Certaines évolutions récentes tendent d'ailleurs à permettre une équivalence entre collecte excessive et abus d'exploitation en position dominante, la fourniture de données étant assimilée à un prix payé[63].

Néanmoins, le type d'abus est déterminant pour admettre qu'il s'agisse d'un indice de sur-collecte et devrait être précisément identifié.

Concernant les abus de position dominante, les pratiques consistant à favoriser ses propres services (*self-preferencing*) publicitaires sont des exemples de situations où une possible sur-collecte pourrait avoir eu lieu. En effet, si l'accumulation de données visait à faciliter ce type de pratiques, le respect du principe de minimisation des données pourrait s'en trouver affecté.

---

[58] I. Graef, D. Clifford et P. Valcke (2018). Fairness and enforcement; bridging competition, data protection, and consumer law, *International Data Privacy Law*, 2018, 8(3).
[59] L'EDPS est l'autorité chargée de la protection des données pour les institutions, organes et organismes de l'Union européenne.
[60] https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf
[61] Directive n° 2005/29 du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur.
[62] Article 5.1.c du RGPD ; art. 6 du RGPD.
[63] Directive n° 2019/770 du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, article 3.1 al. 2.

L'abus de dépendance économique peut aussi constituer des indices de sur-collecte dès lors qu'il fait intervenir des échanges de données personnelles entre les entreprises. En effet, cet abus se caractérise par une exploitation excessive de la situation de dépendance par le biais de pratiques anormales, déséquilibrées ou excessives imposant « *de façon directe ou indirecte des conditions de transaction non équitables* »[64]. Ainsi, le caractère excessif pourrait découler d'une volonté de sur-collecte de la part de l'entreprise en situation de dominance.

Proposition n°4 : à l'appui du respect du principe de minimisation, développer l'analyse du rôle joué par les pratiques anti-concurrentielles dans l'accumulation des données *et les indices de collecte de données au détriment des personnes qui ne peuvent s'y opposer.*

3.2.6 La qualification des acteurs

Les déséquilibres de marché peuvent affecter les choix du responsable du traitement en matière de protection des données : du fait de son faible pouvoir de marché, un responsable de traitement pourrait voir son choix de partenaires commerciaux limité. En raison de ces choix limités, il pourrait plus difficilement assurer la compatibilité avec le RGPD des traitements dont il est responsable : il pourrait par exemple échouer à imposer à son sous-traitant des mesures lui permettant de respecter ses propres obligations au titre du RGPD, ou ne pas trouver sur le marché de fournisseur de solutions techniques conformes à la réglementation.

Cependant, un choix limité de partenaires commerciaux et le rapport de force déséquilibré que cela pourrait engendrer n'ont pas vocation à exonérer le responsable du traitement de ses propres obligations au regard de la protection des données : en effet, le responsable du traitement reste par exemple toujours libre du choix de son sous-traitant, même si l'offre présente sur le marché est limitée.

De même, un rapport de force déséquilibré entre deux acteurs n'aurait pas d'effet sur la qualification au sens du RGPD pour un traitement donné. En effet, le pouvoir de marché n'entre pas dans les critères de détermination de la qualification au sens du RGPD.

Par ailleurs, il serait opportun que les autorités de protection des données tiennent compte de ces déséquilibres dans leur pratique de contrôle, afin de prendre en compte l'ensemble de la chaîne de traitement et les acteurs ayant un effet de levier sur les autres.

En cas de manquement du sous-traitant à ses obligations vis-à-vis du responsable de traitement au titre du RGPD, il reste possible pour le responsable de traitement de mettre en cause son co-contractant sur le terrain du droit commun des obligations : fournir en tant que sous-traitant un service dont le fonctionnement méconnaîtrait par lui-même le RGPD engage ainsi la responsabilité civile du sous-traitant vis-à-vis de son responsable de traitement[65].

3.3 Une approche conjointe par les risques

3.3.1 Les risques congloméraux et verticaux

La Commission européenne précise que les « concentrations verticales concernent des sociétés opérant à différents niveaux de la chaîne d'approvisionnement »[66]. C'est le cas, lorsqu'un fabricant fusionne avec un de ses distributeurs par exemple. En revanche, les « concentrations conglomérales sont des concentrations entre entreprises entretenant des relations qui ne sont ni purement horizontales (concurrents opérant sur le même marché en cause) ni verticales (fournisseurs ou clients) »[67]. Ainsi, l'intégration conglomérale ou verticale crée des risques concurrentiels spécifiques.

---

[64] CJUE, aff. T-151/01, 24 mai 2007, Duales System Deutschland / Commission, Rec. p. II-1607, pt 120-122.
[65] Le contrat liant le responsable du traitement et le sous-traitant peut en particulier être frappé de nullité si le non-respect des obligations du cocontractant au titre du RGPD constitue une erreur sur les qualités essentielles de l'objet du contrat (voir en ce sens CA Grenoble, 12 janv. 2023, n° 21/03701, dans le cas de la conception d'un site web).
[66] Commission européenne, 18 octobre 2018, Lignes directrices sur l'appréciation des concentrations non horizontales au regard du règlement du Conseil relatif au contrôle des concentrations entre entreprises, 2008/C 265/07, point 4.
[67] Ibid, point 5.

Si les concentrations verticales ou conglomérales sont « généralement moins susceptibles de créer des problèmes de concurrence que les concentrations horizontales »[68], elles peuvent, dans certains cas, avoir pour effet d'entraver la concurrence effective d'une manière significative. Deux effets principaux sont systématiquement étudiés : les effets coordonnés et non coordonnés.

Les « *effets non coordonnées peuvent principalement se produire lorsque les concentrations non horizontales entraînent un verrouillage du marché* »[69], c'est-à-dire lorsque la concentration « *entrave ou ferme l'accès des entreprises rivales existantes ou potentielles aux sources d'approvisionnement ou aux débouchés, réduisant ainsi leur capacité et/ou leur incitation à animer la concurrence* »[70]. Il y a alors un risque d'augmentation du prix proposé aux consommateurs ou de réduction de la qualité du service proposé. Du point de vue de la protection des données personnelles, une telle situation pourrait orienter les consommateurs vers des alternatives moins protectrices de la vie privée ou des données personnelles afin de bénéficier d'un meilleur prix. Ainsi, la forte intégration – verticale ou conglomérale – de l'entreprise aurait-elle pour effet de limiter l'accès à une meilleure protection de la vie privée. Ce risque est d'autant plus fort dans l'économie des plateformes, qui bénéficient parfois d'effets de gamme importants créant des incitations à la concentration verticale ou conglomérale.

Pour leur part, les « *effets coordonnés se produisent lorsque l'opération de concentration change la nature de la concurrence de telle sorte que les entreprises qui, jusque-là, ne coordonnaient pas leur comportement, seraient dorénavant beaucoup plus susceptibles de le faire pour augmenter leurs prix ou porter atteinte, d'une autre manière, à la concurrence effective* »[71]. Cette situation accroît le risque pour la protection des données personnelles en renforçant l'incitation à la combinaison de données (coordination pour l'accès aux intrants). D'ailleurs, le DMA, bien qu'interdisant la combinaison de données pour les contrôleurs d'accès, n'apporte qu'une réponse partielle à cet égard puisqu'il reste limité à un renvoi des dispositions relatives à la combinaison des données collectées par la plateforme essentielle à la base légale du consentement. En effet, l'entreprise pourra combiner des données personnelles si le choix précis a été présenté à l'utilisateur final et qu'il donne son consentement au sens des articles 4 et 7 du RGPD[72].

D'autres pratiques peuvent également avoir un effet sur la protection de la vie privée et des données personnelles. C'est le cas notamment des ventes liées et groupées qui consistent respectivement à subordonner l'achat d'un produit à un autre et à ne rendre disponible à l'achat que l'ensemble des produits[73]. Par de telles pratiques, en particulier lorsque l'entreprise est dominante, celle-ci peut chercher à évincer ses concurrents et orienter les choix des consommateurs vers des produits moins protecteurs en matière de données personnelles et de vie privée. En particulier, ces pratiques peuvent conduire à limiter artificiellement le développement d'innovations favorables à la protection de la vie privée, notamment « *lorsque les concurrents évincés par l'entreprise dominante sont, du fait de ce refus, dans l'impossibilité de mettre sur le marché des produits ou des services innovants et/ou lorsque l'innovation subséquente est susceptible d'être freinée* »[74].

En outre, la concentration d'entreprises peut conduire à ce qu'une des parties à la concentration récupère des données détenues par l'autre entreprise. Si cette conséquence peut ne pas soulever de risque du point de vue de la concurrence, l'objectif de la concentration pourrait être considérée, dans certains cas, comme une volonté du responsable de traitement de contourner les règles du RGPD sur la réutilisation des données personnelles. L'accroissement des projets de concentration fondés sur les données (« *data driven mergers* ») augmente le risque que de telles situations surviennent, que l'intégration soit verticale, conglomérale ou horizontale.

La compréhension de ces situations et pratiques, ainsi que l'intégration de leurs incidences sur la protection de la vie privée est importante pour améliorer l'analyse et les décisions qui peuvent être prises.

---

[68] Ibid, point 11.
[69] Ibid, point 18
[70] Ibid.
[71] Ibid., point 19.
[72] Article 5.2 du Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

[73] Commission européenne, 24 février 2009, Communication de la Commission — Orientations sur les priorités retenues par la Commission pour l'application de l'article 82 du traité CE aux pratiques d'éviction abusives des entreprises dominantes, 2009/C 45/02.
[74] Ibid., point 87.

3.3.2 Les risques structurels et comportementaux

Pour appréhender au mieux les incidences des pratiques et comportements des entreprises pour la protection des données personnelles et de la vie privée. Il convient de distinguer les risques structurels et comportementaux. Ces deux catégories n'emportent pas les mêmes effets sur le marché et peuvent donc avoir des conséquences différentes en matière de protection des données personnelles. En effet, si les risques structurels correspondent aux problématiques provenant de la structure du marché entre les acteurs, les risques comportementaux concernent les pratiques et comportements mis en place par l'entreprise.

En effet, certaines pratiques anticoncurrentielles ou concentrations peuvent avoir pour effet de modifier la structure du marché en créant ou consolidant un ou des acteurs sur le marché. Ces situations provoquent un risque accru de renforcement du pouvoir de marché d'une entreprise, prenant la forme d'un pouvoir sur les données. Ce renforcement peut conduire à favoriser des comportements néfastes du point de vue de la protection des données. À titre d'exemple, l'accroissement du pouvoir sur les données d'une entreprise peut conduire à faciliter la mise en place de pratiques de sur-collecte qui pourraient être contraires au principe de minimisation. Ces situations sont davantage identifiées dans les projets de concentration analysés par l'Autorité de la concurrence.

Pour leur part, les risques comportementaux proviennent des pratiques ayant pour objectif de modifier le fonctionnement du marché. Ces situations peuvent conduire à la réduction du niveau global de la concurrence sur le marché et à y renforcer la position d'un ou plusieurs acteurs.

L'analyse de ces risques doit ainsi pouvoir être menée en commun par les deux autorités : tant du point de vue des concentrations que de l'analyse des pratiques de marché des acteurs. Dans l'idéal, les deux autorités devraient avoir un programme de travail conjoint d'exploration des risques, avec l'identification périodique de sujets d'intérêt commun pour lesquels des échanges informels d'expertises, des auditions conjointes volontaires et des études communes seraient envisagés.

Par ailleurs, les agents de la CNIL peuvent, en l'état actuel du droit, être mobilisés en tant que rapporteurs externes par l'Autorité de la concurrence dans le cadre de l'instruction d'une affaire, ce qui peut également contribuer au partage d'expertises. De même, les agents de l'Autorité de la concurrence peuvent être invités en tant que de besoin aux « clubs conformité » sectoriels de la CNIL, lorsque des sujets concurrentiels sont susceptibles d'y être évoqués.

Proposition n°5 : explorer conjointement les risques et les marchés *sur la base d'échange d'expertises, d'auditions conjointes volontaires ou de la réalisation d'études communes entre la CNIL et l'Autorité de la concurrence.*

3.3.3 Les analyses d'impact relatives à la protection des données (AIPD)

Lorsque la structure du marché n'est pas suffisamment concurrentielle, la ou les entreprises dominantes peuvent avoir plus d'incitations à réaliser des traitements de données, parfois sensibles, à grande échelle. De même, l'acquisition d'un pouvoir sur les données (ex : accès privilégié ou moins coûteux, possibilités de combinaison, économies d'échelle) suscite des risques supplémentaires pour les personnes (cf. encadré 2). Dans ces hypothèses, il pourrait être nécessaire d'effectuer une analyse d'impact relative à la protection des données (AIPD) pour ces traitements. En effet, une AIPD doit être menée quand le traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* » (art. 35-1 du RGPD). A cet égard, la collecte de données personnelles à large échelle, combinée à un autre facteur de risque, est un critère déterminant du caractère obligatoire de la réalisation d'une AIPD[75].

Ainsi, la notion de « *pouvoir sur les données* », en tant qu'élément du risque à analyser, pourrait conforter la nécessité de mettre en place une AIPD. L'étude des impacts potentiels notamment serait susceptible d'être améliorée en tenant davantage compte du caractère risqué des traitements de l'entreprise eu égard à sa position sur le marché et son influence sur les données.

[75] G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679, 4 avr. 2017.

En particulier, l'évaluation de l'intérêt légitime du responsable du traitement lors de la description des opérations de traitement envisagées[76], de la balance des intérêts entre la personne et le responsable de traitement et des finalités du traitement devrait être complétée par une prise en compte du pouvoir sur les données de l'entreprise. En outre, des situations de dominance pourraient, dans certains cas, avoir pour effet de modifier l'évaluation de la nécessité et de la proportionnalité des opérations de traitement[77].

3.4 Mieux structurer la coopération, y compris pour la mise en œuvre

3.4.1 Des organisations variées selon les pays

Dans l'économie numérique, la coopération entre autorités de protection des données et de concurrence en matière de mise en œuvre de la régulation (*enforcement*), c'est-à-dire sur des cas concrets pour lesquels des manquements sont constatés, est particulièrement utile. Il existe de nombreux exemples de coopération entre des autorités de protection des données et de concurrence en Europe et dans le monde. La plupart correspondent à des mises en commun de moyens pour analyser des secteurs. Toutefois, peu de pays bénéficient d'une structuration formelle de la coopération entre les deux autorités qui, seule, permet l'échange d'informations sur les cas. À titre d'exemple, des pays comme l'Argentine, le Brésil, le Japon ou le Canada développent de nombreuses collaborations entre leurs régulateurs nationaux sans structure formelle.

C'est le cas également de l'Allemagne, bien qu'une modernisation de la loi allemande en matière de concentration ait eu lieu, de l'Italie ou encore du Mexique. Néanmoins, dans certains pays, la coopération est davantage organisée soit par des dispositions dans la loi, qui permettent le cas échéant de lever l'obligation de secret professionnel, soit par des déclarations communes. La coopération entre la CNIL et l'Autorité de la concurrence est à placer dans cette dernière catégorie.

Enfin, des formes de coopération plus structurées existent aussi, telles que l'*Australian Digital Platform Regulators Forum* (DP-REG), le *Netherlands' Digital Regulation Cooperation Platform* (SDT), l'*Irish Digital Regulators Group* (DRG) et le *Digital Regulation Cooperation Forum* (DRCF) au Royaume-Uni. Celles-ci s'apparentent à des forums d'échanges entre autorités, sans être réservés aux autorités de protection des données et de concurrence. Ces formes de coopération peuvent être considérées comme les plus avancées. En France, la loi SREN a créé un réseau national de coordination de la régulation des services numériques, qui regroupe des AAI et des services de l'Etat, mais n'empiète pas sur les missions des AAI définies par la loi[78].

En particulier, le DRCF[79] propose au Royaume-Uni une organisation aboutie de coopération entre les autorités de protection des données, de la concurrence, des marchés financiers et des communications. Ainsi, le DRCF produit régulièrement des études, organise des séminaires, ainsi que des conférences et participe à l'élaboration de positions communes de ces membres. Pour fonctionner, ce forum dispose d'une équipe de permanents complétée par des agents des autorités membres. Toutefois, le DRCF n'a pas vocation à se transformer en une structure dotée de pouvoirs propres ni à coopérer sur des cas. Il est destiné à renforcer la cohérence, accroître les collaborations et développer les capacités des autorités membres.

3.4.2 Une structuration efficace avec l'Autorité de la concurrence

Le mécanisme de saisine pour avis entre la CNIL et l'Autorité de la concurrence permet à chaque autorité de saisir l'autre lorsque des situations sont identifiées. Ce mécanisme donne une pleine maîtrise aux autorités pour moduler la fréquence et les sujets des saisines. D'ailleurs, les différents avis rendus par les deux autorités montrent la diversité des possibilités de contributions. De plus, le renforcement de la coopération au travers de cas concrets permet à chaque autorité de mieux comprendre les analyses de l'autre autorité.

En effet, tant l'article R. 463-9 du code de commerce que l'article 15 de la loi n° 2017-55 du 20 janvier 2017 portant statut général des autorités administratives indépendantes et des autorités publiques indépendantes

[76] Article 35.7.a du RGPD.
[77] Article 35.7.b du RGPD.
[78] Nouvel article 7-4 de la loi pour la confiance dans l'économie numérique, modifiée par l'article 51 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique.
[79] Le DRCF est un organisme non statutaire et volontaire créer par le gouvernement britannique. Quatre régulateurs britannique - la CMA, l'ICO, l'Ofcom et la FCA – y contribuent. Il a pour objectif de favoriser la coopération et les échanges entre ces régulateurs. Pour ce faire, cet organisme publie des études, organise des ateliers de travail, des conférences et participe à l'élaboration des position communes.

permettent aux deux autorités d'échanger des informations sur des cas sans être tenues par le secret professionnel envers l'autre autorité.

De fait, l'Autorité de la concurrence a régulièrement mobilisé ce dispositif dans le cadre de ses procédures contentieuses et la CNIL a saisi l'Autorité de la concurrence pour avis pour la première fois en 2023 dans le cadre de son projet de recommandation relatif aux applications mobiles[80]. Les avis ont systématiquement fait l'objet d'une attention particulière des services des deux autorités afin de prendre en compte au mieux les remarques et recommandations ainsi recueillies. Le renforcement de la coopération avec l'Autorité de la concurrence montre également que l'organisation actuelle permet un travail conjoint et que cette coopération peut être accentuée en conservant l'organisation initiale.

En outre, la structuration actuelle est simple et permet d'assurer aux acteurs économiques une lisibilité des actions des deux autorités. Elle assure une cohérence dans la volonté de maintenir une clarté dans les compétences de chaque autorité, tout en prenant en compte les enjeux de l'autre. Par ailleurs, les autorités commencent à bénéficier de l'expérience des saisines et des échanges informels, ce qui permet de faciliter la mise en œuvre du cadre de coopération.

3.4.3 Des possibilités d'approfondissement via un point de contact

Toutefois, sans modifier le cadre existant, des améliorations pourraient être envisagées afin de renforcer l'articulation entre protection des données personnelles et concurrence. Cette coopération doit s'exercer sur trois plans : les concepts, la doctrine et les cas de mise en œuvre[81].

La déclaration conjointe mentionne déjà des « *travaux prospectifs communs* (…) *permettant d'identifier de nouveaux enjeux de régulation nécessitant une convergence* »[82], ce qui couvre le dialogue des concepts et des outils. La déclaration conjointe appelle en effet les deux autorités à « *mieux faire dialoguer les règles de droit dont elles ont respectivement la charge* »[83]. La définition d'un programme de travail annuel en la matière pourrait être envisagée afin d'inciter aux échanges sur ces sujets. Il serait alors nécessaire de définir ce qui permettrait d'animer le débat. De même, sous un angle plus sectoriel ou thématique, des séminaires, ateliers, études conjointes ou réunions d'échanges entre services peuvent être organisés pour stimuler la réflexion. Ces sujets prospectifs s'ajouteraient ainsi à la coopération sur les cas, qui sont soumis aux autorités ou dont elles se saisissent, déjà existante. Enfin, la production d'une communication régulière sur l'état de la coopération entre la CNIL et l'Autorité de la concurrence pourrait permettre de faire un bilan régulier de la coopération, de présenter et expliquer au public et aux entreprises les principaux résultats de la coopération.

Pour être efficace, l'organisation régulière de réunions et travaux communs nécessite de centraliser les besoins et les moyens disponibles. Par conséquent, il pourrait être envisagé de créer au sein de chaque autorité un point de contact chargé du pilotage de la coopération (identification des sujets, coopération interne pour faciliter leur traitement, *reporting*).

Enfin, ni le cadre législatif ni celui de la déclaration conjointe n'explicitent le fonctionnement de la coopération lorsqu'un désaccord survient. À ce stade, il n'existe pas d'obligation pour les deux autorités de converger entièrement et sur tous les points, à condition de pouvoir démontrer qu'elles ont « tenu compte », même partiellement, de l'avis de l'autre autorité sur les points essentiels et que le résultat témoigne d'une convergence globale.

***Proposition n°6** : afin d'approfondir la coopération entre les deux autorités selon trois axes : les concepts, la doctrine et les cas, **instaurer au sein de chaque autorité un point de contact chargé de piloter la coopération**.*

[80] https://www.cnil.fr/fr/applications-mobiles-la-cnil-publie-ses-recommandations-pour-mieux-proteger-la-vie-privee
[81] Autorité de la concurrence et Commission nationale de l'informatique et des libertés, 2023, Concurrence et données personnelles : une ambition commune, p. 13.
[82] Ibid.
[83] Ibid., p. 1.

4 Conséquences opérationnelles pour la CNIL

Pour la CNIL, protéger la vie privée et les données personnelles passe par une meilleure prise en compte des réalités économiques et concurrentielles. Même si le RGPD n'est pas une régulation économique mais relevant des libertés fondamentales, l'angle économique et concurrentiel concourt de manière significative à son effectivité et à son impact.

Par une action volontariste, la CNIL peut contribuer à construire une économie plus favorable à la vie privée et à la protection des données personnelles, qui permettra d'accroître les effets positifs sur les utilisateurs qui sont aussi consommateurs (4.1). Pour ce faire, il est indispensable de développer les capacités de la CNIL à mieux comprendre et déterminer comment intégrer les questions de concurrence dans ses travaux (4.2). Enfin, la prise en compte de certains outils issus de l'analyse concurrentielle pourrait permettre d'améliorer le calcul du montant des sanctions pour lesquelles les pratiques de l'entreprise renforcent son pouvoir économique (4.3).

4.1 Orienter l'économie vers une meilleure prise en compte de la vie privée

4.1.1 La promotion de l'égalité concurrentielle

Les instruments de droit souple (référentiels, recommandations, codes de conduite, etc.) de la CNIL ont pour objectif d'éclairer les acteurs de marché sur les différentes dispositions de la réglementation dans leurs domaines respectifs et leur interprétation. Ils peuvent jouer un rôle déterminant dans la façon dont les entreprises construisent leurs stratégies de collecte et d'utilisation des données personnelles. En tout état de cause, ils permettent d'orienter les entreprises d'un même secteur vers des pratiques plus respectueuses de la vie privée. Ils favorisent donc la mise en place de standards améliorant la protection des données personnelles.

Les codes de conduite et recommandations permettent également d'orienter les comportements des entreprises vers une meilleure intégration de la vie privée dans leurs modèles d'affaires. Leur mise en place peut être un facteur de différenciation important pour une entreprise sur le marché. Ainsi, tout en donnant les moyens de construire des modèles d'affaires ambitieux, ces codes de conduite et recommandations instaurent un cadre concurrentiel plus équitable y compris lorsqu'il existe des capacités asymétriques entre les entreprises. Ils concourent également à la sécurité juridique pour les entreprises.

À titre d'exemple, la recommandation relative aux applications mobiles publiée en septembre 2024 a rappelé aux différents acteurs de ces écosystèmes les obligations qu'ils doivent respecter. Bien que ce marché soit caractérisé par la présence d'acteurs structurants, elle encourage l'ensemble des entreprises à adopter des comportements plus vertueux pour la vie privée et la protection des données personnelles. En outre, elle permet de leur proposer de nombreuses bonnes pratiques qui nécessitent de repenser leurs modèles d'affaires en intégrant davantage la protection des données personnelles.

Aussi, à travers la protection de la vie privée, la CNIL promeut des conditions équitables de collecte et d'utilisation des données personnelles. Ces conditions permettent aux plus petits comme aux plus grands acteurs de bénéficier de conditions d'application de la règlementation similaires. Par ailleurs, la démarche d'accompagnement mise en place par la CNIL à destination de tous les acteurs permet aux entreprises de bénéficier de conditions équitables d'accès au régulateur.

4.1.2 L'innovation

Le rôle de l'innovation pour la concurrence est fondamental. L'innovation peut stimuler la concurrence en incitant les acteurs à créer de nouveaux produits ou services susceptibles d'être appréciés par les consommateurs. Par conséquent, les autorités de concurrence apprécient à la fois la concurrence existante et potentielle lors de leurs évaluations concurrentielles. L'innovation peut être un paramètre déterminant de cette concurrence potentielle en permettant de limiter ou concurrencer l'existence d'un pouvoir de marché ou la domination d'une entreprise sur un marché.

En outre, l'innovation peut également être utilisée « *comme un facteur contrebalançant un pouvoir de marché, comme un moyen de défense justifiant un comportement anticoncurrentiel ou comme un gain d'efficacité* »[84].

[84] OCDE, 15 novembre 2023, Concurrence et innovation - Le rôle de l'innovation dans les affaires d'application du droit de la concurrence – Note de référence, DAF/COMP(2023)12, p. 5.

Ce rôle n'apparaît que dans certaines situations et conditions spécifiques. En effet, certains marchés se caractérisent par un dynamisme important en matière d'innovation, qui peut permettre de concurrencer des entreprises dominantes possédant un pouvoir de marché important. L'histoire de la construction des marchés numériques a montré que ces positions pouvaient justement être rapidement contestées dès lors que des innovations de rupture étaient proposées.

L'introduction du RGPD a constitué une révolution à la fois règlementaire et technique. Par conséquent, si lors des premières années de mise en œuvre du règlement les entreprises se sont attachées à se mettre, pour la plupart, en conformité, de nouvelles opportunités se sont également développées. Ainsi, le RGPD a permis d'accélérer la recherche et l'investissement en matière de conformité RGPD et de protection de la vie privée. De fait, les entreprises ont saisi l'importance de la protection des données personnelles dans leurs modèles d'affaires, puisque la transition vers des modèles plus vertueux nécessite de proposer des solutions innovantes. À ce titre, les investissements de conformité contribuent à l'innovation de manière significative.

Ainsi, en plus d'être un paramètre de concurrence, la protection de la vie privée et des données personnelles est également devenue un moteur de l'innovation dans de nombreux domaines, tel que la cybersécurité, l'informatique en nuage ou l'intelligence artificielle. Aussi, la promotion de la protection de données personnelles concourt à inciter les acteurs à poursuivre leurs innovations. Une promotion plus importante de la vie privée comme paramètre d'innovation permettra de favoriser la contestabilité des marchés. L'exemple du marché de la publicité montre que lorsque la protection de la vie privée est promue, des solutions innovantes peuvent émerger rapidement de la part d'entreprises de toutes tailles, favorisant *de facto* une concurrence plus intense sur le marché. Toutefois, les autorités de protection de la concurrence et des données personnelles doivent coopérer étroitement pour empêcher tout dévoiement de la protection des données ou de la concurrence au détriment de l'un ou de l'autre.

Cela signifie, d'une part, au-delà de la prise en compte en amont des enjeux de concurrence en protection des données (cf. supra), que l'Autorité de la concurrence doit reconnaître la protection de la vie privée comme un objectif légitime dans les modèles d'affaires, mais aussi que la CNIL doit être attentive à l'aider à détecter les comportements de « *privacy washing* ».

4.1.3 Accroître les pouvoirs des personnes : la portabilité

Comme le prévoit l'article 20.1 du RGPD, les utilisateurs « *ont le droit de recevoir les données personnelles les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données personnelles ont été communiquées y fasse obstacle* »[85]. Le droit à la portabilité est donc un droit pour les personnes qui peut s'exercer dans certaines conditions.

Comme le rappelle l'OCDE, les « *mesures prises afin de garantir la portabilité des données et l'interopérabilité peuvent jouer pour promouvoir la concurrence, à la fois au sein des plateformes numériques et entre elles. Ces mesures peuvent en particulier traiter des problèmes de "prise en otage" du consommateur, promouvoir le dégroupage et permettre le multi-hébergement* »[86].

Par conséquent, les mesures favorisant la portabilité peuvent utilement bénéficier à l'utilisateur en lui permettant d'exercer ses droits et en favorisant la concurrence sur les marchés. Une attitude plus ambitieuse permettrait à la fois de donner plus d'effectivité au droit à la portabilité et d'avoir une contribution propre à l'animation de la concurrence, à la lutte contre les effets de « lock-in » (verrouillage) des grands services numériques et de l'innovation dans l'économie.

En particulier, le droit à la portabilité peut être utilisé par les autorités de concurrence comme un moyen de renforcer la contestabilité des marchés dans l'application de l'article 102 TFUE et du contrôle des concentrations.

D'ailleurs, dans le domaine du numérique, la capacité des autorités nationales de concurrence à pouvoir ouvrir des enquêtes dans le cadre du DMA permet de faire davantage le lien entre la promotion d'une plus grande contestabilité des marchés et la protection des données personnelles. En effet, l'article 6.9 du DMA dispose que le « *contrôleur d'accès assure aux utilisateurs finaux et aux tiers autorisés par un utilisateur final, à leur demande et gratuitement, la portabilité effective des données fournies par l'utilisateur final ou générées par l'activité de l'utilisateur final dans le cadre de l'utilisation du service de plateforme essentiel concerné, y*

[85] Article 20.1 du RGPD.
[86] OCDE, 4 janvier 2022, Portabilité des données, interopérabilité et concurrence des plateformes numériques, DAF/COMP(2021)5, p. 2.

compris en fournissant gratuitement des outils facilitant l'exercice effectif de cette portabilité des données, et notamment en octroyant un accès continu et en temps réel à ces données ».

L'utilisateur dispose donc d'un droit à la portabilité à la fois dans le cadre du DMA et du RGPD. Le périmètre du droit à la portabilité du DMA étant plus large que celui du RGPD, il pourrait permettre de protéger l'utilisateur en tenant compte à la fois des données personnelles et du comportement concurrentiel de l'entreprise.

***Proposition n°7** : engager une réflexion commune spécifique concernant le droit à la portabilité des données personnelles, et ses conséquences en matière de protection de données personnelles et de concurrence. Cette réflexion pourra, le cas échéant, impliquer d'autres acteurs ou autorités compétents en matière de portabilité des données personnelles ou d'interopérabilité, tels que l'Arcep et être articulée avec les différents forums existants ou en cours de mise en place (ex : Groupe de haut niveau du DMA, réseau national de coordination de la régulation des services numériques).*

4.2 Mieux prendre en compte en amont la protection de la concurrence

4.2.1 Développer une sensibilisation régulière aux enjeux concurrentiels

Accroître la prise en compte des enjeux concurrentiels dans les travaux de la CNIL passe par une sensibilisation en interne aux problématiques de concurrence. Pour ce faire, des formations internes pourraient être organisées sur des sujets économiques généraux et sur l'analyse concurrentielle, afin de mieux comprendre comment s'articulent les travaux d'une autorité de la concurrence et ce qu'ils peuvent apporter à la CNIL. Des formations croisées entre les agents de la CNIL et de l'Autorité de la concurrence pourraient également être envisagées. Cela permettra de proposer des exemples spécifiques et de partager l'expérience d'enquêtes par exemple.

La CNIL pourrait aussi renforcer ses mécanismes de veille et d'alerte en invitant régulièrement l'Autorité de la concurrence à présenter les décisions et travaux les plus pertinents pour la CNIL. Ces veilles et alertes pourraient être complétées par une présentation régulière des principaux travaux passés, en cours et à venir des deux institutions.

Les sujets concurrentiels ayant des aspects en lien avec la protection des données personnelles pourraient également être plus régulièrement communiqués en séance plénière de la CNIL. La synthèse d'un avis ou d'une décision de l'Autorité de la concurrence ou de la Commission européenne, lorsqu'ils ont trait aux données, comportent régulièrement des enjeux voire des conséquences en matière de vie privée ou de protection des données personnelles. Le collège pourrait donc bénéficier utilement d'un éclairage.

De plus, il est déterminant pour la CNIL de continuer à s'interroger sur les conséquences économiques des décisions avec une vision à la fois *ex-post* et *ex-ante*. En effet, l'intégration dans les travaux de la CNIL des enjeux concurrentiels et économiques permettrait de mieux prendre en compte les effets potentiels des décisions ou recommandations de la CNIL. Parmi les points à vérifier lors de ces études d'impact, figure l'impact concurrentiel de la décision ou de la direction de doctrine retenue, afin que le processus décisionnel se déroule à ce sujet en toute connaissance de cause.

***Proposition n°8** : **organiser régulièrement des formations croisées** aux enjeux de concurrence et de protection des données à destination des deux autorités.*

4.2.2 Approfondir l'intégration de l'économie dans les travaux de la CNIL

Un des bénéfices premiers d'une plus grande intégration des enjeux concurrentiels dans les travaux de la CNIL est de pouvoir mieux appréhender le contexte économique et de marché dans lequel se situent les entreprises concernées. Pour bénéficier pleinement des analyses concurrentielles, la CNIL doit avoir au préalable connaissance des principaux enjeux économiques pour une entreprise et du ou des marchés sur le(s)quel(s) elle est active. Aussi, la poursuite des analyses des modèles d'affaires en interne est-elle indispensable. En effet, la CNIL devrait pouvoir se faire une première opinion avant d'intégrer le cas échéant d'autres analyses (provenant de l'industrie ou d'un régulateur économique) dans ses travaux. L'intégration des analyses de modèles d'affaires et plus généralement du contexte économique de l'entreprise devrait donc être renforcée dans les travaux de la CNIL.

L'utilisation de l'analyse économique devrait aussi permettre d'améliorer l'identification des zones à explorer pour la CNIL. À titre d'exemple, l'émergence de nouveaux modèles d'affaires, l'évolution d'un secteur économique, l'utilisation d'une nouvelle technologie plus rentable, peuvent conduire à transformer les usages

en matière de données personnelles. Dans certaines situations, ces changements peuvent générer une modification des risques pour la protection des données personnelles. Il appartient à la CNIL d'être en capacité de les détecter, voire de les anticiper, pour mettre en place les recommandations nécessaires et maintenir une vigilance accrue sur ces sujets.

Enfin, une expertise économique en matière de marchés et de modèles d'affaires, qualitative mais aussi quantitative, est indispensable en interne afin de bien comprendre l'impact d'une décision à venir (sur un acteur et sur le marché correspondant) ou d'une direction de doctrine (résultant d'un acte de droit souple ou de la réponse à une demande de conseil).

4.3 Préciser notre approche proportionnelle en matière de sanctions

4.3.1 Des outils similaires mais différents

L'intégration de la position de marché dans le mécanisme de sanction de la CNIL doit être réalisée avec précaution. En effet, le pouvoir de sanction confié à l'Autorité de la concurrence a pour objectif de « *prévenir et de réprimer les pratiques anticoncurrentielles, qui peuvent avoir un impact considérable sur l'économie* »[87]. Il couvre également l'ensemble des contentieux en matière de concentrations, y compris les manquements dans les phases de procédure. En revanche, la CNIL peut engager une procédure de sanction en cas de manquement au RGPD ou à la loi Informatique et Libertés. Elle s'attache à l'impact qu'ont les pratiques reprochées sur l'ordre public de la protection des données et la préservation de droits fondamentaux. Ces mécanismes ne visent donc pas les mêmes objectifs.

Néanmoins, les autorités disposent toutes les deux d'une capacité à proportionner le montant de leurs amendes au cas par cas et disposent d'une variété de possibilités (publicité de la sanction, mise en demeure, injonction, etc.). En revanche, concernant le calcul du montant des sanctions, les critères diffèrent mais peuvent parfois se croiser lorsqu'il s'agit de prendre en compte la capacité financière d'une entreprise par exemple. Toutefois, le calcul de la sanction ne peut pas reposer sur les mêmes règles, puisqu'en droit de la concurrence, le point de départ est la valeur du préjudice causé « au marché »[88]. Or, de nombreuses sanctions de la CNIL ne permettent pas de raisonner en termes de valeur du marché affecté, car ces pratiques n'ont pas pour objet ou pour effet de renforcer le pouvoir de marché d'une entreprise. Le raisonnement s'attachera plutôt, d'un point de vue économique, au bénéfice tiré du manquement ou aux dommages et préjudices individuels.

En revanche, la position de marché du mis en cause, lorsqu'elle se traduit par un pouvoir sur les données, peut aggraver l'une ou l'ensemble des composantes des préjudices résultant d'une violation du RGPD : bénéfices tirés du manquement, préjudices aux personnes, préjudice pour la société. Il pourrait donc être opportun d'identifier quels éléments objectifs en la matière, structurels ou comportementaux, constatables empiriquement, permettent de mieux appréhender la formation ou la capacité d'une entreprise à porter préjudice à un nombre important d'utilisateurs.

Ainsi, comme en concurrence, le calcul du montant des sanctions en protection des données peut donc reposer sur un ensemble d'éléments économiques objectifs.

4.3.2 Identifier et s'approprier des paramètres concurrentiels aggravants

Même si la position dominante ou le pouvoir de marché de l'entreprise sont des notions ancrées dans le contexte d'évaluation d'une autorité de concurrence, ils peuvent être adaptés dans le cadre de l'analyse des facteurs à prendre en compte pour calculer une amende en protection des données. D'ailleurs, le k du 2 de l'article 83 du RGPD précise que « *toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce* »[89] doit être prise en compte pour en déterminer le montant. Ainsi, lorsqu'une entreprise dispose d'une capacité à collecter et exploiter de vastes ensembles de données par exemple, c'est-à-dire d'un pouvoir des données (*data power*[90]), celle-ci pourrait constituer une circonstance aggravante. En effet, dans le cadre d'une violation des règles du RGPD, cette capacité pourrait permettre à l'entreprise de causer des dommages plus importants et donc d'en accentuer la gravité. Ce pouvoir sur les données pourrait notamment provenir d'une position dominante sur le marché et donc d'un accès privilégié à un vaste ensemble des données personnelles,

[87] https://www.autoritedelaconcurrence.fr/fr/competence-contentieuse.
[88] https://www.autoritedelaconcurrence.fr/sites/default/files/Communique_sanction.pdf.
[89] Article 83.2 point k du RGPD.
[90] Klaudia Majcher, "Coherence between data protection and competition law in digital markets", Oxford data protection and privacy law series, Oxford UP, 2023.

d'effets de réseau désincitant les consommateurs à changer de fournisseur au profit de la concurrence ou d'effets de gamme permettant de combiner aisément des jeux de données entre eux.

D'autres éléments pouvant caractériser des circonstances aggravantes pourraient être utilisés par la CNIL : c'est le cas notamment des décisions de l'Autorité de la concurrence visant à sanctionner une entreprise pour des pratiques anticoncurrentielles. S'il ne relève pas du même cadre, un comportement non conforme au droit de la concurrence pourrait alerter la CNIL sur les moyens à disposition de l'entreprise pour mettre en place ces pratiques. Si une entreprise est capable de mettre en place des mécanismes pouvant avoir un effet sur ses concurrents, elle pourrait également être en capacité de mettre en place une stratégie visant les utilisateurs qui aurait des conséquences néfastes sur leur vie privée. Le pouvoir de marché de l'entreprise, qui lui permet d'influencer les conditions dans lesquelles les affaires sont menées sur un marché donné, et se traduit en protection des données par un pouvoir sur les données, pourrait donc être déterminant dans l'appréciation des capacités de l'entreprise à pouvoir agir positivement ou négativement pour la protection de la vie privée et des données personnelles sur le même marché et évaluer le rôle (positif, négatif ou neutre) de cette entreprise en la matière.

L'existence d'accords entre entreprises, qu'ils soient conformes au droit de la concurrence ou non, pourrait également donner une indication sur l'augmentation potentielle des risques pour la protection des données personnelles. En effet, dans certaines situations, les accords peuvent conduire à la combinaison de données personnelles. D'ailleurs, le DMA confirme cette approche, même si son champ d'application est restreint aux contrôleurs d'accès. Ainsi les accords entre entreprises peuvent-ils avoir pour objet d'échanger ou combiner des données personnelles, accroissant alors les risques pour les personnes. En outre, ce type d'accords pourrait être un indice qu'il s'agit d'une des « *opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (Art. 35.4 du RGPD)* »[91].

4.3.3 Mieux proportionner les sanctions au comportement de l'entreprise

L'examen du principe de proportionnalité lors de la phase d'étude du montant d'une amende de la CNIL peut, dans des circonstances particulières, minorer le montant final. Pour ce faire, l'autorité doit tenir compte des risques concernant la viabilité de l'entreprise et sa capacité à payer en tenant compte du contexte social et économique dans lequel elle se situe[92]. La CNIL pourrait utilement s'appuyer sur les analyses concurrentielles existantes pour identifier si des preuves objectives de détérioration ou d'amélioration du secteur économique dans lequel se trouve l'entreprise existent. Les enquêtes sectorielles réalisées par l'Autorité de la concurrence, ainsi que les analyses menées au sein de ses décisions[93] constituent ainsi des éléments mobilisables rapidement par la CNIL dans le cadre défini par l'arrêt Meta Platforms, précité.

En outre, la CNIL pourrait renforcer la prise en compte de la notion d'entreprise au sens du droit de la concurrence dans ses procédures de sanction. Cela permettrait de mieux proportionner les sanctions aux capacités financières de l'entreprise. En effet, la CJUE définit, dans le cadre d'affaires en matière de concurrence, la notion d'entreprise comme « tou*te entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement* »[94]. Dans son arrêt C-807/21, elle précise qu'une entité désigne une « *unité économique même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales. Cette unité économique consiste en une organisation unitaire d'éléments personnels, matériels et immatériels poursuivant de façon durable un but économique déterminé* »[95]. La Cour considère donc que « *dans le cas où le destinataire de l'amende administrative est ou fait partie d'une entreprise, au sens des articles 101 et 102 TFUE, le montant maximal de l'amende administrative est calculé sur la base d'un pourcentage du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise concernée* »[96]. Cet arrêt permet la mise en cause d'une filiale européenne responsable de traitement, tout en faisant porter l'appréciation économique sur le calcul de la sanction sur la société mère

---

[91] CNIL, Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.
[92] CEPD, 24 mai 2023, Lignes directrices 04/2022 sur le calcul des amendes administratives au titre du RGPD, pp. 45-46.
[93] À titre d'exemple, la CNIL avait pris en compte, dans sa décision de sanction du 7 décembre 2020 concernant Google (paragraphe 124 à 127), le point 313 de la décision n° 19-D-26 du 19 décembre 2019 de l'Autorité de la concurrence concernant Google Search.
[94] CJUE, aff. C-807/21, 5 déc. 2023, Deutsche Wohnen SE contre Staatsanwaltschaft Berlin, pt 56.
[95] Ibid.
[96] Ibid., point 57.

(remontée des bénéfices dans les bilans, plafond de chiffre d'affaires applicable, soutien en capital en cas de difficulté, etc).

D'ailleurs, la méthode de détermination des sanctions pécuniaires mise à jour en 2011 par l'Autorité de la concurrence, et modifiée en 2021, sans être transposable, peut être une source d'inspiration pour réfléchir aux moyens mobilisables par la CNIL[97]. Elle permet de bénéficier de l'expérience en matière de détermination des sanctions pécuniaires des autorités de concurrence, en renseignant utilement sur les éléments retenus pour apprécier la gravité des faits, tels que la nature de l'infraction, des activités des personnes susceptibles d'être affectées ou la connaissance infractionnelle de la pratique.

Enfin, l'analyse concurrentielle pourrait permettre de mieux appréhender la nécessité d'utiliser l'effet réputationnel comme une élément de dissuasion. En effet, l'article 22 de la loi informatique et libertés précise que « *la formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne, aux frais des personnes sanctionnées* »[98]. Ainsi, à titre d'exemple, lorsque l'analyse concurrentielle montre que les pratiques et/ou décisions de l'entreprise mise en cause peuvent avoir un effet sur les choix des concurrents, alors la publication de la sanction pourrait permettre de renforcer son effet dissuasif.

Proposition n°9 : mieux proportionner les sanctions au comportement de l'entreprise en faisant de ce dernier, le cas échéant, un facteur aggravant *de la sanction au titre de l'article 83.2 k) RGPD : majoration des bénéfices tirés du manquement, accroissement de gravité des dommages aux personnes, effet écosystémique éventuellement négatif de l'entreprise.*

5 Conséquences pour la coopération avec l'Autorité de la concurrence

Comme l'illustre l'exemple du *Bundeskartellamt* (autorité de la concurrence allemande), le renforcement de la coopération entre les deux autorités pourrait être l'occasion pour l'Autorité de la concurrence d'enrichir les méthodes d'analyse concurrentielles, à la lumière des dernières avancées doctrinales, notamment lorsque des données personnelles sont concernées Le concours de la CNIL pourrait permettre de faciliter l'identification et la compréhension des pratiques des acteurs en la matière. Cela nécessite de renforcer les possibilités de coopération et de proposition de la CNIL vis-à-vis de l'Autorité de la concurrence (5.1). La déclaration conjointe signée par la CNIL et l'Autorité de la concurrence en décembre 2023 permet d'ores et déjà de fixer un cadre de coopération renforcé, qu'il conviendrait de préciser en pratique (5.2). En particulier, un apport de la CNIL dans l'analyse des engagements comportementaux et structurels adéquats, ou encore une réflexion conjointe sur les programmes de conformité des entreprises pourraient permettre à l'Autorité de la concurrence de prendre davantage en compte la protection des données personnelles (5.3).

5.1 Assister l'Autorité de la concurrence dans ses enquêtes et décisions liées à la protection des données

5.1.1 La définition du marché pertinent

Le marché pertinent correspond au(x) marché(s) en cause aux fins de l'application du droit de la concurrence. Il permet à la Commission européenne « *d'identifier et de délimiter le périmètre à l'intérieur duquel s'exerce la concurrence entre les entreprises. La définition du marché vise principalement à identifier de manière systématique les contraintes concurrentielles effectives et immédiates auxquelles sont confrontées les entreprises concernées lorsqu'elles proposent des produits donnés sur un territoire donné* »[99]. Elle permet donc

[97] Autorité de la concurrence, 30 juillet 2021, Communiqué de l'Autorité de la concurrence relatif à la méthode de détermination des sanctions pécuniaires.
[98] Article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[99] Commission européenne, 22 février 2024, Communication de la Commission sur la définition du marché en cause aux fins du droit de la concurrence de l'Union, C/2024/1645, point 6.

« *d'identifier les concurrents concernés de l'entreprise ou des entreprises en question lorsqu'elles proposent ces produits ainsi que les clients concernés. Seuls les produits qui exercent des contraintes concurrentielles effectives et immédiates au cours de la période considérée font partie du même marché en cause que ceux de la ou des entreprises concernées, tandis que d'autres contraintes moins effectives, ou simplement potentielles, sont considérées comme faisant partie de l'appréciation concurrentielle* »[100] .

Ainsi la Commission définit-elle « *généralement le marché en cause dans les cas où il importe d'évaluer la capacité concurrentielle relative des entreprises* »[101]. La définition des marchés pertinents est donc une étape cruciale dans les affaires concurrentielles, que ce soit pour la qualification de pratiques anticoncurrentielles ou le contrôle des concentrations.

La méthodologie, les principaux critères et éléments de preuve sur lesquels se fondent les marchés en cause ont été actualisés en 2024 afin de tenir compte des évolutions qui se sont produites au cours des vingt dernières années, telles que « *la numérisation de l'économie et des nouveaux modes de fourniture des biens et des services, ainsi que de la nature de plus en plus interconnectée et mondialisée des échanges commerciaux* »[102]. Cette actualisation s'inscrit dans un objectif de contribution de la politique de concurrence à la double transition écologique et numérique et à la résilience du marché unique en maintenant le bon fonctionnement des marchés et remédiant à leurs défaillances.

Dans ce contexte, les orientations actualisées de la notice sur les marchés pertinents incluent la prise en compte de paramètres de concurrence qualitatifs. En particulier, lorsqu'elle définit le marché en cause, « *la Commission tient compte des différents paramètres de la concurrence que les clients considèrent comme pertinents sur le territoire et la période évalués. Ces paramètres peuvent inclure le prix du produit, mais aussi son degré d'innovation et sa qualité sous différents aspects* »[103], tel que la protection de la vie privée offerte. En effet, l'essor des modèles d'affaires centrés sur la collecte et l'utilisation de données met en exergue la nécessité de prendre en compte la protection de la vie privée et des données personnelles dès la définition du marché pertinent.

Aussi, sa prise en compte permettra d'améliorer la définition des marchés de produits et des marchés géographiques, en mettant en évidence les différentes segmentations des marchés en cause par exemple.

En particulier, ces considérations trouvent une pertinence accrue « *dans les cas impliquant des produits et services numériques, technologiques ou de communication, où les données des consommateurs font partie du produit* »[104]. D'ailleurs, « *dans l'affaire Microsoft/LinkedIn, la Commission a pris en compte les exigences en matière de protection de la vie privée et le cadre réglementaire relatif à la protection des données dans l'évaluation de la définition du marché géographique. L'enquête de la Commission a mis en évidence des différences dans les exigences réglementaires et de protection de la vie privée entre les pays de l'EEE, que les parties prenantes considèrent comme des exemples de différences dans la fourniture de services de réseaux sociaux dans l'EEE* »[105]. En effet, dans ce cas, certaines parties prenantes considéraient la protection de la vie privée comme un élément déterminant pour comprendre les exigences locales des clients, puisque les règles en matière de protection de la vie privée varient en fonction du pays.

Le cas échéant, si les marchés dans lesquels opèrent les entreprises concernées n'ont pas fait l'objet d'une publication de doctrine par la CNIL, les bonnes pratiques actuelles amènent l'Autorité de la concurrence à contacter la CNIL. À l'instar des échanges informels tenus entre les deux autorités lors de l'examen du projet de fusion TF1/M6, de premiers échanges informels permettent d'identifier les traitements de données personnelles existants. S'il y a lieu, une demande d'avis peut également être formulée afin de bénéficier d'une analyse complète des traitements des entreprises concernées.

5.1.2 Le contrôle des concentrations

Au sein de l'Union européenne, le contrôle des concentrations se définit comme tout changement durable du contrôle des entreprises concernées par l'opération qui résulte « *de la fusion de deux ou de plusieurs entreprises ou parties de telles entreprises, ou de l'acquisition, par une ou plusieurs personnes détenant déjà le contrôle*

---

[100] Ibid.
[101] Ibid, point 8.
[102] Ibid, point 3.
[103] Ibid., point 15.
[104] Commission européenne, Non-Price Competition: EU Merger Control Framework and Case Practice, Competition Policy brief, p. 6.
[105] Ibid.

d'une entreprise au moins ou par une ou plusieurs entreprises, du contrôle direct ou indirect de l'ensemble ou de parties d'une ou de plusieurs autres entreprises, que ce soit par prise de participations au capital ou achat d'éléments d'actifs, contrat ou tout autre moyen »[106]. Le contrôle a pour objectif d'établir la compatibilité de ces opérations avec le maintien d'une concurrence suffisante sur les marchés affectés.

En particulier, les « *concentrations qui entraveraient de manière significative une concurrence effective dans le marché commun ou une partie substantielle de celui-ci, notamment du fait de la création ou du renforcement d'une position dominante, doivent être déclarées incompatibles avec le marché commun* »[107].

En outre, la Commission européenne considère la protection des données personnelles et de la vie privée comme un paramètre de concurrence qui peut être « *particulièrement important dans les fusions des industries numériques et technologiques, où les entreprises utilisent les données collectées auprès des clients/utilisateurs à des fins commerciales. À ce titre, les données qu'une entreprise contrôle sont devenues, dans certains secteurs, un moteur essentiel de la concurrence et une source d'avantage concurrentiel* »[108]. Le développement des modèles d'affaires fondés sur l'exploitation et la collecte des données personnelles renforce la nécessité de considérer la vie privée comme un paramètre concurrentiel de plus en plus important.

Par ailleurs, « *la vie privée peut être un élément important de la qualité d'un produit ou d'un service offert et donc un paramètre de la concurrence entre les parties à la concentration et leurs rivaux, ainsi qu'un élément de différenciation* »[109]. Ainsi, même si la protection des données personnelles – et de la vie privée – relève de la réglementation éponyme, le contrôle des concentrations peut y trouver des éléments d'évaluation très précieux.

Le nombre de projets de concentrations fondés sur les données s'est accru, ce qui a conduit la Commission à évaluer dans quelle mesure des entreprises se faisaient « *concurrence en matière de respect de la vie privée et si l'opération pourrait avoir une incidence négative sur la concurrence liée à la protection de la vie privée* »[110]. L'affaire Apple/Shazam illustre le rôle que peut avoir la protection de la vie privée comme élément important de la concurrence entre des fournisseurs de services de diffusion de musique en continu. L'affaire Microsoft/LinkedIn montre également que la protection de la vie privée est un « *paramètre important de la concurrence et un moteur du choix des clients sur le marché des services de réseaux sociaux professionnels* »[111]. La protection de la vie privée a notamment été utilisée pour évaluer l'impact de pratiques potentielles de verrouillage du marché suite à l'opération.

En outre, le renforcement de la prise en compte du dommage à le vie privée, créé tant par des facteurs structurels que comportementaux, (notamment mais pas exclusivement, lorsque les modèles d'affaires à fusionner sont hétérogènes dans leur valeur ajoutée à la vie privée, lorsque la concentration accroît l'échelle des traitements ou les possibilités de combinaison des données, ou encore lorsque la concertation apparaît motivée par la volonté d'acquérir la maîtrise de jeux de données) pourrait permettre de mieux appréhender les dommages potentiels à l'économie. De même, une évaluation relative des niveaux de conformité RGPD des entités en cause permettrait de faire des recommandations pour éviter les risques d'abaissement du niveau global de conformité du nouvel ensemble.

Par ailleurs, la vie privée pourrait également être étudiée en tant que gain d'efficacité probable résultant de la concentration. Ainsi, une conformité au RGPD ou une amélioration de la prise en compte de la vie privée pour les utilisateurs permet d'améliorer la qualité des produits. Ces effets pourraient également, dans certains cas, être pris en considération dans l'analyse des éléments contrebalançant les effets négatifs de la concentration.

De plus, le contrôle des concentrations peut permettre de protéger les entreprises pionnières dans le domaine de la protection de la vie privée. En effet, ces entreprises plus petites et disposant de moins de ressources sont capables de faire concurrence par la qualité de leurs offres notamment en termes de protection de la vie privée[112]. L'acquisition d'une entreprise de cette catégorie pourrait permettre à une grande entreprise de privilégier ses propres produits tout en ayant la capacité de limiter, voire en supprimer, la diffusion des innovations de l'entreprise pionnière. Dans cette situation, le contrôle des concentrations aurait la capacité de protéger à la fois la concurrence et la vie privée des consommateurs. Toute stratégie de vigilance en matière d'acquisitions

---

[106] Article 3.a et 3.b du Règlement (CE) n° 139/2004 du Conseil du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises (« le règlement CE sur les concentrations »), Journal officiel n° L 024 du 29/01/2004, p. 0001 – 0022.
[107] Article 2.3 du règlement CE sur les concentrations.
[108] Commission européenne, Non-Price Competition: EU Merger Control Framework and Case Practice, Competition Policy brief, p. 11.
[109] Ibid.
[110] Ibid, p. 12.
[111] Ibid.
[112] OCDE, 16 juin 2023, Theories of harm for digital mergers – Background Note, DAF/COMP(2023)6, p. 1-51.

prédatrices devrait donc comporter une composante de mesure du risque pour la vie privée et les données personnelles.

Aussi la prise en compte de la protection de la vie privée est-elle déterminante dans de nombreux cas d'évaluation de projets de concentration. La méthodologie permettant cette prise en compte est encore en construction et dépendra aussi de potentiels contentieux. Mais d'ores et déjà, il paraît indispensable de construire une méthodologie cohérente d'évaluation de la vie privée comme paramètre concurrentiel. Le concours de la CNIL en la matière peut permettre à l'Autorité de la concurrence de mieux identifier les comportements non conformes ou problématiques du point de vue de la protection des données personnelles, afin de les prendre plus facilement en compte dans ses évaluations.

Enfin, certains projets de concentration pourraient nécessiter une analyse plus approfondie de l'importance des données personnelles pour les parties à la concentration. Il pourrait s'agir par exemple de la combinaison de données personnelles, d'accès à des données sensibles, etc. Un avis de la CNIL permettrait de contribuer à une amélioration de la compréhension des effets de la concentration potentielle sur le marché. Aussi, le recueil de l'avis de la CNIL pourrait être envisagé lors des phases d'analyse de projets de concentrations. Ces échanges pourront être favorisés dans le cadre de l'instruction par l'Autorité de la concurrence de certaines procédures d'examen approfondi (« phase 2 »), qui sont de nature à présenter des problématiques plus complexes en termes d'analyse de la dynamique concurrentielle. Les délais de traitement prévus par la loi pour ces procédures (65 jours ouvrés supplémentaires au-delà des 25 ouvrés de la phase d'examen rapide « phase 1 ») offrent une possibilité plus importante de mener des discussions constructives entre la CNIL et l'Autorité de la concurrence si nécessaire, y compris des échanges informels portant spécifiquement sur les remèdes si le dossier s'y prête.

Proposition n°10 : encourager une saisine de la CNIL, à titre formel ou informel, lorsque la vie privée et les données personnelles sont en jeu dans un dossier de concentration*, en particulier en cas de procédure d'examen approfondi (phase 2).*

5.1.3 Les pratiques anticoncurrentielles (*antitrust*)

Le Traité sur le fonctionnement de l'Union européenne interdit également les pratiques anticoncurrentielles (*antitrust*) que ce soit sous forme d'accords et de pratiques commerciales (article 101)[113] ou d'abus de position dominante[114].

L'article 101 interdit les accords ou ententes par lesquelles des entreprises restreignent ou faussent le jeu de la concurrence. « *Les ententes peuvent être horizontales (entre des concurrents au même niveau de la chaîne d'approvisionnement fixant des prix ou limitant la production) ou verticales (par exemple entre un fabricant et un distributeur). Toutefois, l'article 101, paragraphe 3, autorise les accords restrictifs s'ils génèrent plus d'effets positifs que d'effets négatifs (par exemple s'ils améliorent la production ou la distribution d'un produit)* »[115].

En outre, l'article 102 « *interdit aux entreprises d'abuser de leur position dominante (détenant une part de marché importante) en pratiquant des prix exagérément bas afin d'empêcher d'autres concurrents de pénétrer le marché ou en exerçant une discrimination entre partenaires commerciaux* »[116].

En application de ces deux articles, la Commission et les autorités nationales de concurrence peuvent infliger des amendes aux entreprises participant à ce type de pratique.

L'intégration de la protection de la vie privée dans l'analyse des pratiques anticoncurrentielles trouve particulièrement à s'appliquer dans les situations d'abus de position dominante. En particulier dans le domaine du numérique, les possibilités offertes par l'exploitation de bases de données massives peuvent inciter, dans certains cas, à combiner différentes bases de données comportant des données personnelles. Les avantages concurrentiels conférés par la détention de telles bases de données ont également un effet incitatif sur le comportement des entreprises en matière de collecte et d'exploitation des données.

Dès lors, ces pratiques pourraient être constitutives d'un abus si elles ont pour objectif, même secondaire, de limiter la concurrence effective sur le marché. En particulier, les données personnelles peuvent permettre de rendre suffisamment unique une base de données pour constituer potentiellement une barrière à l'entrée ou à réduire la contestabilité du marché. Le respect du RGPD peut alors être déterminant pour identifier si

[113] Article 101 du TFUE.
[114] Article 102 du TFUE.
[115] Office des publications de l'Union européenne, 24 mars 2017, Synthèses de la législation de l'UE – Antitrust.
[116] Ibid.

l'entreprise a, en plus d'avoir commis un potentiel abus de position dominante, bénéficié d'un avantage indu conféré par une collecte et/ou une exploitation non conforme au règlement sur la protection des données, et si ces deux manquements se recoupent. Ainsi, dans ce cas de figure également, des échanges informels portant spécifiquement sur les remèdes seraient utiles si le dossier s'y prête.

En outre, bien que pouvant, sous certaines conditions, être conforme au RGPD, la mise en commun de données personnelles pourrait permettre à des entreprises de s'échanger des informations déterminantes sur leurs clients respectifs, même si les travaux de la CNIL encouragent les acteurs à se conformer également au droit de la concurrence. Ce type de pratique pourrait alerter l'Autorité de la concurrence, notamment si elle constate des formes d'alignement dans les pratiques – commerciales ou de prix par exemple – ou des stratégies d'évitement[117].

D'ailleurs, ces ententes entre entreprises sur les conditions de collecte ou de partage des données, visant à organiser un défaut de conformité au RGPD ou aboutissant à dégrader le respect de la vie privée sur un marché donné, si elles ne sont pas poursuivies par l'Autorité de la concurrence au titre de l'antitrust, pourraient constituer un facteur aggravant dans le cadre d'une procédure de sanction de la CNIL.

***Proposition n° 11** : encourager une **saisine de la CNIL, à titre formel ou informel, lorsque la mise en commun ou la combinaison de bases de données sont en jeu dans un dossier d'antitrust**, afin d'examiner si d'éventuelles non conformités au RGPD en la matière, même motivées par une recherche d'efficacité, ne constitueraient pas un abus de position dominante.*

5.2 Une mise en pratique de la déclaration conjointe

5.2.1 La fréquence des échanges informels

Pour de nombreux travaux de la CNIL, telles que les notes internes, communications, recommandations, etc., un éclairage concurrentiel permet de mieux comprendre le secteur et l'écosystème dans lequel évoluent les acteurs concernés. Néanmoins, la saisine formelle pour avis ne doit pas être une solution systématique pour l'ensemble des travaux de la CNIL. C'est le cas, lorsque les travaux correspondent à des notes internes ou à des communications au collège de la CNIL. En effet, le processus de saisine est plus rigide que des échanges informels. En particulier, ces derniers permettent d'obtenir de nombreuses informations rapidement.

Ainsi, lors des premières phases d'analyse, des échanges informels avec les services de l'Autorité de la concurrence permettraient d'améliorer la connaissance d'un secteur. La CNIL et l'Autorité de la concurrence pourraient réfléchir à une grille permettant d'identifier les moments où des échanges devraient être probablement envisagés. Lorsque ces échanges font ressortir des enjeux et des problématiques plus importantes nécessitant des avis croisés, ils devraient permettre de faciliter l'expression d'un besoin de saisine.

L'accroissement de ces échanges informels pourrait augmenter le nombre de demandes émanant de services différents. Par conséquent, il apparaît important de faciliter la relation entre les services de la CNIL et de l'Autorité de la concurrence afin de garantir une pleine utilisation de ces échanges. Pour ce faire, les deux institutions pourraient créer un point d'entrée unique afin de faciliter la mise en contact avec les services adéquats et la répartition des dossiers. Ce point de contact aurait une fonction de pilotage et de programmation des échanges entre services concernés, en identifiant en le plus amont possible quels échanges seraient nécessaires et sur quels thèmes. Ce point d'entrée aurait aussi la capacité de pouvoir répondre aux questions générales – étude en cours, calendrier de travaux, etc. – rapidement et de mieux comprendre les informations dont les services demandeurs ont besoin (cf. proposition n°6).

5.2.2 La fréquence des saisines pour avis

L'Autorité de la concurrence est à l'origine de plusieurs saisines de la CNIL pour avis. La première saisine de l'Autorité de la concurrence par la CNIL a, elle, eu lieu en 2023 dans le cadre de la recommandation sur les applications mobiles. Un accroissement de la fréquence des avis pourrait donc être envisagé sans que cette possibilité ne soit systématisée compte tenu de la charge de travail que représente la production d'un avis. Toutefois, cet accroissement suppose d'initier une réflexion conjointe sur la manière dont les délais de réponse aux saisines pourraient être optimisés pour satisfaire au mieux les rythmes de régulation des deux autorités.

[117] Eymas F. et Bensebaa F. (2021), Petits distributeurs indépendants : de l'évitement à l'indifférence concurrentielle ?, Finance Contrôle Stratégie, 24(3), https://doi.org/10.4000/fcs.8258.

En particulier, une augmentation de la fréquence d'utilisation de ces avis permettra de développer une culture commune de saisine qui en facilitera l'utilisation. De manière identique à l'intégration des commentaires de l'Autorité de la concurrence dans la recommandation sur les applications mobiles, l'Autorité de la concurrence pourrait faciliter le développement de cette culture commune en rédigeant avec la CNIL un document public expliquant comment l'avis de la CNIL a été pris en compte dans ses propres avis.

L'augmentation de la fréquence des avis passe également par une meilleure identification des sujets adéquats. Leur détection pourrait être facilitée par la construction d'une grille permettant de détecter quand une saisine serait potentiellement utile. Ce document pourrait être coconstruit par l'Autorité de la concurrence et la CNIL. Il pourrait également intégrer la grille sur les échanges informels précédemment proposée (cf. pt 5.2.1).

5.2.3 Construire une réflexion commune

Le développement des analyses croisées prenant en compte la concurrence et la protection des données personnelles nécessite également de faire se rencontrer les travaux et réflexions de la CNIL et de l'Autorité de la concurrence. Si des ateliers de réflexion ont déjà eu lieu ponctuellement, les deux autorités pourraient mettre en place des ateliers réguliers sur des thèmes d'actualité. Ils permettraient de réunir des agents de la CNIL et de l'Autorité de la concurrence sur des sujets définis à l'avance. Ces ateliers se dérouleraient à tour de rôle dans les locaux de la CNIL, puis dans ceux de l'Autorité de la concurrence, avec deux animateurs provenant chacun d'une autorité différente. Ils permettraient d'accroître la connaissance et la compréhension des analyses des services de l'autre autorité sur un sujet d'intérêt commun. Ils donneraient lieu à un relevé de conclusion opérationnel permettant d'enrichir la doctrine des deux autorités sur les questions retenues.

En complément de ces ateliers réguliers, un séminaire « concurrence et données personnelles » pourrait être organisé à moyen terme. Il permettrait de communiquer et d'échanger sur l'évolution des décisions, documents et travaux sur cette question. Il serait l'occasion de réunir les agents des autorités, ainsi que des personnalités du monde académique, économique et de la société civile. De manière identique aux ateliers internes, cet évènement serait coorganisé par la CNIL et l'Autorité de la concurrence. Le concours d'une université pourrait être envisagée, ainsi qu'une rotation du lieu de l'évènement.

Proposition n°12 : capitaliser sur la coopération en matière de doctrine *en rédigeant des relevés de conclusions opérationnels lors des ateliers internes, systématiser les documents de restitution au public de la manière dont les avis croisés ont été intégrés et en organisant à intervalles réguliers des événements de type académique sur les sujets « concurrence et protection des données ».*

En outre, lorsque des sujets d'intérêt commun ont été identifiés par les deux autorités. La CNIL et l'Autorité de la concurrence pourraient réaliser des études thématiques communes. Ces études thématiques pourraient être complétées par des auditions conjointes volontaires, ne nécessitant pas la mobilisation des pouvoirs d'enquête de l'Autorité (cf. proposition 5 supra). En particulier, lorsque des éléments relatifs au RGPD sont identifiés, la contribution des services de la CNIL devrait pouvoir permettre de faciliter le travail de l'Autorité de la concurrence, y compris pour déterminer si la CNIL doit être saisie pour avis.

5.3 Réflexion sur les outils alternatifs à la sanction

5.3.1 Les engagements comportementaux

L'article L. 464-2 du code de commerce et l'article 9 du règlement 1/2003 précisent que des engagements peuvent être pris par les entreprises pour mettre fin aux pratiques anticoncurrentielles existantes. Il s'agit alors pour les autorités de concurrence de rendre ces engagements obligatoires pour les entreprises. Cette procédure permet à l'entreprise de proposer des solutions adaptées à leur modèle d'affaires, tout en permettant aux autorités de diminuer les coûts de négociation et la durée des procédures[118].

Plusieurs types d'engagements peuvent être pris. Néanmoins, ils sont dépendants de la nature de l'infraction et, en tenant compte du principe de proportionnalité, de leur capacité à résoudre le problème de concurrence initial. En effet, le principe de la proportionnalité en droit de la concurrence impose de « *rechercher le remède*

[118] Marie Cartapanis, Engagements (pratiques anticoncurrentielles), Dictionnaire de droit de la concurrence, Concurrences, Art. N° 12301.

le plus adapté au problème de concurrence rencontré. Cette quête de proportionnalité inspire aussi la détermination de la durée des engagements »[119].

Parmi eux, les engagements comportementaux sont les plus utilisés pour répondre à des pratiques potentiellement anti-concurrentielles. Ils correspondent à une régulation des comportements de l'entreprise en utilisant des contraintes commerciales ou stratégiques[120]. Ces engagements peuvent par exemple donner lieu à des modifications ou suppressions de clauses contractuelles (Aut. Conc., déc. N^os 06-D-24, 11-D-08), à garantir l'accès à une infrastructure essentielle ou à un groupement fermé (Aut. Conc., déc. N° 12-D-06), effectuer une communication d'informations à des concurrents (Aut. Conc., déc. N° 14-D-09), interdire à deux entreprises du même groupe de soumissionner à des marchés publics simultanément (Aut. Conc., déc. N° 08-D-29) ou imposer la mise en place de programmes de conformité (Aut. conc., déc. n^os 14-D-19, 15-D-19)[121].

Ainsi l'Autorité de la concurrence dispose-t-elle d'une flexibilité importante dans la détermination précise des engagements comportementaux. Cette flexibilité pourrait lui permettre, lorsque la vie privée est identifiée comme un des paramètres importants des pratiques analysées, d'imposer des mesures prenant en compte le respect de la vie privée.

Lorsqu'elle identifie des pratiques potentiellement anti-concurrentielles faisant intervenir des traitements potentiellement non-conformes au RGPD, l'Autorité de la concurrence pourrait rendre obligatoire un engagement consistant pour une entreprise à se rapprocher de la CNIL dans le but de se mettre en conformité. Ainsi, dès lors que de telles pratiques font intervenir des données personnelles, l'Autorité de la concurrence pourrait rendre obligatoire, après échange avec la CNIL pour en apprécier l'opportunité, une prise de contact avec elle.

Plus généralement, il pourrait être opportun pour l'Autorité de la concurrence **de consulter informellement la CNIL, le cas échéant, sur la rédaction des engagements en matière de vie privée, protection des données personnelles et conformité RGPD**, la CNIL se mettant en mesure, de son côté, de fournir une réponse très rapidement au collège de l'Autorité.

Proposition n°13 : *Lorsque des préoccupations de concurrence en lien avec des traitements potentiellement non-conformes au RGPD ont été identifiées,* ***réfléchir à l'opportunité, pour l'Autorité de la concurrence, de rendre obligatoires des engagements*** *par lesquels les entreprises concernées s'engagent à prendre contact avec la CNIL pour remédier à ces non-conformités.*

5.3.2 Les engagements structurels

Hormis les engagements comportementaux, les entreprises peuvent également proposer des engagements structurels. Ceux-ci correspondent à des mesures « *modifiant directement et par eux-mêmes la structure des marchés (le nombre, la qualité ou le périmètre des opérateurs actifs sur un marché)* »[122]. Ces engagements peuvent prendre la forme de transferts définitifs, de renonciations de droits de propriété ou contractuels. À titre d'exemple, les mesures peuvent avoir pour finalité d'imposer une cession d'actifs à une entreprise afin de restaurer ou maintenir la concurrence sur un marché. En particulier, les engagements structurels ont vocation à être plus limités et brefs dans le temps par rapport à des engagements comportementaux qui peuvent s'étendre et nécessiter un suivi de la part de l'Autorité de la concurrence.

Néanmoins, même si l'imposition d'engagements structurels dans le cadre de procédures concernant de potentielles pratiques anticoncurrentielles est possible, elle n'est en pratique pas utilisée par l'Autorité de la concurrence sous cette forme. En effet, les pratiques anti-concurrentielles ont trait aux comportements les plus néfastes pour le marché d'entreprises. Par conséquent, les engagements comportementaux permettent de mieux cibler ces pratiques.

En revanche, des remèdes dit « quasi-structurels » peuvent être imposés. Ils correspondent à des engagements ayant des effets rapides mais nécessitant un contrôle simple et peu coûteux. Flexibles par nature, ils peuvent également porter sur une modification substantielle des règles d'organisation et de fonctionnement des entreprises. À titre d'exemple, c'est le cas des accords de licence (Aut. conc., déc. n° 05-D-25), de la mise en

[119] Autorité de la concurrence, Les engagements comportementaux, Les essentiels, La documentation Française, Direction de l'information légale et administrative, Paris, 2019, p.41.
[120] Ibid.
[121] Ibid, p. 103.
[122] Ibid., p. 27.

place ou évolution de la comptabilité analytique (décision no 17-D-09), de la séparation des activités en marché et hors marché d'un monopoleur (Aut. conc., déc. n° 12-D-04)[123].

La CNIL pourrait permettre de contribuer à la mise en œuvre d'engagements lorsqu'ils concernent des données personnelles. En particulier, lorsque des accords de licence incluent l'accès à des données personnelles, l'Autorité pourrait imposer à l'entreprise de se mettre en contact avec la CNIL pour s'assurer de la compatibilité des propositions avec le RGPD (cf. proposition n°13).

5.3.3 Favoriser la « conformité conjointe »

La déclaration conjointe précitée met en avant l'importance de la « *prise en compte par les acteurs économiques de la vie privée et des données personnelles comme du respect du cadre concurrentiel dès la conception d'un produit ou d'un service* »[124]. Cette démarche doit contribuer à améliorer et orienter les choix des consommateurs vers les entreprises les plus vertueuses en matière de vie privée. Il y a donc un enjeu crucial à inciter les entreprises à réfléchir aux caractéristiques de leurs produits ou services à la fois du point de vue de la conformité au droit de la concurrence et au RGPD. Par ailleurs, la pertinence de prendre en compte les AIPD, par exemple dans les dossiers de fusion, résulte de ce qui a été dit supra.

D'ailleurs, l'Autorité de la concurrence encourage les entreprises à se doter d'un programme de conformité en matière de concurrence. Le document-cadre de l'Autorité indique que ce programme peut être conçu de manière autonome, ou être intégré à une politique générale de conformité aux normes, qui traiterait également des autres dimensions de la conformité, par exemple en matière de protection des données personnelles[125].

Une prise de position plus exigeante vis-à-vis de ces programmes de conformité permettrait de clarifier le message auprès des entreprises. En effet, toute entreprise devrait privilégier la mise en place d'une politique générale de conformité aux normes afin d'articuler efficacement l'ensemble des règles existantes. Dans ce but, la CNIL et l'Autorité de la concurrence pourraient travailler sur un document-cadre conjoint sur les programmes de conformité, notamment en matière d'études d'impact. Les entreprises bénéficieraient à la fois d'une sécurité juridique accrue et d'une meilleure lisibilité de ces programmes. Les deux institutions tireraient également un avantage à favoriser une conformité conjointe, que l'entreprise se place initialement du point de vue du RGPD ou du droit de la concurrence.

6 Conséquences pour la coopération au niveau européen

Si une meilleure articulation de la protection des données et la concurrence au niveau national est nécessaire, celle-ci doit s'articuler avec l'environnement européen existant. C'est en effet au niveau européen que l'articulation des deux cadres et le dialogue des concepts et des outils aurait le plus d'impact, notamment envers les grands acteurs du numérique.

Il convient pour la CNIL comme pour l'Autorité de la concurrence de comprendre et d'intégrer les évolutions normatives européennes afin de maintenir l'efficacité de la coopération au niveau national (6.1). La CNIL et l'Autorité de la concurrence ont également un intérêt commun à diffuser et promouvoir les principaux principes de leur coopération, afin de favoriser la projection des avancées nationales au niveau européen (6.2). Au-delà des décisions et analyses, la prise en compte de la concurrence pourrait aller jusqu'à avoir pour effet d'initier une réflexion sur la gouvernance européenne actuelle de la protection des données (6.3).

6.1 Intégrer les évolutions normatives européennes

6.1.1 Prendre en compte les autres textes européens

La coopération entre les autorités comme la CNIL et l'Autorité de la concurrence s'est également renforcée au niveau européen grâce à la mise en place de nouveaux forums d'échanges. À titre d'exemple, un Groupe de Haut niveau a été créé afin de mener des réflexions sur l'interaction entre le règlement sur les marchés numériques (« DMA ») et les autres régulations existantes. Il regroupe différents réseaux de régulateurs dont le CEPD et le

[123] Ibid., p. 103.
[124] Autorité de la concurrence et Commission nationale de l'informatique et des libertés, 2023, Concurrence et données personnelles : une ambition commune, p. 11.
[125] Autorité de la concurrence, Document-cadre du 24 mai 2022 sur les programmes de conformité aux règles de concurrence, p. 1.

réseau européen de concurrence (« REC »). En effet, le DMA comporte plusieurs références aux données personnelles et au RGPD. Ce texte aux effets importants sur la concurrence nécessite une coopération étroite entre les autorités de la concurrence et de protection des données.

Le règlement sur les données (« Data Act ») renforce également la nécessité de coopérer aux niveaux national et européen, puisqu'il concerne à la fois la concurrence et la protection des données personnelles. D'ailleurs, le CEPD avait indiqué reconnaître « *également l'importance de l'objectif d'offrir un droit plus efficace à la portabilité des données, et accueillent favorablement cet objectif, en vue de faciliter l'innovation, de promouvoir la concurrence* »[126]. Toutefois, différents risques existent, tels que la collecte, le partage et l'utilisation à l'insu de la personne, générés par les droits d'accès, d'utilisation et de partage des données des entreprises à d'autres entités, notamment d'autres entreprises, etc.[127] Un cadre de coopération européen est donc indispensable pour garantir une bonne articulation entre les enjeux de la concurrence et ceux de la protection des données personnelles. De manière identique, les problématiques concernant l'interopérabilité nécessitent une coopération accrue avec les autorités de la concurrence pour comprendre l'ensemble des enjeux concurrentiels en fonction des secteurs étudiés.

6.1.2 Veille constante et incidence sur les initiatives européennes similaires

La participation aux séminaires européens peut permettre de maintenir une veille constante sur les initiatives européennes en matière de coopération. Des échanges informels réguliers entre la CNIL et l'Autorité de la concurrence pourront être organisés pour mettre en commun les informations concernant ces initiatives. À ce titre, des échanges entre les points de contact sont à prévoir, afin de garantir l'efficacité des échanges d'information.

Bien que des travaux réalisés par la *Global Privacy Assembly* (« GPA ») existent, l'OCDE pourrait avoir un rôle prépondérant dans l'organisation des réflexions sur l'inter-régulation. Elle pourrait davantage s'intéresser aux spécificités européennes et contribuer au décloisonnement du débat sur le plan international en accroissant le nombre d'ateliers et groupes de travail dédiés à l'articulation entre la protection des données personnelles et la concurrence. La CNIL et l'Autorité de la concurrence pourraient également s'informer sur les récents développements de l'OCDE en la matière. Ces différents formats d'échange seraient l'occasion d'approfondir les réflexions et de contribuer à maintenir un environnement dynamique de réflexion sur ce sujet.

6.2 Projeter nos avancées dans les structures européennes

6.2.1 Promouvoir la déclaration conjointe au niveau européen

Parmi les pays de l'Union européenne, la déclaration conjointe entre la CNIL et l'Autorité de la concurrence propose un des cadres de coopération les plus avancés en matière d'articulation entre protection des données et concurrence. Afin de maintenir une sécurité juridique importante pour l'ensemble des acteurs, mais aussi pour éviter tout risque de *forum-shopping*, qui consisterait pour une entreprise à sélectionner l'autorité de protection des données la plus favorable à ses intérêts, la définition d'une approche harmonisée au plan européen à cet égard est certainement pertinente. Elle permettrait en outre à chacune des autorités de protection des données nationales de se saisir de ce sujet à l'instar des homologues les plus avancés : si le CEPD permet déjà de mettre en place des mécanismes de coordination entre autorités de protection des données, la mise en place d'un dispositif de coordination au niveau européen avec les autorités de concurrence pourrait ainsi faciliter les coopérations au niveau national.

La CNIL pourrait ainsi positionner la déclaration conjointe comme un des exemples de coopération pouvant inspirer les pratiques des autorités de protection des données européennes. Pour ce faire, la CNIL devrait accentuer l'utilisation de la déclaration conjointe en tant que référence dans les travaux européens. Cette promotion d'une coopération pourrait avoir sa contrepartie de la part de l'Autorité de la concurrence. Aussi, l'intégration de la déclaration conjointe comme référence devrait-elle être encouragée par l'Autorité de la concurrence. En particulier, lorsque la CNIL et l'Autorité de la concurrence travaillent sur des sujets similaires, voire communs, au niveau européen, une coordination des positions peut être réalisée au préalable au moyen d'échanges informels au plan national.

---

[126] Avis conjoint 2/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), point 11, p.8.
[127] Ibid., point 13 et 14, p. 8.

La mise en place d'une coopération accrue entre les autorités de protection des données et de concurrence nécessite de réfléchir aux moyens permettant de mieux prendre en compte la concurrence dans nos travaux européens de manière plus générale. Pour ce faire, un discours cohérent et régulier sur les bénéfices de notre coopération doit être assuré dans les différents niveaux de discussion du CEPD. En particulier, la participation aux équipes de rédaction (« drafting teams ») permet d'avoir une incidence directe sur la rédaction de positions articulant au mieux la concurrence et la protection des données. La présence de la CNIL dans les sous-groupes et groupes de travail peut également permettre de promouvoir au mieux ses travaux sur le même sujet. En outre, notre parole en plénière pourrait permettre de soutenir la nécessité de renforcer la coopération à l'échelle de l'Union européenne à ce sujet.

6.2.2 Promouvoir publiquement les travaux sur l'articulation dans le cadre du CEPD

Par ailleurs, de nombreux séminaires de dimension européenne sont organisés. Ces lieux d'échanges donnent l'occasion de faire connaître la déclaration conjointe et d'identifier les initiatives proches ou équivalentes. La CNIL et l'Autorité de la concurrence peuvent intervenir conjointement dans des séminaires et ateliers concernant l'articulation entre concurrence et données personnelles. À titre d'exemple, l'OCDE a organisé récemment un évènement sur la question permettant de montrer la capacité des deux autorités à coopérer[128]. La CNIL devrait donc poursuivre ce travail d'identification des lieux d'échanges utiles pour promouvoir la déclaration en associant l'Autorité de la concurrence à cette démarche.

D'ailleurs, au niveau de la Commission européenne, une conférence réunissant des acteurs institutionnels, académiques, privés, de la société civile, afin de réfléchir sur l'articulation entre la concurrence et les données personnelles pourrait être organisée. Elle permettrait de mettre en avant les différents cadres de coopération existants en Europe, avec la déclaration conjointe entre la CNIL et l'Autorité de la concurrence comme exemple de coopération avancé. Cette conférence serait également l'occasion de mettre en avant les nouveaux développements académiques et privés sur ces questions afin d'identifier les sujets nécessitant davantage de coopération entre autorités.

6.2.3 Le rôle clé de la *task force* C&C

La promotion de nos travaux au niveau européen relève, au sein du CEPD, de la mission de la *task force* Consumer and Competition (C&C), créée en mars 2023 et chargée des travaux concernant l'articulation entre la protection des données personnelles, la concurrence et la protection du consommateur. La CNIL pourrait continuer à nourrir ces travaux pour promouvoir un cadre de coopération renforcé. En particulier, cette *task force* travaille déjà en cohérence avec le réseau européen de concurrence, le CEPD et la Commission européenne. Aussi, bénéficie-t-elle d'une capacité à identifier et mobiliser les acteurs pertinents pour développer des réflexions sur l'articulation entre la concurrence et les données personnelles.

Le mandat de la *task force* C&C étant établi pour deux ans et se terminant début 2025, il pourrait être proposé de prolonger ce cadre en en faisant un point focal, au sein du CEPD, de l'articulation entre ces différents cadres juridiques y compris sur des dossiers concrets. Après une première étape de définition de doctrine, se traduisant cette année par la publication d'un document de position inspiré de la déclaration conjointe, la *task force* pourrait utilement jouer un rôle en matière d'intégration concrète des préoccupations de concurrence dans les dossiers du CEPD. Elle devrait à ce titre être systématiquement consultée par les différents sous-groupes lorsqu'un dossier soulève des enjeux d'articulation entre ces différents cadres juridiques. En outre, la *task force* pourrait développer un rôle de « *peer review* » afin d'inciter les différentes autorités nationales à développer leur profil en matière de coopération avec leurs homologues.

Ainsi, la CNIL pourrait s'appuyer sur les travaux de la *task force* pour promouvoir une harmonisation des pratiques au niveau européen et encourager la coopération. En outre, la présence de la CNIL dans ce groupe de travail en tant que coordinateur permet de maintenir une dynamique favorable à la coopération entre autorités. La CNIL devrait également encourager le développement de documents de doctrine rédigés conjointement avec le réseau européen de concurrence.

A terme, comme l'ont montré les travaux sur le « *consent or pay* », la *task force* devrait pouvoir jouer un rôle pivot dans l'organisation d'un dialogue régulier entre le CEPD et le réseau européen de concurrence.

[128] OCDE, 13 juin 2024, The intersection between competition and data privacy – Background Note, DAF/COMP(2024)4.

Proposition n°14 : reconduire la task force « C&C » et développer son programme de travail *pour lui faire jouer un rôle pivot dans l'articulation entre concurrence, protection des consommateurs et données personnelles au plan européen et faire avancer le collectif européen en la matière.*

6.3 Pour une réflexion sur la gouvernance européenne en matière de données ?

6.3.1 Des réseaux de coopérations différents

Les articles 56, 60, 61 et 62 du RGPD organisent la coopération en matière répressive entre les autorités de protection des données en créant un système de guichet unique, d'assistance mutuelle et d'opérations conjointes. Les autorités ont donc la possibilité de mettre en place des actions cordonnées afin d'étudier une affaire. De plus, elles doivent prendre les mesures appropriées pour répondre aux demandes lorsque le mécanisme d'assistance mutuel est déclenché. Le mécanisme d'assistance peut concerner « *les demandes d'informations et les mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et les enquêtes* »[129]. Par ailleurs, conformément au système de guichet unique, dans le cas d'une plainte concernant un traitement transfrontalier mobilisant plusieurs établissements au sein de l'Union européenne, c'est l'autorité de protection des données de l'Etat Membre où est situé l'établissement principal qui est compétente. Elle est alors qualifiée d'autorité chef de file.

De manière équivalente, la création du réseau européen de la concurrence par le règlement (CE) n° 1/2003 a permis de mettre en place un mécanisme de coopération formel entre les autorités de concurrence. L'objectif principal étant l'application efficace et uniforme des articles 101 et 102 du Traité sur le fonctionnement de l'Union européenne. Une des différences essentielles de fonctionnement de ce réseau par rapport aux autorités de protection des données est le mécanisme de coopération pour l'attribution des affaires et l'assistance. En effet, l'autorité de concurrence recevant la plainte ou engageant une procédure reste généralement en charge des affaires, néanmoins une réattribution peut être envisagée au commencement de la procédure « *si cette autorité estime qu'elle n'est pas bien placée pour agir ou si d'autres autorités s'estiment bien placées, elles aussi, pour agir* »[130]. Dans ce cas, afin de « *préserver efficacement la concurrence et l'intérêt communautaire* »[131], les membres du réseau peuvent réattribuer l'affaire à une autorité mieux placée à condition de ne pas interrompre les enquêtes en cours.

Cet aménagement du principe du pays d'origine en matière de concurrence, non seulement permet de réduire les risques de *forum shopping* en privilégiant les marchés sur lesquels les risques concurrentiels sont les plus élevés, mais favorise également une saine émulation entre autorités nationales, en étant un aiguillon en termes d'expertise et de mobilisation des équipes. Il pourrait constituer un précédent intéressant dans le cas de la protection des données, qui repose entièrement sur le principe du pays d'établissement du siège du responsable de traitement et le rôle des autorités nationales, ce qui est parfois problématique[132].

6.3.2 Les mérites d'autres règles d'allocation des cas

Ainsi, une analyse comparative pourrait être menée afin d'examiner si les règles d'attribution et le rôle du CEPD ne pourraient évoluer à terme en mettant en place un principe s'inspirant de celui du réseau européen de concurrence d'autorité bien placée pour s'occuper de l'affaire. Un tel aménagement du principe du pays d'origine serait assez naturel en protection des données, un domaine qui vise à protéger les droits fondamentaux des personnes concernées dans les pays où sont commercialisés les biens et services concernés.

Pour lancer la réflexion, en matière de concurrence la Commission définit trois principaux critères permettant d'identifier si une autorité est bien placée : (1) le caractère substantiel des effets des pratiques ou accords de l'entreprise sur son territoire, (2) la capacité de l'autorité à faire cesser efficacement l'infraction et (3) la capacité de réunir les preuves à l'appui du recours, y compris avec le concours des autres autorités[133]. Il s'agirait donc, si cette piste était retenue, de proposer une évolution de l'article 56 du RGPD en ouvrant la possibilité d'attribution

---

[129] Article 61.1 du RGPD.
[130] Communication de la Commission relative à la coopération au sein du réseau des autorités de concurrence, 2004/C 101/03, Journal officiel n° C 101 du 27/04/2004, p. 0043 – 005, point 6.
[131] Ibid., point 7.
[132] Voir l'interview d'I. Falque-Pierrotin dans EDPS, 2024 par exemple.
[133] Ibid., point 8.e.

à des autorités qui ne seraient ni l'autorité de contrôle chef de file, ni l'autorité concernée au sens de l'article 60 du RGPD.

Cette « autorité bien placée » pourrait par exemple être parmi celles qui disposent de plus de compétences et d'expérience en matière économique et concurrentielle. Dans son rôle de coordination, le Secrétariat du CEPD pourrait faciliter ce processus d'attribution dans des conditions de neutralité fortes de manière équivalente à la Commission européenne dans le cadre du réseau européen de concurrence.

Les autorités de protection des données pourraient également s'inspirer de l'utilisation du réseau européen de concurrence par les autorités. Cela pourrait se traduire par un accroissement de l'utilisation des articles 61 et 62 du RGPD pour les traitements transfrontaliers. Bien que ces dispositions soient déjà utilisées, des situations nationales pourraient bénéficier d'une assistance des autres autorités de protection des données. En particulier, l'article 62 peut permettre de renforcer les capacités de contrôle au niveau européen, à l'instar de ce que les autorités de concurrence sont en capacité de faire, via par exemple des contrôles conjoints.

6.3.3 Vers une réflexion prospective

Si un mécanisme de coopération existe entre les autorités de protection des données, ainsi qu'un dispositif de guichet unique permettant d'harmoniser les décisions des autorités de contrôle au niveau européen, il n'est pas équivalent au système de compétences parallèles du réseau européen de concurrence. En effet, en matière de concurrence, dans certaines situations, la Commission européenne peut être bien placée pour traiter d'une affaire permettant d'assurer une meilleure prise en compte des affaires ayant des effets sur l'ensemble de l'Union européenne. Tel n'est pas le cas en matière de protection des données, le CEPD n'ayant pas de compétence de supervision des responsables de traitement privés établis dans les différents Etats-membres. C'est pourquoi, la réponse à la question n'est pas univoque : une réflexion prospective pourrait être initiée à cet égard – à l'instar de ce qui a été fait avant la mise en place du réseau européen de concurrence – sur les moyens d'une division efficace du travail et d'une application efficace et homogène du RGPD, qui s'attacherait (i) examiner les mérites du dispositif retenu en matière de concurrence (ii) vérifier la légitimité du rôle de l'autorité du pays d'établissement en matière de protection des droits et (iii) garantir la non-fragmentation du marché intérieur via des processus de coopération appropriés.

Une autre différence entre les deux cadres résulte de la nécessité, prévue par le RGPD, pour les autorités de protection des données d'être des autorités indépendantes du pouvoir central. De ce fait, l'architecture fédérale reposant sur une compétence exclusive de la Commission européenne ne pourra pas être retenue. Les règles de division du travail ne devraient pas pouvoir être influencées par la Commission mais décidées d'un commun accord au sein du CEPD. Au moment où certaines autorités pourraient hésiter à s'engager dans cette voie, cet état de fait pourrait comporter un certain nombre de garanties pour une évolution maîtrisée de la gouvernance européenne de la protection des données.

Proposition n°15 : mener une analyse comparative et prospective des différents systèmes de répartition des compétences entre autorités de régulation et de contrôle dans l'Union européenne, *en s'intéressant notamment aux systèmes mis en place en matière de protection de la concurrence, de protection des données personnelles, de régulation des marchés financiers, des médias ou de l'énergie.*

***

7 Annexe : liste des propositions

Proposition n°1 : prendre en compte les questions concurrentielles en amont dans les travaux de la CNIL. Développer une meilleure maîtrise des effets des décisions de la CNIL sur la concurrence permet de promouvoir une cohérence générale de l'application de la concurrence et de la protection des données. L'accroissement de cette cohérence contribue à faciliter la valorisation de comportements vertueux à la fois pour le respect de la concurrence et la protection de la vie privée et des données personnelles. Il concourt également à renforcer la prévisibilité des actions de régulation et par conséquent la sécurité juridique des entreprises.

Proposition n°2 : expérimenter le concept de « pouvoir sur les données » en tant qu'éclairage doctrinal, lorsqu'il est plus adapté que les concepts concurrentiels existants (dominance ou pouvoir de marché) dans les analyses de protection des données de la CNIL, lorsqu'il s'agit d'apprécier les relations entre une personne concernée et un responsable de traitement.

Proposition n°3 : développer dans la pratique de la CNIL la prise en compte des illicéités concurrentielles au titre du a) du 1 de l'article 5 du RGPD. Les comportements de concurrence déloyales ou les pratiques anti-concurrentielles, s'ils sont jugés ou documentés par les autorités de concurrence, peuvent constituer des facteurs complémentaires aux manquements aux règles de protection des données. Dans le cas contraire, il conviendra de saisir l'Autorité de la concurrence pour avis.

Proposition n°4 : à l'appui du respect du principe de minimisation, développer l'analyse du rôle joué par les pratiques anti-concurrentielles dans l'accumulation des données et les indices de collecte de données au détriment des personnes qui ne peuvent s'y opposer.

Proposition n°5 : explorer conjointement les risques et les marchés, sur la base d'échange d'expertises, d'auditions conjointes volontaires ou de la réalisation d'études communes entre la CNIL et l'Autorité de la concurrence.

Proposition n°6 : afin d'approfondir la coopération entre les deux autorités selon trois axes : les concepts, la doctrine et les cas, **instaurer au sein de chaque autorité un point de contact chargé de piloter la coopération**.

Proposition n°7 : **engager une réflexion commune spécifique concernant le droit à la portabilité des données personnelles, et ses conséquences en matière de protection de données personnelles et de concurrence**. Cette réflexion pourra, le cas échéant, impliquer d'autres acteurs ou autorités compétents en matière de portabilité des données personnelles ou d'interopérabilité, tels que l'Arcep et être articulée avec les différents forums existants ou en cours de mise en place (ex : Groupe de haut niveau du DMA, réseau national de coordination de la régulation des services numériques).

Proposition n°8 : **organiser régulièrement des formations croisées** aux enjeux de concurrence et de protection des données à destination des deux autorités

Proposition n°9 : **mieux proportionner les sanctions au comportement de l'entreprise en faisant de ce dernier, le cas échéant, un facteur aggravant** de la sanction au titre de l'article 83.2 k) RGPD : majoration des bénéfices tirés du manquement, accroissement de gravité des dommages aux personnes, effet écosystémique éventuellement négatif de l'entreprise.

Proposition n°10 : **encourager une saisine de la CNIL, à titre formel ou informel, lorsque la vie privée et les données personnelles sont en jeu dans un dossier de concentration**, en particulier en cas de procédure d'examen approfondi (phase 2).

Proposition n° 11 : proposer à l'Autorité de la concurrence de **saisir la CNIL, à titre formel ou informel, lorsque la mise en commun ou la combinaison de bases de données sont en jeu dans un dossier d'antitrust**, afin d'examiner si d'éventuelles non conformités au RGPD en la matière, même motivées par une recherche d'efficacité, ne constitueraient pas un abus de position dominante.

Proposition n°12 : capitaliser sur la coopération en matière de doctrine en rédigeant des relevés de conclusions opérationnels lors des ateliers internes, systématiser les documents de restitution au public de la manière dont les avis croisés ont été intégrés et en organisant à intervalles réguliers des événements de type académique sur les sujets « concurrence et protection des données ».

Proposition n°13 : Lorsque des préoccupations de concurrence en lien avec des traitements potentiellement non-conformes au RGPD ont été identifiées, **réfléchir à l'opportunité, pour l'Autorité de la concurrence, de rendre obligatoires des engagements par lesquels les entreprises concernées s'engagent à prendre contact avec la CNIL** pour remédier à ces non-conformités.

Proposition n°14 : reconduire la task force « C&C » et développer son programme de travail pour lui faire jouer un rôle pivot dans l'articulation entre concurrence, protection des consommateurs et données personnelles au plan européen et faire avancer le collectif européen en la matière.

Proposition n°15 : mener une analyse comparative et prospective des différents systèmes de répartition des compétences entre autorités de régulation et de contrôle dans l'Union européenne, en s'intéressant notamment aux systèmes mis en place en matière de protection de la concurrence, de protection des données personnelles, de régulation des marchés financiers, des médias ou de l'énergie.