Translations proofread by EDPB Members.
This language version has not yet been proofread.

Document de synthèse concernant l'interaction entre le droit en matière de protection des données et le droit de la concurrence

Adopté le 16 janvier 2025

Synthèse

Promouvoir la coopération entre les autorités chargées de la protection des données à caractère personnel et les autorités de concurrence peut être utile pour protéger les personnes et élargir leur choix. Dans la pratique, les données à caractère personnel et les règles applicables à leur traitement occupent une place de plus en plus centrale à mesure que les modèles commerciaux des entreprises évoluent. Il est donc essentiel d'examiner les moyens de promouvoir la cohérence entre des domaines de réglementation qui sont distincts mais interagissent, en gardant à l'esprit les risques associés à leur application incohérente tant au niveau individuel qu'au niveau sociétal. Cela nécessitera une meilleure compréhension de la relation entre les notions employées dans les domaines du droit en matière de protection des données et du droit de la concurrence, de manière à renforcer la capacité des autorités chargées de la protection des données à tenir compte du contexte économique, ainsi que la capacité des autorités de concurrence à intégrer dans leurs appréciations et décisions des considérations potentiellement pertinentes en matière de protection des données.

- Conformément à l'arrêt de la CJUE dans l'affaire C-252/21, la **coopération entre les autorités chargées de la protection des données et les autorités de concurrence est, dans certains cas, obligatoire et non facultative**.
- Les décideurs politiques **devraient être conscients de la possibilité que les autorités et organismes de réglementation compétents pour surveiller le secteur numérique doivent coopérer plus étroitement dans certains cas**.
- Actuellement, le **degré de coopération entre autorités varie considérablement d'un État membre à un autre et n'est pas harmonisé par le droit de l'Union**.
- Au sein des autorités, des mesures internes telles que la mise en place d'une équipe spécifiquement chargée de coordonner les tâches de coopération et de faire office de **point de contact unique pour les autres autorités pourraient favoriser la coopération avec les autres autorités de contrôle**.
- Afin de garantir une coopération efficiente, les autorités devraient **développer une compréhension et une connaissance de base** du cadre réglementaire utilisé par les homologues concernés.

Table des matières

1 INTRODUCTION 4

2 PROMOUVOIR LA COOPÉRATION ET LES CONVERGENCES 4

2.1 Protéger les personnes 4

2.2 L'évolution de la protection des données dans le contexte du développement de l'économie numérique 5

3 COMMENT LES NOTIONS EMPLOYÉES PEUVENT INTERAGIR 6

3.1 Protéger les personnes et leur prise de décision 6

3.2 Licéité au titre de l'article 5, paragraphe 1, point a): application de l'affaire Meta dans le cadre du RGPD 7

3.3 Exemple de renforcement de la prise en compte de la protection des données 8

4 S'APPUYER SUR LA COOPÉRATION 9

4.1 Pourquoi les autorités chargées de la protection des données et les autorités de concurrence devraient coopérer 9

4.2 Modèles de coopération existants dans les États membres de l'UE 9

4.3 Moyens d'améliorer la coopération 10

5 CONCLUSIONS 11

Le comité européen de la protection des données a adopté le document de synthèse suivant:

1 INTRODUCTION

1. Pour les autorités de réglementation chargées de la protection des données, les modifications récentes du paysage juridique soulèvent de nombreuses questions qui se situent à la frontière entre le droit en matière de protection des données et le droit de la concurrence. Il ressort clairement de l'arrêt Meta/Bundeskartellamt[1] que les objectifs réglementaires en matière de protection des données et de concurrence ne peuvent pas toujours être poursuivis isolément. Au contraire, les autorités de réglementation pourraient devoir coopérer et se coordonner afin d'explorer des synergies et de prendre part à des activités de contrôle cohérentes, efficaces et complémentaires. Une telle coopération peut bénéficier aux personnes, aux entreprises et à d'autres entités: elle permet aux différentes autorités de réglementation de protéger les personnes dans l'UE de la manière la plus efficace et la plus efficiente possible et garantit une interprétation et une application cohérentes des normes juridiques.

2. Bien que le RGPD et le droit de la concurrence puissent s'appliquer aux mêmes acteurs et aux mêmes activités, il s'agit de domaines juridiques clairement distincts, fondés sur des notions et des objectifs juridiques différents et dotés de leur propre cadre d'application. Alors que le droit en matière de protection des données vise à garantir le droit fondamental des personnes concernées à la protection de leurs données à caractère personnel, en particulier contre un traitement illicite, déloyal et opaque de celles-ci[2], le droit de la concurrence vise quant à lui à «protéger le bon fonctionnement des marchés»[3]. Il convient donc de mener une analyse pour examiner les situations dans lesquelles il existe une interaction entre protection des données et concurrence.

3. Avec le présent document de synthèse, le CEPD fournit une brève analyse de cette interaction et formule des recommandations en vue du renforcement de la coopération existante entre les autorités de réglementation.

2 PROMOUVOIR LA COOPÉRATION ET LES CONVERGENCES

2.1 Protéger les personnes

4. Le droit en matière de protection des données et le droit de la concurrence de l'UE sont des cadres et domaines juridiques clairement distincts qui visent des objectifs différents. Ils présentent toutefois un certain nombre de points communs potentiels, tels que la protection des personnes et de leurs choix. En effet, alors que la politique de protection des données vise à protéger les personnes contre tout traitement illicite ou déloyal de leurs données à caractère personnel, la politique de concurrence a

[1] Arrêt du 4 juillet 2023, Meta Platforms e.a. (C-252/21, ECLI:EU:C:2023:537), également dénommé «**arrêt Bundeskartellamt**» dans le présent document de synthèse.
[2] Voir l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte ») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (TFUE), qui disposent que toute personne a droit à la protection des données à caractère personnel la concernant.
[3] Commission européenne: Direction générale de la concurrence, 2017, *La politique de concurrence de l'UE en action: DG Concurrence en action,* Office des publications de l'Union européenne, https://data.europa.eu/doi/10.2763/897035.

pour objet de garantir, dans l'intérêt des consommateurs, les conditions d'une concurrence libre et non faussée entre les entreprises sur les marchés en cause[4], en promouvant l'innovation, la diversité de l'offre et des prix attractifs[5]. Cet objectif de protection des personnes en leur qualité de consommateurs qui est visé par le droit de la concurrence trouve son expression dans l'interdiction des ententes et des abus de position dominante et la lutte contre les concentrations anticoncurrentielles, lesquels, à défaut d'intervention, peuvent causer un préjudice aux consommateurs, sous la forme d'une hausse des prix, d'une réduction du choix et d'une baisse de la qualité et de l'innovation[6].

5. Un affermissement du lien entre la protection des données à caractère personnel et la concurrence peut contribuer à la protection des personnes et au bien-être des consommateurs en renforçant la conception commune du respect de leurs droits fondamentaux et du bon fonctionnement de marchés concurrentiels.

6. Il serait donc bénéfique de renforcer la coopération entre les autorités chargées de la protection des données et les autorités de concurrence, en particulier dans les cas où l'application du droit de la concurrence et l'application des règles de protection des données se recoupent de manière évidente. Cela aiderait à déterminer et à résoudre en amont les tensions qui pourraient survenir dans certaines situations entre les deux domaines du droit. Une coopération accrue entre autorités permettrait ainsi d'améliorer la cohérence et l'efficacité de leurs actions respectives, au bénéfice tant des personnes que des entités qui doivent se conformer aux exigences légales des deux domaines.

2.2 L'évolution de la protection des données dans le contexte du développement de l'économie numérique

7. L'économie numérique a placé les données à caractère personnel au cœur de nombreux modèles commerciaux. La protection des données est donc, dans certains cas, devenue un paramètre important de la concurrence[7]. Dans le même temps, la législation de l'UE en matière de protection des données vise à empêcher le traitement illicite et déloyal des données à caractère personnel, notamment dans les cas de déséquilibre de pouvoir entre les responsables du traitement et les personnes dont les données à caractère personnel sont collectées.

8. Dans sa nouvelle communication sur la définition du marché en cause[8], la Commission reconnaît que, lors de la définition du marché en cause, la protection de la vie privée et des données à caractère

[4] Voir articles 101 et 102 du TFUE.

[5] Commission européenne: Direction générale de la concurrence, 2024, *Protecting competition in a changing world: Evidence on the evolution of competition in the EU during the past 25 years*. Office des publications de l'Union européenne, https://data.europa.eu/doi/10.2763/089949.

[6] Par exemple, l'article 102 du TFUE précise qu'un abus de position dominante consiste à « limiter la production, les débouchés ou le développement technique au préjudice des consommateurs».

[7] Voir également Commission européenne, Competition policy brief, April 2024, Non-Price Competition: EU Merger Control Framework and Case Practice, Issue 1, p. 4. Le point 51 de l'arrêt rendu dans l'affaire C-252/21 indique que «*l'accès aux données à* caractère *personnel et la possibilité de traitement de ces données sont devenus un paramètre significatif de la concurrence entre entreprises de l'économie numérique*. *Partant, exclure les règles en matière de protection des données à caractère personnel du cadre juridique à prendre en considération par les autorités de la concurrence lors de l'examen d'un abus de position dominante méconnaîtrait la réalité de cette évolution économique et serait susceptible de porter atteinte à l'effectivité du droit de la concurrence au sein de l'Union*.»

[8] Commission européenne, 2024, Communication de la Commission – Communication de la Commission sur la définition du marché en cause aux fins du droit de la concurrence de l'Union, Journal officiel C 1645, ELI: http://data.europa.eu/eli/C/2024/1645/oj

personnel offerte aux consommateurs peut être l'un des paramètres de la concurrence à prendre en considération[9]. En d'autres termes, le respect de la vie privée est considéré comme l'un de ces paramètres, en particulier «dans l'appréciation des concentrations numériques et technologiques»[10].

9. Un marché concurrentiel peut être un facteur de facilitation déterminant pour créer les conditions propices à des options respectueuses de la vie privée[11]. Autrement dit, si le consommateur dispose de différentes options sur le marché, cela peut encourager une réduction au minimum de la quantité de données à caractère personnel collectées ou permet d'éviter des interconnexions et des utilisations massives de données à caractère personnel provenant de différentes sources qui sont préjudiciables aux utilisateurs[12]. L'inverse est également possible. C'est le cas des stratégies d'exclusion, qui limitent le nombre d'acteurs sur le marché et peuvent donc affecter artificiellement le nombre de solutions respectueuses de la vie privée. L'absence d'alternatives commerciales peut amener les utilisateurs à opter pour des produits moins respectueux de la vie privée.

10. Dans le secteur numérique, le comportement des entreprises occupant une position dominante peut soulever des questions quant à la contribution du traitement des données à caractère personnel au renforcement et à l'exploitation d'une position. Les avantages fondés sur les données découlant de la combinaison et de l'utilisation croisée de données à caractère personnel provenant de différentes sources par les «contrôleurs d'accès» sur les marchés numériques et les risques que de tels avantages présentent pour l'équité et la contestabilité de ces marchés sont mis en évidence par les interdictions énoncées à l'article 5, paragraphe 2, du règlement sur les marchés numériques[13].

3 COMMENT LES NOTIONS EMPLOYÉES PEUVENT INTERAGIR

3.1 Protéger les personnes et leur prise de décision

11. Dans l'arrêt Bundeskartellamt, la CJUE a précisé le rôle de la position dominante dans le contexte de la validité du consentement énoncée dans le RGPD. Á cet égard, une position dominante n'implique pas systématiquement que le consentement n'est pas valable[14]. Néanmoins, certaines conditions sont requises pour garantir la validité du consentement[15], étant donné que la position dominante est susceptible d'affecter la «*liberté de choix de cet utilisateur qui pourrait ne pas être en mesure de refuser*

[9] 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, Journal officiel, C/2024/1645, point 13.
[10] Dans le contexte de la concurrence non tarifaire, voir European Commission, Competition policy brief, April 2024, Non-Price Competition: EU Merger Control Framework and Case Practice, Issue 1, section 1.3, p. 5.
[11] Commission européenne, 20 décembre 2020, document de travail des services de la Commission - Rapport d'analyse d'impact accompagnant la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques), points 65 et 66.
[12] OCDE, 13 juin 2024, The intersection between competition and data privacy – Background Note, points 39, 47 et 57, p. 11.
[13] 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).
[14] Arrêt Bundeskartellamt de la CJUE, point 154.
[15] CEPD, 17 avril 2024, avis 08/2024 sur la validité du consentement dans le cadre des modèles «consentir ou payer» mis en place par les grandes plateformes en ligne

ou de retirer son consentement sans subir un préjudice»[16] et «*est susceptible de créer un déséquilibre manifeste [...] entre la personne concernée et le responsable du traitement*»[17].

12. Par exemple, «s'il existe un déséquilibre manifeste de pouvoir, le consentement ne peut être utilisé que dans des "situations exceptionnelles" et lorsque le responsable du traitement, conformément au principe de responsabilité, peut prouver qu'il n'y a "absolument aucune conséquence négative" pour la personne concernée si elle ne donne pas son consentement, notamment dans les cas où les personnes concernées se voient proposer une autre solution sans incidence négative»[18], y compris la possibilité de discrimination ou d'exclusion sociale, en particulier dans les cas où les services numériques jouent un rôle de premier plan, ou sont déterminants pour la participation des personnes à la vie sociale ou à l'accès aux réseaux professionnels, d'autant plus s'il existe des effets de verrouillage ou de réseau[19]. La position dominante peut donc être utile pour déterminer à quel moment un responsable du traitement des données peut produire un impact sur les utilisateurs. Si cette notion n'est pas suffisante en soi pour apprécier la validité du consentement au titre du RGPD, elle est utile dans le cadre d'une appréciation plus large du déséquilibre de pouvoir au sens du RGPD. En outre, un responsable du traitement ne doit pas occuper une «position dominante» au sens de l'article 102 du TFUE pour que sa position sur le marché soit considérée comme pertinente aux fins de l'application du RGPD[20].

3.2 Licéité au titre de l'article 5, paragraphe 1, point a): application de l'affaire Meta dans le cadre du RGPD

13. Dans son arrêt, la CJUE a jugé que, lorsque les autorités de concurrence examinent si une entreprise abuse de sa position dominante au sens de l'article 102 du traité sur le fonctionnement de l'Union européenne (TFUE), sous réserve du respect de leurs obligations de coopération loyale avec les autorités de contrôle chargées de la protection des données, elles peuvent évaluer si les conditions générales d'utilisation des entreprises relatives au traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes au RGPD, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus[21]. Toutefois, les évaluations des autorités de concurrence concernant la conformité des conditions générales d'utilisation avec le RGPD aux fins de l'article 102 du TFUE ne sauraient remplacer l'évaluation de l'autorité compétente en matière de protection des données (ci-après l'«APD»)[22], en particulier de l'autorité de contrôle chef de file (ci-après l'«ACCF») dans le cas d'un traitement transfrontalier dans l'Union européenne[23]. Sur la base de l'article 4, paragraphe 3, du traité sur l'Union européenne (TUE), la CJUE a considéré que les différentes autorités nationales concernées sont toutes liées par le devoir de coopération loyale et que les autorités de concurrence sont tenues de consulter les APD et de coopérer avec elles lorsqu'elles sont appelées, dans l'exercice de leurs compétences, à examiner si le comportement d'une entreprise est conforme aux dispositions du

[16] Arrêt Bundeskartellamt, point 148, renvoyant au considérant 42 du RGPD.
[17] Ibid., point 149, renvoyant au considérant 43 et à l'article 7, paragraphe 4, du RGPD.
[18] CEPD, 17 avril 2024, avis 08/2024 sur la validité du consentement dans le cadre des modèles «consentir ou payer» mis en œuvre par les grandes plateformes en ligne, point 79, p. 21.
[19] Ibid., point 182, p. 39.
[20] Ibidem, points 103 à 105.
[21] Arrêt Bundeskartellamt, point 62.
[22] Article 55 du RGPD.
[23] L'ACCF étant, aux termes de l'article 56 du RGPD, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant, elle est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60.

RGPD[24]. Par conséquent, conformément à l'arrêt rendu par la CJUE dans l'affaire C-252/21, la coopération entre les autorités de réglementation est, dans certains cas, obligatoire et non facultative. Selon une jurisprudence constante de la Cour, le principe de coopération loyale consacré à l'article 4, paragraphe 3, du TUE implique que, dans les domaines réglementaires couverts par le droit de l'UE, l'Union et les États membres, y compris leurs autorités administratives, se respectent et s'assistent mutuellement dans l'accomplissement des missions découlant des traités[25]. En particulier, les États membres doivent prendre toutes les mesures propres à remplir leurs obligations découlant du droit de l'Union et s'abstenir de prendre toute mesure susceptible de mettre en péril la réalisation des objectifs du droit de l'Union[26].

14. L'arrêt de la CJUE incite fortement les autorités à rationaliser leur coopération et à s'accorder sur des modalités pratiques de consultation.

3.3 Exemple de renforcement de la prise en compte de la protection des données

15. S'appuyant sur des expériences telles que celle du centre d'échange numérique (Digital Clearinghouse) mis en place par le contrôleur européen de la protection des données et ses premiers avis sur la nécessité d'une application cohérente[27], le CEPD a publié en 2020 une déclaration[28] sur les incidences des concentrations en matière de protection de la vie privée, qui souligne le risque d'une éventuelle interconnexion et accumulation supplémentaires de données sensibles à caractère personnel concernant des citoyens européens par une grande entreprise de technologie. Le CEPD rappelle qu'«il est essentiel d'évaluer les implications à long terme sur la protection des droits économiques, des droits en matière de protection des données et des droits des consommateurs chaque fois qu'une importante concentration est planifiée»[29]. Il indique également que «les conséquences potentielles de cette concentration sur le plan de la protection des données à caractère personnel dans l'Espace économique européen» seront examinées par le CEPD[30]. Par conséquent, la protection de la vie privée et des données devrait être soigneusement prise en considération, le cas échéant, lors des examens des concentrations[31].

16. Compte tenu de l'incidence possible de la protection des données de l'UE dans les examens des concentrations, une coopération accrue entre les autorités de concurrence et les autorités chargées de la protection des données, y compris au niveau de l'UE, pourrait aider les autorités de réglementation à être mieux informés sur d'éventuels problèmes de données à caractère personnel.

---

[24] Arrêt Bundeskartellamt, points 54, 58 et 59.
[25] Ibid., point 53 et article 4, paragraphe 3, du TUE.
[26] Voir à cet effet: arrêts du 7 novembre 2013, UPC Nederland (C-518/11, EU:C:2013:709), point 59, et du 1er août 2022, Sea Watch (C-14/21 et C-15/21, EU:C:2022:604), point 156.
[27] Avis du contrôleur européen de la protection des données intitulé «Vie privée et compétitivité à l'ère de la collecte de données massives», https://www.edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_fr.pdf;
avis du contrôleur européen de la protection des données sur une application cohérente des droits fondamentaux à l'ère des données massives», https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf
[28] CEPD, 19 février 2020, Déclaration relative aux incidences des concentrations en matière de vie privée.
[29] Ibidem.
[30] Ibidem.
[31] Voir également Commission européenne, Competition policy brief, April 2024, Non-Price Competition: EU Merger Control Framework and Case Practice, Issue 1, p. 5.

4 S'APPUYER SUR LA COOPÉRATION

4.1 Pourquoi les autorités chargées de la protection des données et les autorités de concurrence devraient coopérer

17. Le CEPD a examiné la question de la coopération entre les autorités, notamment en consultant des experts dans ce domaine et en lançant une enquête pour comprendre comment diverses autorités coopèrent entre elles.

18. Sur cette base, le CEPD a pu tirer les conclusions suivantes: une bonne coopération entre les autorités favorise la cohérence et les synergies entre les décisions prises en matière de concurrence et de protection des données. Cela profite non seulement aux personnes, mais aussi aux entreprises, en améliorant la compréhension des modalités d'application des cadres réglementaires.

19. En outre, alors que la législation et la jurisprudence dans les deux domaines juridiques s'étoffent, la nécessité d'une coopération entre les autorités compétentes concernées pourrait même s'accroître.

4.2 Modèles de coopération existants dans les États membres de l'UE

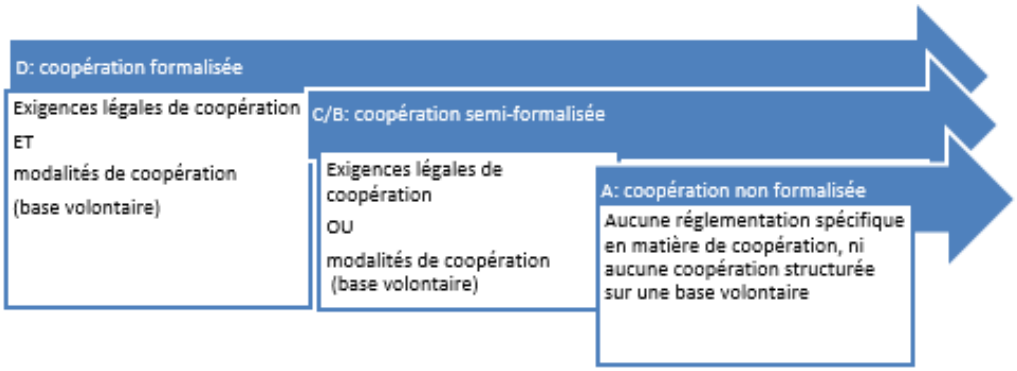
20. Actuellement, le degré de coopération entre les autorités, qui dépend à la fois du cadre juridique et d'autres éléments, tels que le niveau de confiance mutuelle entre autorités, varie considérablement d'un État membre à un autre et n'est pas harmonisé par le droit de l'Union. Le CEPD a procédé à une analyse des modèles de coopération existants dans les États membres de l'UE en septembre 2023. Le tableau suivant se dégage en fonction du degré de formalisation de la coopération:

    A. Dans certains États membres, aucune disposition juridique spécifique n'impose ou ne permet une coopération entre les APD et les autorités de concurrence, et il n'existe aucune coopération régulière et structurée sur une base volontaire. La coopération se déroule de manière informelle au moyen de consultations ad hoc, par exemple dans le cadre de procédures administratives, d'enquêtes sectorielles, de projets conjoints occasionnels dans des domaines où les compétences réglementaires se chevauchent ou de la rédaction de documents d'orientation.

    B. La coopération peut également être menée sans base juridique spécifique dans le droit national, sur la base de modalités de coopération régulière, coordonnée et structurée. Celles-ci peuvent être définies dans des protocoles de coopération, des déclarations communes ou des protocoles d'accord élaborés conjointement. Ces modalités, qui ne sont pas forcément juridiquement contraignantes, détaillent des aspects tels que des ateliers conjoints, des formations, des événements, des réunions régulières et des échanges de bonnes pratiques.

    C. Dans certains États membres, des exigences juridiques régissent explicitement la coopération. La forme précise de coopération varie en fonction du cas d'espèce. Ce type de coopération débouche généralement sur l'élaboration d'avis concernant des affaires à la demande de l'autre autorité.

    D. Le niveau de coopération formalisée ou structurée est le plus élevé dans les États membres disposant à la fois d'exigences juridiques et de modalités pratiques de coopération entre les autorités.



21. Même un niveau minimal de coopération formalisée permet aux autorités de coopérer dans le cadre de contacts occasionnels sur des questions spécifiques. Dans certaines circonstances, ces autorités peuvent dans certains cas être tenues de coopérer sur la base du principe de coopération loyale.

4.3 Moyens d'améliorer la coopération

22. Il pourrait s'avérer bénéfique que les autorités apprennent les unes des autres, recensent les questions d'intérêt commun et les domaines d'interaction possibles, indépendamment des consultations ad hoc, réduisent autant que possible les obstacles à la coopération et élaborent conjointement des actions stratégiques. À cette fin, des ateliers, des réunions informelles ou régulières ou des groupes de travail spéciaux constitués d'experts pourraient être convenus dans des **cadres de coopération**, tels que des accords administratifs, des déclarations communes ou des protocoles d'accord. Ces instruments pourraient également définir des principes, des méthodes et des règles clés de coopération entre les autorités (par exemple, en ce qui concerne la forme de communication à utiliser, les délais de réponse - y compris toute objection pertinente, des lignes directrices communes, des recommandations, etc.), ainsi que l'examen des décisions et sanctions adoptées précédemment par chacune des autorités. Ces accords pourraient également régir la quantité d'informations partagées, ce qui peut être échangé (par exemple, des données à caractère personnel) et le degré de coordination attendu entre les autorités concernées sur un sujet donné.

23. Compte tenu du cadre constitutionnel et administratif de l'État membre concerné, le **législateur national et/ou le gouvernement devraient également être conscients de la nécessité pour les autorités et organismes de réglementation de coopérer plus étroitement dans le secteur numérique**. Cela pourrait également être important pour veiller à ce que les autorités disposent des outils et des ressources nécessaires pour pouvoir coopérer de manière efficiente et pour s'attaquer aux exigences légales susceptibles d'empêcher les autorités de partager des informations et, partant, de coopérer efficacement au cours des enquêtes.

24. Au sein des autorités, des mesures internes telles que la mise en place d'une équipe spécifiquement chargée de coordonner les tâches de coopération et de faire office de **point de contact unique** pour les autres autorités pourraient favoriser la coopération avec d'autres autorités de contrôle. Il pourrait également s'avérer utile que le point de contact bénéficie régulièrement de formations sur le paysage juridique pertinent et les évolutions juridiques connexes de la coopération en général et qu'il participe aux groupes de travail ou réseaux correspondants[32]. En outre, afin de garantir une coopération

[32] Par exemple: le groupe de travail du CEPD sur la concurrence et le droit des consommateurs, le groupe de travail «Citoyens numériques et consommateurs» de l'Assemblée mondiale pour la protection de la vie privée, les échanges avec le réseau de coopération en matière de protection des consommateurs au sein du cadre

efficiente, les autorités devraient **développer une compréhension et une connaissance de base** du cadre réglementaire supervisé par les homologues concernés de l'autre domaine juridique. Par exemple, avant d'entamer des discussions avec une autorité de concurrence sur une question spécifique, les autorités chargées de la protection des données gagneraient à acquérir à titre préliminaire une compréhension de la notion de marché en cause en général, de la question de savoir si certaines entités sur ce(s) marché(s) occupent (ou peuvent occuper) une position dominante, etc.

25. Une **forme de coopération plus structurée et plus régulière** peut être préférable, voire nécessaire, dans certaines situations pour garantir l'application cohérente et efficace des différentes législations de l'UE (voir illustration ci-dessus, C et D). Établir des protocoles de coopération entre les différentes autorités compétentes dans le cadre du devoir de coopération loyale peut être le moyen le plus efficace de garantir des consultations réciproques d'une portée appropriée au moment opportun. Cela peut également aider à éviter les cas de double peine dans les affaires où deux autorités compétentes décident d'infliger des sanctions à la même entité pour le même comportement en vertu de deux ou plusieurs cadres juridiques distincts[33].

26. Enfin, des enquêtes sectorielles conjointes et des enquêtes communes pourraient également être menées, dans la mesure du possible et conformément au cadre juridique applicable, comme une forme de coopération encore renforcée entre les autorités.

5 CONCLUSIONS

27. Promouvoir des synergies entre les autorités chargées de la protection des données à caractère personnel et les autorités de concurrence peut améliorer la capacité des deux régimes à protéger les personnes concernées et les utilisateurs. En pratique, la place des données à caractère personnel et des règles applicables à leur traitement devient de plus en plus centrale à mesure que les modèles commerciaux des entreprises évoluent. Il est donc essentiel d'examiner les moyens d'accroître la cohérence entre des réglementations qui sont distinctes mais interagissent, en gardant à l'esprit les incidences de leur application incohérente tant au niveau individuel qu'au niveau sociétal. Cela nécessitera en particulier une meilleure compréhension de la relation entre les notions employées dans les domaines de la protection des données et du droit de la concurrence, de manière à renforcer la capacité des autorités chargées de la protection des données à tenir compte du contexte économique, ainsi que la capacité des autorités de concurrence à intégrer dans leurs appréciations et décisions des considérations potentiellement pertinentes en matière de protection des données.

CPC-DPA. Un aperçu des collaborations existantes du CEPD est disponible à l'adresse suivante: https://www.edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_fr.

[33] Arrêt de la Cour de justice du 22 mars 2022, bpost SA / Autorité belge de la concurrence (C-117/20, ECLI:EU:C:2022:202). Selon la CJUE, pour un cumul valable des procédures et des sanctions en vertu des règles sectorielles et du droit de la concurrence, les deux législations en cause doivent poursuivre des objectifs légitimes d'intérêt général (point 44). En outre, pour un cumul valable de poursuites et de sanctions, il faut apprécier s'il existe «*des règles claires et précises permettant de prévoir quels actes et omissions sont susceptibles de faire l'objet d'un cumul de poursuites et de sanctions ainsi que la coordination entre les différentes autorités, si les deux procédures ont été menées de manière suffisamment coordonnée et rapprochée dans le temps et si la sanction le cas échéant infligée à l'occasion de la première procédure sur le plan chronologique a été prise en compte lors de l'évaluation de la seconde sanction*» (point 51).

Pour le comité européen de la protection des données
La présidente

Anu Talus