Contribution à la consultation EDPB

Digital DPO le 30 octobre 2026

1. Observations générales

Lisibilité : Le document est difficile à suivre. On ne voit pas comment l'analyse juridique (section 2) s'articule avec l'analyse technique (section 3). La lecture oblige à des allers-retours. Les conséquences de l'échec d'un critère sont traitées loin du critère lui-même (§ 52, puis § 97-103). Les exemples sont aussi repris plusieurs pages plus loin (ex. 10 et 23 ; ex. 12, 19, 22 et 25 ; ex. 16 et 21).

Cohérence générale : Le texte se contredit sur des points structurants.

L'effet du test n'est pas fixé : pour une même condition, les trois critères satisfaits dans l'une ou l'autre approche, les données sont « considérées sans risque comme anonymes » (résumé, § 3), « regardées comme anonymes » (§ 46, 52) ou « présumées anonymes » (§ 95).

Le § 52 pose que l'échec d'un critère ne rend pas la donnée personnelle ; le § 97 conclut pourtant que l'échec du No Inference exclut l'anonymat.

Le § 89 écarte les acteurs non autorisés lorsque la sécurité est appropriée ; l'ex. 22 retient les pirates malgré une sécurité conforme à l'état de l'art. Le § 88 demande lui aussi de tenir compte des fuites.

Le § 12 fait de la personne pour qui l'anonymisation est voulue le critère de la perspective pertinente ; le § 30 étend ensuite celle-ci à tout acteur malveillant.

L'identification suppose de distinguer la personne et de pouvoir la traiter différemment (§ 19), mais l'ex. 5 (CCTV footage) et le § 25 (adresse mac fingerprinting) se contentent de la distinction.

Positionnements difficiles à comprendre : Plusieurs choix ne sont pas suffisamment justifiés :

- Une donnée anonyme pour une entité devient « indirectement » personnelle pour elle si elle la transmet à un tiers dont on « ne peut exclure » qu'il identifie (§ 21), seuil plus bas que la probabilité « insignifiante » du § 22 ; les arrêts cités (*Breyer*, *Scania*, *SRB*) portaient pourtant sur des transmissions ou des voies d'accès effectives, non simplement possibles ;
- Le §12 tient compte d'une prise en compte relativisée du périmètre des entités concernées (anonymisation pour mon propre usage ou anonymisation pour des tiers définis) en citant *OC c/ Commission*. Cette prise en compte est pourtant abandonnée plus loin dans le texte en prenant en compte des entités dont l'accès est illégitime frauduleux voire criminel **;**

- La justification apportée par l'EDPB pour justifier que le sous-traitant hérite du statut de la donnée est uniquement téléologique (contournement du RGPD), et peu convaincante. D'autant plus que la sous-traitance peut ne concerner qu'un traitement spécifique et ne pas couvrir des traitements distincts pour lesquels le sous-traitant opère en tant que responsable de traitement.
- La motivation du ré-identifiant est écartée comme facteur, mais la valeur des données et les risques qu'il encourt sont pris en compte (§ 31).
- Le § 26 retient l'identification « impossible », là où la CJUE vise l'identification « irréalisable en pratique » (Breyer pt 46) ;
- Le § 30 compte parmi les entités pertinentes cybercriminels, employés malveillants et services de renseignement étrangers : l'analyse de sécurité (art. 32) se confond avec la qualification de la donnée (art. 4§1) ;

2. Mise en œuvre des tests

Ordre des tests : Le texte présente les critères dans l'ordre No Record Isolation, No Linkage, No Inference (§ 54-82), puis traite l'échec de chacun (§ 98-103). L'annexe 1 commence au contraire par la liaison et l'inférence, pour « étendre » les données, avant d'appliquer les trois critères ; elle ne prévoit de rattrapage que si seul le No Record Isolation est violé. On ne sait donc pas quel ordre suivre, ni que faire d'un échec du seul No Linkage.

Quand poursuivre l'analyse : Après un échec, l'analyse complémentaire « peut être nécessaire » (§ 95), le passage à l'approche contextuelle est facultatif (§ 96, 100, 103) et le re-test des données liées n'a pas de terme (§ 102). Le texte ne dit ni quand poursuivre est obligatoire, ni quand on peut s'arrêter.

Exemples : Les exemples éclairent peu les cas difficiles :

- le même jeu de patients sert aux ex. 12, 19, 22 et 25 sous des qualifications différentes, sans que le texte conclue sur son anonymat ;
- l'ex. 12 classe en liaison la révélation d'un attribut commun à un groupe, que l'ex. 19 traite comme une inférence ;
- l'ex. 13 (« Connor aime le vert ») est trop simple pour guider un cas réel ;
- l'ex. 22 retient les pirates mais écarte les proches, selon un raisonnement difficile à reproduire.

Seuils : Les seuils qui décident de l'issue ne sont pas définis : probabilité « insignifiante » (§ 22), lien établi « avec certitude ou forte probabilité » (§ 60), agrégation « correcte » (§ 58), résultat « suffisamment proche » avec une confiance « suffisante » (§ 87), « marges de sécurité adéquates » (§ 88). Faute d'ordre de grandeur ou de métrique de référence, le texte ne clarifie

pas l'avis 05/2014 sur ce point. **Les critères ne produisent donc pas un résultat binaire, ce qui prive le test de la sécurité juridique attendue et rend l'ensemble inconsistant.**

No Inference : un test quasi impraticable. Une inférence est « spécifique » si l'information inférée se rapporte à une personne identifiée ou identifiable, c'est-à-dire si c'est déjà une donnée personnelle (§ 67). Le critère suppose donc acquis ce qu'il doit établir. S'y ajoutent l'exigence d'un effet sur les droits et intérêts (§ 67) et une preuve de non-dépendance qui suppose de conserver le jeu d'origine (§ 71), que le § 39 invite à supprimer. Or l'échec de ce critère exclut directement l'anonymat (§ 97).

En raisonnant par l'absurde, l'application du critère de No inference conduira immanquablement à considérer que toute donnée peut hypothétiquement conduire tout tiers à qualifier une personne identifiable ou identifier.

3. Questions

1. Le sous-traitant raisonne depuis la perspective du responsable (§ 15), le prestataire indépendant depuis la sienne (ex. 4). Quelle perspective retenir pour un prestataire qui agit à la fois pour le compte d'un client et pour ses propres finalités ?

2. L'EDPB peut-il donner des seuils ou des métriques de référence pour apprécier une probabilité « insignifiante » ou une confiance « suffisante » (§ 22, 87) ?

3. Le § 12 fait dépendre la perspective pertinente de la personne pour qui l'anonymisation est voulue ; le § 30 y ajoute tout acteur malveillant. Laquelle de ces règles délimite les entités à prendre en compte ?

4. Le test du § 71 b) suppose de conserver le jeu d'origine, que le § 39 invite à supprimer. Comment prouver après suppression qu'une inférence ne repose pas sur les données?

5. Le § 21 rend la donnée personnelle, y compris pour l'émetteur, dès que l'identification par un destinataire « ne peut être exclue » ; le § 22 exige une probabilité non « insignifiante ». Quel seuil s'applique, faut-il un transfert effectif comme dans les arrêts cités, et quelles obligations pèsent alors sur l'émetteur ?

6. Le § 89 écarte les acteurs non autorisés lorsque la sécurité est appropriée ; les § 30 et 88 et l'ex. 22 les retiennent. Faut-il en tenir compte lorsque la sécurité est conforme à l'état de l'art ?

7. Quel effet concret ont les engagements contractuels de non-ré-identification sur l'évaluation (§ 34, 90) ? la formulation retenue laisserait penser que les accords entre les entités n'apportent pas de protection effective contre un risque de ré-identification. Cette position n'irait-elle pas à l'encontre de l'essence de l'article 28 du RGPD (ou art.26) en le privant de tout effet utile ?

Conclusion

Nous nous attendions à une approche précise du droit apportant une sécurité juridique aux acteurs traitant des données personnelles et à ceux traitant des données dérivées de données personnelles suite à l'application de techniques éprouvées protégeant les personnes d'éventuels risques liés à l'utilisation desdites données après leur collecte.

Après leur analyse et leur lecture, le sentiment et les craintes que nous avons sur la publication du document est que l'objectif d'éviter le contournement du RGPD a conduit les rédacteurs à une assimilation de notions distinctes dans le droit pour éviter que l'anonymisation soit possible en retenant des critères d'exclusion flous ou dans des cas d'utilisation illégitimes.

Cette approche rend le document particulièrement critiquable, notamment dans la mesure où il rend « potentiellement personnelles » des données qui jusqu'alors n'entraient pas dans le scope de la notion de données personnelles que ce soit dans le texte ou dans les décisions de la CJUE.