Chambre Contentieuse

Décision sur le fond 21/2022 du 2 février 2022

Traduction non officielle du néerlandais

Numéro de dossier : DOS-2019-01377

Concerne : Plainte concernant Transparency & Consent Framework

La Chambre Contentieuse de l'Autorité de protection des données, composée de M. Hielke Hijmans, président, et de MM. Yves Poullet et Frank De Smet ;

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après RGPD;

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après LCA);

Vu le règlement d'ordre intérieur tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au Moniteur belge le 15 janvier 2019 ;

Vu les pièces du dossier ;

a pris la décision suivante :

Les plaignants : M. Johnny Ryan, M. Pierre Dewitte et M. Jef Ausloos, Mme Katarzyna Szymielewic ayant mandaté l'ONG Panoptykon pour agir en son nom, ainsi que les ONG Bits of Freedom et La Ligue des Droits de l'Homme, tous représentés par Maîtres Frédéric Debusseré et Ruben Roex, ainsi que M. Bruno Bidon, ci-après « les plaignants » ;

La défenderesse : IAB Europe, dont le siège social est situé [...] 1040 Bruxelles, ayant pour numéro d'entreprise [...], représentée par Maîtres Frank Judo et Kristof Van Quathem, ci-après « la défenderesse ».

Table des matières

A. Faits et procédure

A.1. - Plaintes contre Interactive Advertising Bureau Europe

1. Au cours de l'année 2019, une série de plaintes ont été déposées contre Interactive Advertising Bureau Europe (ci-après IAB Europe), pour avoir enfreint diverses dispositions du RGPD en matière de traitement à grande échelle de données à caractère personnel. Les plaintes portaient notamment sur les principes de légalité, d'adéquation, de transparence, de limitation de la finalité, de restriction du stockage et de sécurité, ainsi que sur la responsabilité.

2. Neuf plaintes identiques ou très similaires ont été déposées, dont quatre directement auprès de l'autorité de protection des données (ci-après dénommée « APD ») et cinq via le système IMI auprès d'autorités de contrôle d'autres pays de l'UE.

3. Le SService d'inspection a également effectué des enquêtes de sa propre initiative, conformément à l'article 63, paragraphe 6, de la LCA. Les plaintes portant sur le même objet et étant dirigées contre la même partie (IAB Europe), sur la base des principes de proportionnalité et de nécessité dans la conduite des enquêtes (article 64 de la LCA), le Service d'inspection a fusionné les dossiers susmentionnés en une seule affaire sous le numéro de dossier DOS-2019-01377.

4. Les plaignants ont accepté cette fusion, ainsi que la demande de la Chambre Contentieuse de fusionner leurs conclusions et de les présenter de manière conjointe, dans l'intérêt de l'économie et de l'efficacité de la procédure.

5. Dans cette affaire internationale, quatre plaignants, dont l'ONG Ligue des Droits Humains, sont domiciliés en Belgique, un en Irlande, quatre dans différents États de l'UE, représentés par l'ONG Panoptykon basée en Pologne, et un plaignant est représenté par l'ONG Bits of Freedom basée aux Pays-Bas.

6. Conformément à l'article 4(1) de la LCA, l'Autorité de protection des données est chargée de contrôler les principes de protection des données contenus dans le RGPD et dans d'autres lois contenant des dispositions sur la protection du traitement des données à caractère personnel.

7. Conformément à l'article 32 de la LCA, la Chambre Contentieuse est l'organe administratif de résolution des litiges de l'APD[1].

8. Conformément aux articles 51 et suivants du RGPD et de l'article 4(1) de la LCA, il appartient à la Chambre Contentieuse, en tant qu'organe administratif de règlement des litiges de l'APD, d'exercer un contrôle effectif sur l'application du RGPD et de protéger les libertés et

[1] La nature administrative des litiges devant la Chambre Contentieuse a été confirmée par la Cour des Marchés. Voir notamment l'arrêt du 12 juin 2019, publié sur le site internet de l'APD, ainsi que la décision 17/2020 de la Chambre Contentieuse.

droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel et de faciliter la libre circulation des données à caractère au sein de l'Union européenne. Ces tâches sont expliquées plus en détail dans le plan stratégique et les plans de gestion de l'APD, établis conformément à l'article 17(2) de la LCA.

9. De plus, pour ce qui est de l'IMI, l'article 56 du RGPD dispose : « *Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant 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.* »

10. L'article 4.23 du RGPD précise la notion de traitement transfrontalier dans les termes suivants : « *un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou (b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ;* »

11. La défenderesse a son seul siège social en Belgique, mais ses activités ont un impact significatif sur des parties prenantes dans plusieurs États membres, y compris les plaignants en Irlande, en Pologne et aux Pays-Bas, ainsi qu'en Belgique. La Chambre Contentieuse tire sa compétence d'une lecture combinée des articles 56 et 4(23)(b) du RGPD. L'APD a été saisie par les autorités de protection des données polonaise, néerlandaise et irlandaise à la suite d'une plainte qui leur a été adressée par les plaignants conformément à l'article 77.1 du RGPD. Elle déclare qu'elle est l'autorité de contrôle principale (article 60 du RGPD).

12. Les autorités de contrôle suivantes ont indiqué leur volonté d'agir en tant qu'autorités de contrôle concernées (« Concerned Supervisory Authority » -« CSA » ci-dessous) : Pays-Bas, Lettonie, Italie, Suède, Slovénie, Norvège, Hongrie, Pologne, Portugal, Danemark, France, Finlande, Grèce, Espagne, Luxembourg, République tchèque, Autriche, Croatie, Chypre et Allemagne (Berlin, Rhénanie-Palatinat, Rhénanie-du-Nord-Westphalie, Sarre, Basse-Saxe, Brandebourg, Mecklembourg-Poméranie occidentale, Bavière), Irlande.

13. Au cours de la procédure, d'autres plaintes, dont l'objet est très similaire à celui de la présente affaire, ont été envoyées à l'APD belge par les APD maltaise, roumaine, croate, grecque, portugaise, suédoise, chypriote et italienne. Ces plaintes ne font pas partie de la présente procédure.

A.2. - La langue de la procédure : Décision interlocutoire 01/2021 modifiée par la décision interlocutoire 26/2021 du 23 février 2021.

14. Le 13 octobre 2020, la Chambre Contentieuse a envoyé une lettre aux parties, conformément à l'article 98 de la loi DPA, les informant de la langue de la procédure (le français), et les invitant à présenter leurs conclusions écrites.

15. En réponse à la demande des plaignants du 27 novembre 2020, et compte tenu du caractère international de cette affaire, la Chambre Contentieuse a rendu le 8 janvier 2021 la décision interlocutoire 01/2021 concernant la langue de la procédure. Suite à un recours des plaignants devant la Cour des Marchés, cette décision interlocutoire a été modifiée le 23 février 2021 (décision interlocutoire 26/2021).

16. En vertu de cette dernière décision interlocutoire, fondée sur un accord avec les parties, la correspondance de l'APD avec les parties se fait en néerlandais et les décisions interlocutoires et finale de la Chambre Contentieuse sont en néerlandais. Néanmoins, la Chambre Contentieuse fournit aux parties une traduction française et une traduction anglaise de la décision finale.

17. Toutefois, les parties sont libres d'utiliser la langue de leur choix (néerlandais, français ou anglais) dans la procédure devant la Chambre Contentieuse, que ce soit par écrit ou oralement. Dans le cas d'IAB Europe, il s'agit du français ou de l'anglais. L'APD n'est pas responsable des traductions des documents de procédure soumis par une partie pour le compte de l'autre.

18. Enfin, la Chambre Contentieuse souligne qu'elle utilise parfois la terminologie anglaise dans cette décision, dans les cas où la traduction en néerlandais réduirait la compréhensibilité de la décision.

A.3. - RTB et TCF

19. En substance, cette affaire concerne, d'une part, la conformité du système du TCF avec le RGPD et, d'autre part, la responsabilité d'IAB Europe, la défenderesse dans cette procédure, et des autres différents acteurs impliqués. En outre, il s'agit également de l'impact du TCF sur ce que l'on appelle le système d'enchères en temps réel (Real-Time Bidding (RTB)). Compte tenu de la complexité du RTB, celui-ci est présenté ci-dessous.

A.3.1. - Définitions et fonctionnement du système d'enchères en temps réel (Real-Time Bidding -RTB-)

20. Contrairement à la publicité « traditionnelle », où les parties impliquées déterminent manuellement et contractuellement les modalités de l'échange d'informations, la publicité en ligne se fait généralement de manière essentiellement automatique et en coulisse, par

le biais de méthodes de « *publicité programmatique* », dont l'enchère en temps réel (RTB) est le principal système[2].

21. L'enchère en temps réel est définie dans la littérature juridique comme « un réseau de partenaires qui permet des applications de big data dans le domaine organisationnel du marketing afin d'améliorer les ventes d'espaces publicitaires prédéterminés grâce à un marketing en temps réel basé sur les données et à une publicité personnalisée (comportementale) ».[3].

22. Les enchères en temps réel désignent l'utilisation d'une enchère en ligne automatisée et instantanée pour la vente et l'achat d'espaces publicitaires en ligne. Plus précisément, cela signifie que lorsqu'un individu accède à un site web ou à une application qui contient un espace publicitaire, en coulisse, grâce à un système d'*enchères* en ligne automatisé et à des algorithmes, des sociétés technologiques représentant des milliers d'annonceurs peuvent instantanément (en *temps réel*) faire une *offre* pour cet espace publicitaire afin d'afficher des publicités ciblées spécifiquement adaptées au profil de cet individu.

23. Les enchères en temps réel fonctionnent en coulisse sur la plupart des sites web commerciaux et sur les applications mobiles. Des milliers d'entreprises sont impliquées et reçoivent des informations sur la personne qui visite le site web. De cette manière, des milliards de publicités sont mises aux enchères chaque jour.

24. Dans un système d'enchères en temps réel, plusieurs parties sont impliquées[4] :

    A. Les entreprises ou organisations qui ont créé et gèrent le système d'enchères en temps réel concerné, notamment en définissant ses *politiques/gouvernance* et protocoles techniques. Les principales sont :

        a. le système « *OpenRTB* » et le « *Advertising Common Object Model* » (AdCOM) qui lui est associé, créés par IAB Technology Laboratory, Inc. (en abrégé « IAB Tech Lab ») et Interactive Advertising Bureau, Inc. (en abrégé « IAB »), tous deux basés à New York ;

        b. le système « Authorised Buyers » (« *Acheteurs autorisés* ») créé par Google.

    L'OpenRTB est un protocole standard qui vise à simplifier l'interconnexion entre les fournisseurs adtech d'espaces publicitaires, les publishers (bourses d'échange d'annonces, plateformes côté vente ou réseaux travaillant avec les publishers) et les acheteurs concurrents d'espaces publicitaires (soumissionnaires, plateformes côté demande ou

[2] M. VEALE, FR. ZUIDERVEEN BORGESIUS, « Adtech and Real-Time Bidding under European Data Protection Law », German Law Journal*, 31 juillet 2021,* p. 8-10.

R. VAN EIJK, « Web Privacy Measurement in Real-Time Bidding Systems - A Graph-Based Approach to RTB system classification », 2019, p. 140: « *un réseau de partenaires permettant des applications de big data dans le domaine organisationnel du marketing afin d'améliorer les ventes par un marketing en temps réel basé sur les données et une publicité personnalisée (comportementale)* », disponible sur available at https://ssrn.com/abstract=3319284; [3] M. VEALE, FR. ZUIDERVEEN BORGESIUS, IBIDEM, P. 3.

[4] *Ibidem.*

réseaux travaillant avec les annonceurs). L'objectif global de l'OpenRTB est d'établir un langage commun pour la communication entre les acheteurs et les ad tech vendors d'espaces publicitaires[5].

B. Du « côté offre », on trouve :

   a. Les entreprises qui possèdent un site web ou une application avec des espaces publicitaires. Dans le jargon RTB, ces entreprises sont appelées « *publishers* ».

   b. Les sociétés exploitant une plateforme en ligne automatisée grâce à laquelle les *publishers* peuvent optimiser la valeur et le volume de leurs ventes d'espaces publicitaires en signalant la disponibilité de leur espace publicitaire à afficher à une personne concernée et en demandant qu'une ou plusieurs demandes d'enchères soient faites pour cet espace publicitaire. Dans le jargon RTB, ces sociétés sont appelées « *Sell-Side Platforms* »(« SSPs »). Les SSP fournissent l'inventaire disponible de leurs publishers aux différents ad exchanges du marché et éventuellement aux réseaux publicitaires et autres « *Demand-Side Platforms* » (« DSPs » -*voir ci-dessous*-). Les SSP les plus avancés fonctionnent en temps réel. Dès qu'un espace publicitaire est appelé lorsqu'une page est consultée sur le site d'un éditeur, le SSP recherche la meilleure offre sur ce type d'espace publicitaire en fonction du profil du visiteur détecté, et diffuse automatiquement l'annonce correspondante[6].

C. Du « côté demande », on trouve :

   a. Les entreprises qui souhaitent afficher des publicités pour leurs produits ou services de manière ciblée aux visiteurs de sites web et aux utilisateurs d'applications (les annonceurs).

   b. Les entreprises exploitant une plateforme en ligne qui permet aux annonceurs et aux agences médias de réaliser et d'optimiser leurs achats d'espaces publicitaires, et sur laquelle sont proposées les annonces des annonceurs[7]. Dans le jargon RTB, ces sociétés sont appelées « *Demand-Side Platforms* » (« DSPs »).

D. Des sociétés, appelées « *Ad Exchanges* », jouent le rôle d'intermédiaires entre elles. Elles réunissent les organisations du côté de l'offre et de la demande et leur permettent de communiquer automatiquement entre elles afin que les DSP puissent répondre aux *demandes d'offres* des SSP.

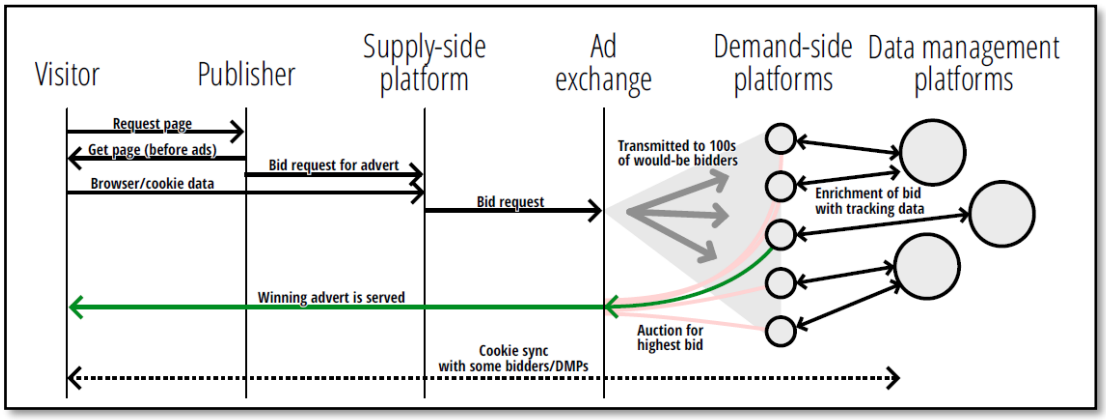
[5] Rapport d'analyse technique du service d'inspection, 6 janvier 2020 (Pièce 53), p. 11.
[6] Rapport d'analyse technique du service d'inspection, 4 juin 2019 (Pièce 24), p. 5-6.
[7] Rapport d'analyse technique du service d'inspection, 4 juin 2019 (Pièce 24), p. 5

E. En outre, il existe ce que l'on appelle des « *Data Management Platforms* » (« DMP ») (plateformes de gestion des données) qui extraient d'énormes quantités et types de données à caractère personnel de sources multiples (telles que des appareils, des cookies, des identifiants mobiles, des pixels, des analyses du comportement de navigation en ligne, des médias sociaux, des données hors ligne, mais aussi de tiers tels que des courtiers en données, etc.), puis centralisent ces données, et enfin les analysent et les catégorisent au moyen d'algorithmes et de l'intelligence artificielle. En utilisant une DMP, un annonceur peut enrichir et combiner les données qu'il possède lui-même sur les clients (potentiels) avec les données qu'il peut obtenir d'une DMP centrale. Ainsi, l'une des principales fonctions d'une DMP est de créer des profils détaillés de consommateurs par l'enrichissement des données afin d'optimiser le ciblage et l'efficacité des campagnes de marketing et de publicité et de proposer des offres personnalisées sur les sites web et dans les applications[8].

25. Une fois qu'un annonceur a établi des profils détaillés de consommateurs par l'intermédiaire d'une DMP, il soumet, par l'intermédiaire de sa DSP, des *demandes d'offres* à des *publishers/SSP* offrant un espace publicitaire correspondant à ces profils de consommateurs.

26. Dans le jargon RTB, les SSP, DSP, Ad Exchanges, annonceurs et DMP sont collectivement appelés « *fournisseurs adtech* ».

27. Schématiquement, cela peut être présenté comme suit[9]:

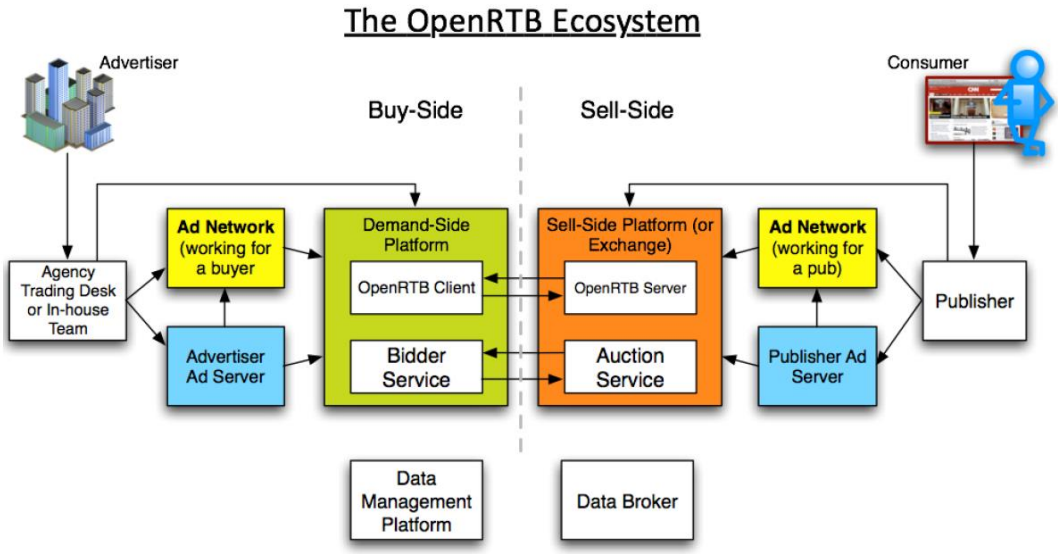


28. Cela peut également être représenté comme suit[10]:

[8] Rapport d'analyse technique du service d'inspection, 6 janvier 2020 (Pièce 53), p. 7.

[9] M. VEALE, FR. ZUIDERVEEN BORGESIUS, « Adtech and Real-Time Bidding under European Data Protection Law », German Law Journal, *31 juillet 2021, p.* 9.

[10] Rapport d'analyse technique du service d'inspection, 4 juin 2019 (Pièce 24), p. 6.



29. Le contenu d'une *bid request*, qui contient des données sur les utilisateurs en ligne, leur appareil et les sites web visités, est capturé par le protocole OpenRTB ou le système Authorised Buyers (acheteurs autorisés). En règle générale, les catégories suivantes de données à caractère personnel peuvent être communiquées aux annonceurs dans le cadre d'une *bid request* [11]:

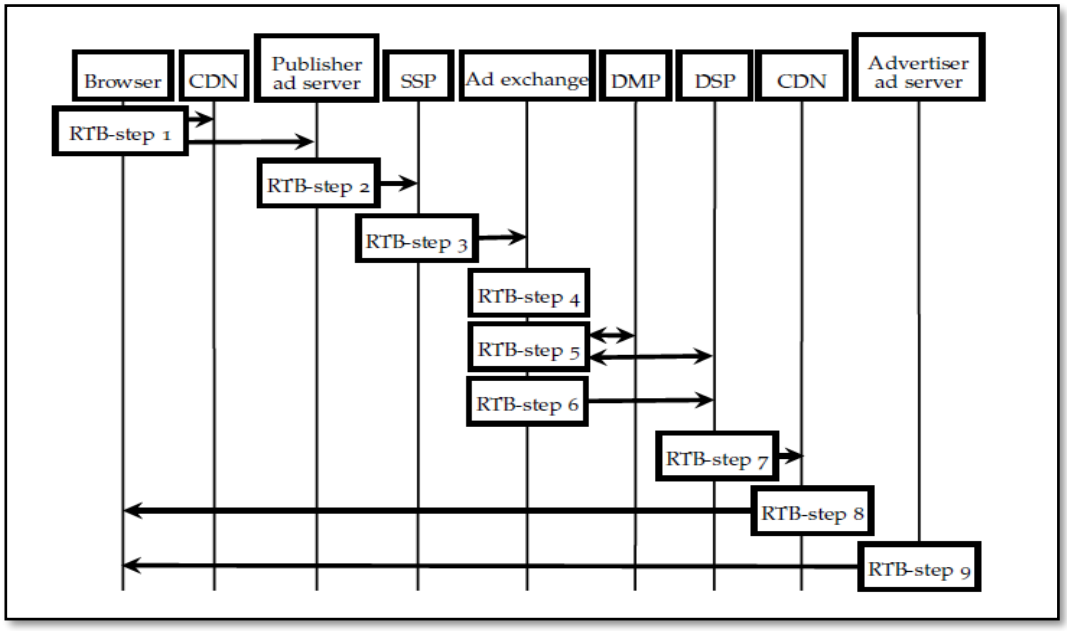
- URL du site visité
- Catégorie ou sujet du site
- Système d'exploitation de l'appareil
- Logiciel et version du navigateur
- Fabricant et modèle de l'appareil
- Opérateur de téléphonie mobile
- Dimensions de l'écran
- Identification unique de l'utilisateur définie par le fournisseur et/ou l'acheteur.
- Identifiant unique de la personne provenant de l'Ad Exchange, souvent dérivé du cookie Ad Exchange.
- L'identification de l'utilisateur d'une DSP, souvent dérivée du cookie de l'Ad Exchange qui est synchronisé avec un cookie du domaine de la DSP.
- Année de naissance
- Genre
- Intérêts
- Métadonnées rendant compte du consentement donné
- Géographie
- Longitude and latitude
- Code postal

30. En conséquence, la Chambre Contentieuse considère que le RGPD s'applique *ratione materiae* au système RTB, dont le protocole OpenRTB et, dans une certaine mesure, le

[11] *Ibidem*, p. 10.

Transparency & Consent Framework (TCF) discuté ci-dessous sont des composants essentiels, puisque les opérations RTB au moyen de *demandes d'offres* impliquent intrinsèquement le traitement de données à caractère personnel.

31. Les différentes étapes et interactions entre les SSP, les DSP et les DMP qui ont lieu dans le système RTB peuvent être résumées comme suit[12] :



i. Un utilisateur final demande une page web ;

ii. Le serveur publicitaire de l'*éditeur* sur la page web sélectionne un SSP ;

iii. Le SSP sélectionne ensuite un *Ad Exchange* ;

iv. L'*Ad Exchange* envoie des *demandes d'offres* à des centaines de partenaires du réseau et leur offre la possibilité de générer une *offre en réponse* ;

v. L'*Ad Exchange* permet aux DMPs et/ou DSPs privilégiés de synchroniser les cookies http ;

vi. L'« *Ad Exchange* » place l'offre gagnante ;

vii. La DSP sert la publicité de l'annonceur ;

viii. La publicité est chargée à partir d'un *CDN* (Content Delivery Network, ou fournisseur de réseau) ;

ix. Le serveur de l'annonceur charge un Javascript pour vérification ;

R.[12] VAN EIJK, « Web Privacy Measurement in Real-Time Bidding Systems- A Graph-Based Approach to RTB system classification », 2019, p. 150-151, disponible sur https://ssrn.com/abstract=3319284.

32. Les *enchères en temps réel* présentent un certain nombre de risques qui découlent de la nature de l'écosystème et de la manière dont les données à caractère personnel sont traitées en son sein. Ces risques comprennent[13] :

- profilage et prise de décision automatisée
- traitement à grande échelle (notamment des catégories spéciales de données à caractère personnel) ;
- utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles ;
- mise en correspondance ou fusion d'ensembles de données ;
- l'analyse ou la prédiction du comportement, de la localisation ou des mouvements des personnes physiques ;
- traitement invisible de données à caractère personnel.

33. En outre, un grand nombre d'organisations — telles que les responsables du traitement, les responsables du traitement conjoints, les sous-traitants ou autres personnes concernées — font partie de l'écosystème. Cela a un impact potentiellement important sur la protection des données. En outre, la plupart des personnes concernées ont une compréhension limitée de la manière dont l'écosystème traite leurs données à caractère personnel.

34. En conséquence, le RGPD s'applique aux traitements effectués dans le cadre du RTB, qui sont d'une nature telle qu'ils peuvent créer un risque important pour les droits et libertés des personnes.

A.3.2. - Cadre de transparence et de consentement d'IAB Europe (Transparency and Consent Framework -TCF-)

35. IAB Tech Lab a conçu le protocole OpenRTB, qui, avec le protocole AdBuyers de Google, est le protocole RTB le plus utilisé dans le monde. IAB Tech Lab, basé à New York aux États-Unis, agit en tant que fournisseur du standard OpenRTB et doit être distingué d'IAB Europe, qui a conçu le Cadre de transparence et de consentement (Transparency and Consent Framework -TCF-).

36. IAB Europe est une fédération qui représente le secteur de la publicité et du marketing numériques au niveau européen. Elle comprend des entreprises membres ainsi que des associations nationales, avec leurs propres entreprises membres. Indirectement, IAB Europe représente environ 5.000 entreprises, dont des grandes entreprises et des membres nationaux[14].

[13] Information Commissioner's Office, « Update report into adtech and real time bidding », 20 juin 2019, p. 9 - https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

[14] Tel qu'indiqué par la PDG de la défenderesse lors de l'audience devant la Chambre Contentieuse, le 11 juin 2021.

37. Selon IAB Europe, la partie défendenderesse dans cette procédure, le TCF assure la *responsabilité* et la transparence de l'OpenRTB. Le TCF constitue un ensemble distinct de politiques (TCF Policies), de technical specifications, de termes et de conditions, créé, géré et administré par IAB Europe, et, selon la défenderesse, devrait être capable d'informer les utilisateurs des intérêts légitimes poursuivis par les annonceurs, ainsi que d'obtenir le consentement valide de ces utilisateurs en ce qui concerne le traitement de leurs données à caractère personnel dans un système d'enchères en temps réel (tel que l'OpenRTB).

38. Bien que l'OpenRTB doive être distingué du TCF, les deux systèmes sont liés. Après tout, IAB Europe prétend que le TCF fournit un cadre opérationnel dans lequel les opérations de traitement des données qui ont lieu sur la base du protocole OpenRTB peuvent être mises en conformité avec le RGPD (et la directive ePrivacy).

39. En ce qui concerne le TCF IAB Europe déclare ce qui suit :

> « *Dans sa forme actuelle, le TCF est une norme de bonnes pratiques intersectorielles qui facilite la mise en conformité du secteur de la publicité numérique avec certaines règles de l'UE en matière de vie privée et de protection des données et qui vise à apporter aux individus une transparence et un contrôle accrus sur leurs données à caractère personnel. Plus précisément, il s'agit d'un « cadre » au sein duquel les entreprises fonctionnent de manière indépendante et qui les aide à satisfaire à l'obligation de disposer d'une base juridique RGPD pour tout traitement de données à caractère personnel et à l'obligation d'obtenir le consentement de l'utilisateur pour le stockage et l'accès aux informations sur un appareil de l'utilisateur en vertu de la directive vie privée et communications électroniques* »[15]

40. De plus, les principaux acteurs au sein du TCF correspondent dans une large mesure aux parties participant à l'OpenRTB (à l'exception des CMP) :

    i. *Publishers*— Parties qui mettent à disposition des espaces publicitaires sur leur site web ou dans leur application et qui sont en contact direct avec les utilisateurs dont les données à caractère personnel sont collectées et traitées. Un *éditeur* peut fournir une CMP (voir ci-dessous) sur son site web ou dans son application pour lui permettre de rechercher et de gérer le consentement des visiteurs/utilisateurs au traitement de leurs données à caractère personnel et de faciliter le fonctionnement du TCF[16]. Les *publishers* décident quels *fournisseurs adtech* peuvent collecter des données sur leur site web et traiter les données à caractère personnel de leurs utilisateurs (et/ou accéder à leurs appareils) et à quelles fins[17].

    ii. *Fournisseurs adtech* — Entreprises qui reçoivent des données à caractère personnel d'*publishers* afin de remplir des espaces publicitaires sur les sites Web

[15] Traduction libre, conclusions en réponse de la défenderesse en date du 25 mars 2021, para. 32.

[16] Information Commissioner's Office, « *Update report into adtech and real time bidding* », 20 juin 2019, p. 11-12https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

[17] Conclusions de la réponse de la défenderesse en date du 25 mars 2021, para. 32.

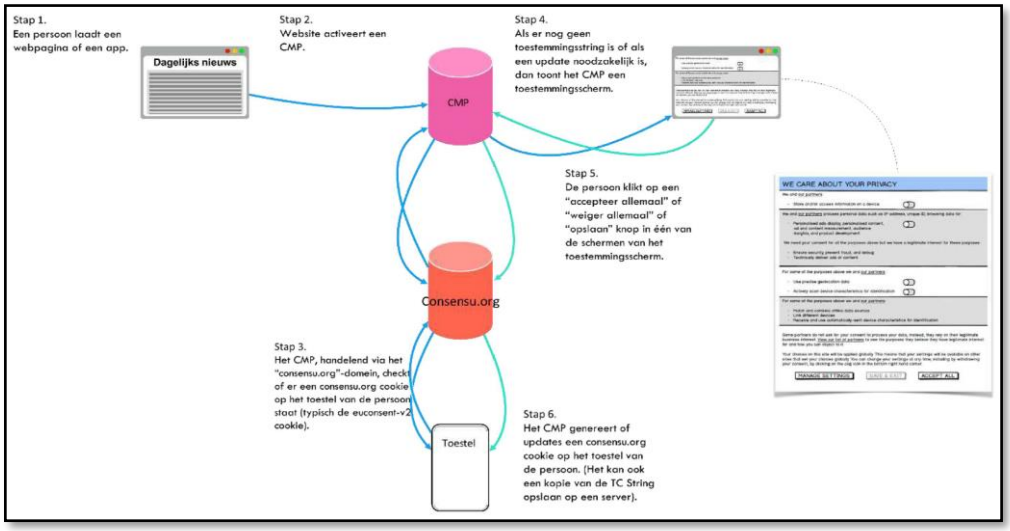
des *publishers* ou dans les applications des publishers, comme les annonceurs, *SSP*, *DSP*, *Ad Exchanges*, et *DMP*.

iii. *Plateformes de gestion du consentement*— Pour le TCF, il existe également des entreprises qui proposent des « *plateformes de gestion du consentement* » (ci-après « Consent Management Platforms » CMP). Concrètement, une CMP prend la forme d'un pop-up qui apparaît lors de la première connexion à un site web pour recueillir le consentement de l'internaute au placement de cookies et d'autres informations d'identification[18].

41. Une partie essentielle de l'intervention d'une CMP est la génération d'une chaîne de caractères composée d'une combinaison de lettres, de chiffres et d'autres caractères. Cette chaîne est appelée « *TC String* » par IAB Europe, pour « *Transparency and Consent String* ». La TC String est destiné à capturer de manière structurée et automatisée les préférences d'un utilisateur lorsqu'il visite un site web ou une application d'un *éditeur* qui a intégré la CMP. Cela concerne notamment la collecte du consentement (ou non) au traitement des données à caractère personnel à des fins de marketing et autres, le partage ou non des données à caractère personnel avec des tiers (*fournisseurs adtech*) et l'exercice ou non du droit d'opposition.

42. Les fournisseurs adtech déchiffrent la TC String pour déterminer s'ils disposent de la base juridique nécessaire pour traiter les données à caractère personnel d'un utilisateur aux fins spécifiées. Grâce à son format de données concis, la CMP peut stocker et récupérer à tout moment les préférences d'un utilisateur et transmettre ces informations aux fournisseurs adtech qui en ont besoin[19].

43. Cela peut être représenté schématiquement comme suit[20] :



[18] Rapport d'analyse technique du service d'inspection, 6 janvier 2020 (Pièce 53), p. 59.
[19] Rapport d'analyse technique du service d'inspection, 6 janvier 2020 (Pièce 53), p. 75.
[20] Conclusions de la défenderesse datée du 18 février 2021, para. 18.

i. Un internaute navigue sur le site d'un *éditeur*, par exemple un site d'information.

ii. L'*éditeur* s'assure qu'une CMP est activée sur son site web ou dans son application lorsque l'utilisateur commence l'utilisation.

iii. La CMP vérifie si une TC String existe déjà pour cet utilisateur ou non. Si une TC String « stocké globalement »[21] est choisi, la CMP contactera le domaine Internet consensu.org géré par IAB Europe pour vérifier à partir de là s'il existe déjà un cookie dit « consensu » sur l'appareil de l'utilisateur. Cela concerne en particulier le cookie *euconsent-v2*.

iv. Si la troisième étape montre que la TC String n'existe pas encore ou n'est pas à jour, dans une quatrième étape, la CMP montrera à l'utilisateur une interface utilisateur où il peut consentir à la collecte et au partage de ses données à caractère personnel.

v. L'internaute fait un choix dans l'interface utilisateur.

vi. La CMP génère la TC *String* et installe un cookie *euconsent-v2* cookie sur le dispositif de l'utilisateur ou met à jour le cookie existant.

A.4. - Rapports du Service d'inspection

A.4.1. - IAB Europe agit en tant que responsable du traitement des données en ce qui concerne le Cadre de transparence et de consentement (Transparency and Consent Framework -TCF) et les opérations de traitement des données à caractère personnel qui s'y rapportent

44. Dans le cadre de cette procédure, le Service d'inspection a concentré son enquête exclusivement sur IAB Europe, que le Service d'inspection a identifié comme le responsable du traitement des données pour le *Cadre de transparence et de consentement* (ci-après, « TCF »). Le Service d'inspection appuie cette première constatation sur le fait que IAB Europe a élaboré le TCF, avec lequel IAB Europe impose des règles contraignantes aux organisations participantes. Selon le Service d'inspection, ces règles contraignantes concernent notamment le traitement des données à caractère personnel dans le cadre de la collecte et du traitement du consentement, ainsi que les préférences des utilisateurs en ligne, en ce qui concerne les finalités du traitement et les *fournisseurs adtech* agréés.

45. Le Service d'inspection fonde son rapport sur deux analyses techniques relatives à la *spécification API Open Realtime Bidding* d'IAB Europe, ainsi qu'aux différents mécanismes de la spécification *OpenMedia* de IAB Tech Lab, notamment le *Cadre de transparence et de consentement*[22].

[21] Également intitulé « consentement à portée globale »

[22] Rapports d'analyse technique du service d'inspection, 4 juin 2019 (Pièce 24) et 6 janvier 2020 (Pièce 53).

46. En ce qui concerne le protocole OpenRTB, le Service d'inspection conclut que IAB Tech Lab, qui a élaboré cette norme technique ouverte et est basé à New York (USA), agit simplement en tant que fournisseur du système vis-à-vis des organisations participantes et ne peut donc pas être considéré comme un responsable du traitement. Contrairement au TCF, l'OpenRTB permet le traitement de données à caractère personnel selon des moyens et des finalités entièrement déterminés par les organisations participantes, mais pas par IAB Tech Lab.

47. Enfin, le Service d'inspection indique que l'APD n'est pas compétente pour le protocole *Authorised Buyers*, qui a été élaboré par Google comme une alternative à la norme OpenRTB.

A.4.2. - Infractions identifiées au RGPD

48. Le Service d'inspection constate que IAB Europe enfreint les dispositions légales et les principes suivants du RGPD avec son *TCF* :

- Articles 5.1.*a* et 5.2 (principes d'équité, de transparence et de responsabilité)
- Article 6.1 (licéité du traitement) ;
- Article 9.1 et 9.2 (traitement portant sur des catégories particulières de données à caractère personnel) ;
- Article 12.1 (transparence des informations, communication et modalités d'exercice des droits des personnes concernées)
- Article 13 (informations à fournir lorsque les données à caractère personnel ont été collectées auprès de la personne concernée)
- Article 14 (informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée)
- Article 24.1 (responsabilité du responsable du traitement) ;
- Articles 32.1 et 32.2 (sécurité du traitement).

49. En dehors du cadre des plaintes, le Service d'inspection constate également des infractions supplémentaires aux dispositions suivantes du RGPD :

- Article 30 (registre des activités de traitement) ;
- Article 31 (coopération avec l'autorité de contrôle)
- Article 24.1 (responsabilité du responsable du traitement) ;
- Article 37 (nomination d'un délégué à la protection des données).

Constatation 1 - IAB Europe utilise à tort l'intérêt légitime comme base légale pour le traitement des données à caractère personnel en vertu du TCF, selon lequel des catégories spéciales de données à caractère personnel peuvent également être traitées dans certains cas.

50. Sur la base des deux versions des Politiques d'IAB *Europe en matière de transparence et de consentement d'IAB Europe*[23] *(ci-après TCF Policies)*, le Service d'inspection note qu'IAB Europe fait peser la responsabilité du respect des principes de transparence et d'équité sur les CMP et/ou les *publishers*. En outre, IAB Europe estime que l'intérêt légitime des organisations participantes constitue une base appropriée pour le traitement des données à caractère personnel dans le cadre du TCF, afin de créer un profil publicitaire des personnes concernées et de leur adresser des publicités personnalisées. Toutefois, selon le Service d'inspection, IAB Europe ne fournit pas de preuves que les intérêts, en particulier les droits et libertés fondamentaux, des personnes concernées ont été dûment pris en considération dans le processus.

51. Par ailleurs, le Service d'inspection note que dans certaines circonstances, des catégories particulières de données à caractère personnel peuvent également être collectées et traitées par les organisations participantes. Par exemple, les organisations participantes pourraient connaître les sites web précédemment visités par une personne concernée, ce qui permettrait de déduire ou de révéler les opinions politiques, les convictions religieuses ou philosophiques, l'orientation sexuelle, les données relatives à la santé ou même l'appartenance syndicale des personnes concernées.

52. Le Service d'inspection considère qu'IAB Europe n'a donc pas respecté de manière adéquate les principes de transparence et d'équité à l'égard des personnes concernées.

Constatation 2 - Les informations fournies ne sont pas conformes aux articles 12.1, 13 et 14 du RGPD.

53. Le Service d'inspection constate également que la politique de confidentialité qu'IAB Europe met à la disposition des personnes concernées n'est pas toujours transparente ou compréhensible, ce qui constitue un manquement aux obligations découlant des articles 12.1, 13 et 14 du RGPD.

54. La politique de confidentialité d'IAB Europe[24] est disponible uniquement en anglais. En outre, la politique de confidentialité contient plusieurs termes qui, sans explication supplémentaire, ne sont pas clairs pour les personnes concernées. À titre d'exemple, le Service d'inspection mentionne les « *services* » et les « *autres moyens* ».

[23] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Pièce 38)
[24] Pièce 41.

55. De plus, selon le Service d'inspection, les informations fournies sont incomplètes et inadéquates. Premièrement, les personnes concernées ne sont pas informées des intérêts légitimes exacts poursuivis par IAB Europe. Deuxièmement, il n'est pas facile pour les personnes concernées de faire la distinction entre les différents destinataires ou catégories de destinataires de leurs données à caractère personnel ; les termes « *tiers* » et « *partenaire* » ne sont pas compréhensibles sans explications supplémentaires. Troisièmement, les personnes concernées ne sont pas informées, d'une part, de la référence à des garanties appropriées ou suffisantes pour le transfert international de leurs données à caractère personnel en dehors de l'EEE ou, d'autre part, de la manière d'en obtenir une copie ou de l'endroit où elle est mise à disposition. Quatrièmement, sur la base de la politique de confidentialité d'IAB Europe, il n'est pas clair pour les personnes concernées que leurs données à caractère personnel peuvent être obtenues par IAB Europe via son TCF[25]. Cinquièmement, les conditions dans lesquelles les personnes concernées doivent fournir leurs données à caractère personnel, notamment si cette collecte est organisée sur la base d'une obligation légale, précontractuelle ou contractuelle, ne sont pas clairement énoncées. Les personnes concernées ne sont pas non plus informées des conséquences possibles d'un refus de fournir leurs données.

56. Par conséquent, la politique de confidentialité ne respecte pas les obligations consacrées par les articles 13 et 14 du RGPD.

Constatation 3 - IAB Europe ne prévoit aucun contrôle de conformité en vertu des règles de la politique TCF

57. Sur la base des deux versions des *TCF Policies*[26], le service d'inspection estime qu'IAB Europe ne contrôle pas suffisamment le respect des règles qu'il a élaborées à l'égard des organisations participantes. En particulier, il serait possible pour une CMP de continuer à échanger des données à caractère personnel avec un éditeur dont il pense raisonnablement qu'il ne respecte pas les règles imposées par le TCF ou la loi[27].

58. Compte tenu du rôle que s'attribue IAB Europe, à savoir celui de *Managing Organization*, ce mépris des risques pour les droits et libertés des personnes concernées indiquerait une violation de l'article 24.1 RGPD ainsi que de l'obligation de fournir une sécurité appropriée pour le traitement des données à caractère personnel, conformément aux articles 32.1 et 32.2 RGPD.

[25] Conditions générales du cadre de transparence et de consentement d'IAB Europe (« Conditions générales ») (pièce 33), p.7.
[26] TCF Policies d'IAB Europe v2019-08-21.3 (Pièce 32) ; TCF Policies d'IAB Europe v2019-04-02.2c (Pièce 38).
[27] TCF Policies d'IAB Europe v2019-08-21.3 (Pièce 32), p11 ; TCF Policies d'IAB Europe v2019-04-02.2c (Pièce 38), p6.

Constatation 4 - IAB Europe n'a pas tenu de registre des traitements.

59. Le Service d'inspection note également qu'IAB Europe ne se considère pas tenue de conserver un registre des activités de traitement, sur la base de l'exception prévue à l'article 30.5 RGPD pour les organisations comptant moins de 250 personnes[28]. Le Service d'inspection souligne également qu'IAB Europe n'a pas fourni initialement au Service d'inspection une copie de son registre des activités de traitement.

60. Ce n'est que dans une deuxième réponse[29] qu'IAB Europe a décidé, par souci d'exhaustivité, de fournir un registre des activités de traitement, bien que l'organisation ne se considère toujours pas soumise à l'obligation prévue à l'article 30.5 RGPD.

Constatation 5 - IAB Europe n'a pas suffisamment coopéré à l'enquête du Service d'inspection

61. Sur la base de la conclusion 4, et en référence au retard avec lequel IAB Europe a répondu aux demandes d'informations supplémentaires du Service d'inspection, le Service d'inspection conclut que le comportement d'IAB Europe dans le cadre de son enquête est en violation de l'obligation de coopérer en vertu de l'article 31 du RGPD.

Constatation 6 - IAB Europe n'a pas désigné de responsable de la protection des données, bien qu'en tant que Managing Organization, elle se réserve le droit d'accéder aux données (à caractère personnel) que les organisations participant au TCF collectent et traitent.

62. IAB Europe affirme[30] qu'elle ne remplit pas les conditions visées à l'article 37.1.*b* du RGPD, car « *IAB Europe est une association professionnelle dont les principales activités consistent à fournir des informations et des outils aux parties prenantes (en particulier, les entreprises) opérant dans le secteur de la publicité numérique, ainsi qu'à fournir des informations au grand public afin d'améliorer leurs connaissances et de les informer de la valeur que la publicité numérique apporte au marché* ». Pour ces raisons, IAB Europe n'a pas désigné de délégué à la protection des données.

63. Selon le Service d'inspection, l'approche d'IAB Europe exposée ci-dessus n'est pas étayée par les faits. IAB Europe a conçu et gère le TCF en sa qualité de *Managing Organization* et, à ce titre, ainsi que selon les termes et conditions du TCF d'IAB Europe[31], a le droit d'accéder à toutes les informations fournies par les organisations participantes, de les stocker et de les traiter.

[28] IAB Europe - Réponse à l'APD belge, 26 juin 2019 (pièce 22), p. 2-3.
[29] Réponse d'IAB Europe au Rapport d'inspection, 10 février 2020 (Pièce 57).
[30] Dans sa réponse au service d'inspection en date du 26/06/2019 et du 20/08/2019, pièces 22 et 29.
[31] Conditions générales du cadre de transparence et de consentement d'IAB Europe (« Conditions générales ») (pièce 33).

A.4.3. - Autres considérations que le Service d'inspection juge pertinentes pour l'appréciation de la gravité des faits.

64. Le Service d'inspection se réfère à l'arrêt de la Cour de Justice de l'Union européenne (ci-après la « Cour de justice » dans l'affaire C-25/17 (Témoins de Jéhovah)[32], dans lequel la Cour a précisé que la définition de responsable du traitement doit être interprétée de manière large afin d'assurer une protection effective et complète des personnes concernées. À cet égard, le Service d'inspection fait valoir qu'IAB Europe tente de se soustraire à sa responsabilité en vertu du RGPD.

65. Le Service d'inspection mentionne les clauses comprises dans le titre 10 « *Responsabilité* » des TCF Terms and Conditions[33], par lesquelles IAB Europe fait peser la responsabilité du traitement des données à caractère personnel collectées par les parties du secteur de la publicité numérique entièrement sur les CMP, les *publishers* et autres *fournisseurs adtech*[34]. En effet, ces clauses prévoient expressément qu'IAB Europe ne garantit en aucune manière que :

- le consentement donné par les CMP ou les *publishers*, partenaires agréés (*fournisseurs adtech globaux*) a été recueilli et traité conformément, entre autres, au RGPD ;
- tout traitement de données effectué dans le cadre ou pour le compte du TCF sera conforme à toutes les lois et réglementations pertinentes, y compris le RGPD.

A.5. - Résumé de la réponse de la défenderesse du 11 février 2021

A.5.1. - IAB Europe n'est pas un responsable du traitement en ce qui concerne le traitement des données à caractère personnel dans le cadre du TCF.

66. IAB Europe réfute, pour l'essentiel, la position du Service d'inspection selon lequel la défenderesse, en sa qualité de *Managing Organization*, agit en tant que responsable du traitement des données à caractère personnel traitées par les participants au TCF.

67. Selon la défenderesse, le TCF n'oblige en aucun cas les organisations participantes à poursuivre certains objectifs, mais vise simplement à fournir les informations, qui doivent être fournies aux personnes concernées conformément aux articles 12 et 13 du RGPD, de manière rationalisée et standardisée au moyen des CMP. En revanche, les finalités réelles

[32] Arrêt de la CJUE du 10 juillet 2018, C-25/17, Témoins de Jéhovah, ECLI:EU:C:2018:551.
[33] Conditions générales du cadre de transparence et de consentement d'IAB Europe (« Conditions générales ») (pièce 33).
[34] En particulier, les *plateformes côté offre*, les *plateformes côté demande*, les *Ad Exchanges*, les annonceurs et les *plateformes de gestion des données*.

du traitement sont déterminées par les organisations participantes, sans l'intervention de la défenderesse.

68. En premier lieu, la défenderesse invoque l'absence de compétence juridique (*ratione personae*) de la part de l'APD, et plus particulièrement du Service d'inspection, pour mener une enquête et contester le TCF. La défenderesse fait également référence à la capacité de l'APD à tenir les véritables responsables du traitement des données, c'est-à-dire les participants au TCF, responsables d'éventuelles infractions au RGPD, le cas échéant.

69. Selon la défenderesse, le TCF en tant que tel n'implique aucun traitement de données à caractère personnel et le rapport d'inspection ne montre pas pour quelles activités de traitement IAB Europe doit être considérée comme le responsable du traitement des données.

70. Deuxièmement, elle avance qu'une définition large de la notion de responsable du traitement, telle que proposée par le Service d'inspection, n'est pas justifiée dans le contexte du TCF, étant donné qu'il existe déjà des responsables du traitement clairement identifiés, d'une part, et compte tenu du fait que le TCF n'a aucune influence sur le traitement des données à caractère personnel qui a lieu dans le contexte du protocole OpenRTB, d'autre part. Plus précisément, la défenderesse mentionne l'absence de toute influence sur les moyens et les fins du traitement au sein du système RTB.

71. La défenderesse considère également que l'arrêt Témoins de Jéhovah précité ne s'applique pas à la situation d'IAB Europe, pour les raisons suivantes :

    - Contrairement à la Communauté des Témoins de Jéhovah, IAB Europe n'organise, ne coordonne et ne promeut en aucune façon le traitement des données à caractère personnel par les participants au TCF.
    - Le traitement des données à caractère personnel par les participants au TCF à des fins de RTB n'est pas dans l'intérêt d'IAB Europe.
    - Les participants au TCF n'ont pas d'objectif commun dans le traitement des données à caractère personnel et ne participent au TCF que dans le but d'atteindre leurs objectifs individuels d'une manière conforme au RGPD.

72. La défenderesse estime que l'arrêt *Wirtschaftsakademie*[35] ne s'applique pas non plus à IAB Europe, car la défenderesse ne diffuse jamais d'informations (c'est-à-dire de publicité) pour le compte ou à la demande d'annonceurs, ne choisit pas de plateforme publicitaire ou d'autre canal de communication et ne fixe pas de paramètres ou de finalités de traitement, contrairement aux participants au TCF qui décident de ces questions. Selon la défenderesse, IAB Europe ne participe pas activement à un traitement RTB et n'est pas à l'origine de ce traitement, de quelque manière que ce soit. Le traitement des données

[35] Arrêt de la CJUE du 5 juin 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.

associé au protocole OpenRTB est effectué exclusivement par les participants au TCF et a donc lieu indépendamment d'IAB Europe ou du TCF.

73. Troisièmement, elle conteste la définition du responsable du traitement telle qu'elle est expliquée dans les lignes directrices publiées par le Conseil européen de la protection des données (EDPB).[36] La défenderesse prétend qu'IAB Europe n'exerce aucun pouvoir discrétionnaire quant aux finalités ou aux moyens du traitement des données à caractère personnel dans le cadre du TCF. En outre, IAB ne traite pas les données à caractère personnel d'une manière qui pourrait être considérée comme « inséparable » ou « inextricablement liée » au traitement des données à caractère personnel par les participants au TCF. De même, le fait que les organisations participantes paient une redevance financière à IAB Europe ne constitue pas, selon la défenderesse, un « avantage mutuel » qui conduirait à une responsabilité de traitement commune.

74. En outre, la défenderesse souligne l'absence de décisions ou de lignes directrices d'autres autorités de contrôle qui pourraient étayer l'avis du Service d'inspection. En particulier, les autorités de contrôle belges, allemandes, françaises et britanniques n'ont pas identifié IAB Europe en tant que responsable (conjoint) du traitement. Plus précisément, la Conférence des autorités indépendantes de protection des données de la Fédération allemande et des Länder a constaté en septembre 2019 qu'IAB Europe agissait uniquement en tant qu'organisation représentative dans le secteur de la *publicité* programmatique. En outre, les autorités de surveillance allemandes ont confirmé leur position en novembre 2019, lorsqu'elles ont annoncé que toute procédure d'exécution liée à des plaintes contre la publicité en ligne devrait être engagée contre les participants au TCF, mais pas contre IAB Europe. Selon la défenderesse, l'autorité de contrôle française (CNIL) a également accepté indirectement l'idée qu'IAB Europe n'était pas responsable des traitements effectués par les participants au TCF. En outre, l'ICO britannique n'aurait jamais identifié IAB Europe comme un potentiel responsable du traitement au sein de l'écosystème RTB, à quelque moment que ce soit.

75. Enfin, la défenderesse évoque les conséquences possibles pour les autres organisations soumises au RGPD si la Chambre Contentieuse devait juger qu'IAB Europe est bien (co-)responsable du traitement des données à caractère personnel dans le cadre du TCF. En particulier, selon la défenderesse, une telle décision signifierait que toute organisation faîtière qui élabore et adopte un code de conduite serait, du seul fait de son rôle de surveillance, considérée conjointement responsable à l'égard des traitements effectués par d'autres organisations conformément à ce code de conduite.

[36] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021.

A.5.2. - Le TCF est conforme au RGPD.

a. Légalité et base juridique

76. Tout d'abord, la défenderesse prétend qu'IAB Europe, contrairement aux organisations participantes, n'est absolument pas tenue d'expliquer au Service d'inspection l'existence d'un intérêt légitime, y compris la mise en balance des intérêts des organisations participantes et des droits et libertés des personnes concernées, puisqu'IAB Europe ne participe pas au TCF et n'agit pas en tant que responsable du traitement.

77. En outre, la défenderesse affirme que l'APD n'est pas autorisée à interdire aux participants au TCF de traiter les données à caractère personnel des personnes concernées sur la base d'un intérêt légitime. Au contraire, l'appréciation du bien-fondé des intérêts légitimes invoqués par les participants doit se faire au cas par cas, et ne peut donc être interdite à l'avance et de manière absolue par l'APD.

78. En ce qui concerne les allégations selon lesquelles IAB Europe traite des catégories particulières de données à caractère personnel dans le cadre du TCF, ou serait coresponsable du traitement de ces données à caractère personnel par les organisations participantes, la défenderesse souligne que ces catégories de données à caractère personnel ne peuvent, le cas échéant, être traitées que dans le cadre de l'OpenRTB, par opposition au TCF. La défenderesse renvoie à cet égard aux TCF Policies, qui interdisent expressément l'utilisation du TCF pour traiter des catégories spéciales de données à caractère personnel.

b. Transparence

79. Compte tenu du fait qu'IAB Europe n'agit pas en tant que responsable du traitement des données à caractère personnel traitées à des fins de RTB, la défenderesse fait valoir qu'on ne peut pas non plus attendre d'elle qu'elle informe les personnes concernées conformément aux articles 12 et 13 du RGPD.

80. En outre, la défenderesse fait valoir que la politique de confidentialité que le Service d'inspection invoque comme preuve d'éventuelles violations du principe de transparence est applicable exclusivement au traitement des données à caractère personnel collectées sur les différents sites Internet exploités par la défenderesse, ainsi qu'aux données à caractère personnel collectées dans le cadre des organisations participantes (en particulier, les coordonnées des représentants de ces organisations). En d'autres termes, la politique de confidentialité à laquelle se réfère le Service d'inspection n'a, selon la défenderesse, aucun rapport avec les activités de traitement dans le cadre du protocole OpenRTB.

81. La défenderesse conteste également toute allégation selon laquelle IAB Europe, en sa qualité de Managing Organization, se réserve le droit d'accéder aux données à caractère personnel collectées et échangées par les organisations participantes dans le cadre du TCF

et du protocole OpenRTB. IAB Europe affirme que cette hypothèse ne repose sur aucune preuve et est due à une interprétation erronée de la possibilité offerte à la défenderesse de traiter les données à caractère personnel des représentants des organisations participantes.

82. En outre, la défenderesse considère qu'elle est en droit de proposer la politique de confidentialité exclusivement en anglais, étant donné que le public cible est principalement constitué d'acteurs professionnels et B2B. La défenderesse souligne que le droit belge ne prévoit aucune obligation de mettre à disposition une politique de confidentialité en français ou en néerlandais et que, par ailleurs, la Belgique n'a pas fait usage de la possibilité d'adopter des exigences supplémentaires concernant l'utilisation de la langue dans le cadre de la directive européenne sur les droits des consommateurs[37].

c. Sécurité

83. La défenderesse fait valoir que les accusations concernant l'absence de mesures techniques et organisationnelles pour protéger les données à caractère personnel dans le cadre du TCF ne sont pas fondées.

84. Tout d'abord, la défenderesse estime qu'IAB Europe n'est pas soumise aux articles 24 et 32 du RGPD en ce qui concerne les traitements de données effectués au sein du TCF, car l'organisation n'est pas un responsable du traitement.

85. Deuxièmement, les TCF Policies d'IAB Europe prévoient que les participants au TCF doivent signaler à IAB Europe les infractions aux règles du TCF. Une fois encore, la défenderesse prétend que le Service d'inspection interprète mal les TCF Policies, notamment en accordant aux CMP le droit de mettre fin à la coopération si elles considèrent qu'un éditeur ne respecte pas les règles, sans subir aucun désavantage contractuel. En outre, la défenderesse note que les infractions aux règles prévues par le TCF peuvent toujours être signalées aux autorités de contrôle, qui prendront alors des mesures si elles le jugent nécessaire.

d. Transfert international de données à caractère personnel

86. IAB Europe réfute les allégations des plaignants concernant le transfert international de données à caractère personnel dans le cadre du TCF. La défenderesse relève à cet égard que ces allégations ne sont pertinentes que dans le contexte du protocole OpenRTB, qui n'est pas en cause dans la présente affaire. Par ailleurs, IAB Europe ne peut être tenue responsable du transfert dans le cadre du protocole OpenRTB.

[37] Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, JO L 304/64.

A.5.3. - IAB Europe n'est pas soumise à l'obligation de tenir un registre des traitements.

87. La défenderesse souligne qu'elle peut invoquer l'exception prévue à l'article 30.5, notamment le fait que l'organisation n'est pas tenue de tenir un registre des activités de traitement, car IAB Europe n'est pas un responsable du traitement des données en ce qui concerne les activités de traitement effectuées au sein du TCFF et, en outre, l'organisation compte moins de 250 employés. Néanmoins, la défenderesse souligne sa propre initiative d'établir un registre et de le soumettre au Service d'inspection, ainsi que le fait que ce registre ne concerne pas les activités de traitement relatives au TCF.

A.5.4. - IAB Europe n'est pas tenue de désigner un délégué à la protection des données.

88. Compte tenu de la nature et de la portée des activités de traitement effectuées par l'organisation, la défenderesse indique qu'IAB Europe n'est pas tenue de désigner un délégué à la protection des données, les critères énoncés à l'article 37 du RGPD n'étant pas remplis.

A.5.5. - IAB Europe a coopéré avec le Service d'inspection.

89. La défenderesse réfute les allégations de coopération insuffisante avec l'enquête, notant que les délais imposés par le Service d'inspection aux parties à une enquête ne sont en aucun cas déterminés par la loi, mais doivent être le résultat d'une évaluation raisonnable et doivent tenir compte des circonstances spécifiques du cas. *En l'espèce*, la défenderesse estime qu'IAB Europe a toujours coopéré de bonne foi et fourni des informations et des réponses dans le but de clarifier son statut par rapport au TCF et de démontrer sa conformité au RGPD, dans la mesure où il s'applique à IAB Europe.

90. En outre, la défenderesse observe que le devoir de coopération prévu à l'article 31 du RGPD ne peut en aucun cas être interprété comme une obligation de fournir une documentation conformément aux dispositions du RGPD que la défenderesse ne considère pas comme nécessaire.

A.5.6. - Il n'y a pas de circonstances aggravantes au détriment d'IAB Europe.

91. Enfin, IAB Europe conteste la conclusion du Service d'inspection selon laquelle le refus de la défenderesse de reconnaître qu'IAB Europe agit en tant que responsable du traitement, ainsi que le volume important de données à caractère personnel traitées et d'organisations participantes, peuvent être considérés comme des circonstances aggravantes.

92. La défenderesse se réfère à l'absence de preuve claire dans le rapport d'enquête que ces circonstances sont aggravantes et conclut que les allégations sont dues à une connaissance insuffisante du fonctionnement du TCF. Par conséquent, la défenderesse

demande à la Chambre Contentieuse de ne pas tenir compte de l'avis du Service d'inspection.

A.6. - Résumé des conclusions des plaignants du 18 février 2021

A.6.1. - IAB Europe est le responsable du traitement pour le TCF.

a. Traitement de données à caractère personnel dans le TCF

93. Les plaignants font valoir qu'un numéro d'identification unique, tel que la TC String générée et stockée dans un cookie, est une donnée à caractère personnel au sens de l'article 4, paragraphe 1, du GDPR, une position qui a également été expressément confirmée par la jurisprudence antérieure au RGPD.

94. Toutefois, selon les plaignants, la TC String est plus qu'un simple identifiant unique, car IAB Europe l'utiliserait également pour collecter des informations concernant les applications qu'une personne concernée utilise et les sites web qu'elle visite. Cela pourrait également révéler des données sensibles sur les personnes concernées au sens de l'article 9 du RGPD.

95. En outre, la génération de la TC String constitue en soi, sans doute aucun, un traitement de données à caractère personnel. Le problème en question est la création automatisée, par une CMP membre du TCF, d'un ensemble unique et lié de caractères destinés à saisir les préférences d'un utilisateur spécifique concernant les échanges de données autorisés avec les annonceurs.

96. Le partage de la TC String avec les CMP se fait, selon les plaignants, de deux manières :

    a. en stockant la TC String dans un *cookie de consentement* global partagé sur le domaine Internet IAB Europe *consensu.org* ; ou

    b. en stockant la TC String dans un système de stockage choisi par la CMP s'il s'agit d'une autorisation spécifique au service.

97. Selon les plaignants, dans les deux cas, IAB Europe est le responsable du traitement de ces opérations de traitement. L'intervention d'IAB Europe est d'ailleurs d'autant plus drastique dans l'hypothèse du cookie de *consentement global* partagé. En effet, ce cookie de *consentement global* partagé qui stocke la TC String pointe vers le domaine « *consensu.org* », géré par IAB Europe, à partir duquel les CMP peuvent accéder et mettre à jour la TC String partagé.

b. IAB agit en tant que contrôleur de données pour les opérations de traitement au sein du TCF.

98. Tout d'abord, les plaignants estiment qu'IAB Europe, dans ses « *Questions fréquemment posées* » sur le TCF, indique explicitement être responsable des TCF Policies.

99. Selon les plaignants, il va de soi que l'organisation qui gère et exploite le TCF est également le responsable du traitement de ce système, y compris tout traitement de données à caractère personnel imposé et organisé par le TCF. En effet, IAB Europe impose ces opérations de traitement de données à caractère personnel aux autres participants de manière contraignante.

100. En outre, IAB Europe exige que les CMP mettent en œuvre le TCF en respectant strictement ses *Technical specifications*. Dans les *Technical specifications* du TCF, IAB Europe explique en détail quelles données à caractère personnel doivent être traitées par les participants, à quelles fins et par quels moyens

101. IAB Europe exige également des CMP, dans le cas d'un *consentement global*, de stocker la chaîne de caractères dans un cookie de consentement global partagé sur le domaine « *consensu.org* ». Ce domaine Internet étant enregistré et géré par IAB Europe, la défenderesse a également accès aux données à caractère personnel traitées dans le TCF.

102. En outre, selon les plaignants, IAB Europe détermine les « moyens essentiels » pour le traitement des données à caractère personnel au sein du TCF. D'une part, IAB Europe précise en détail les éléments qui doivent être inclus dans la TC String. Et, d'autre part, IAB Europe détermine les catégories de destinataires de ces données à caractère personnel, puisque la défenderesse est responsable, selon ses propres termes, de la gestion de la *Global Vendor List* et de la gestion des CMP participant au TCF.

103. Les plaignants estiment également que le TCF ne fournit pas de mécanisme efficace pour faire appliquer certains éléments des TCF Policies [38], alors qu'un code de conduite est censé être un système efficace pour contraindre ses membres à se conformer, comme le prévoit l'article 41 du RGPD.

A.6.2. - Les opérations de traitement effectuées dans le TCF violent le RGPD à différents niveaux

a. Violation des principes de finalité, de proportionnalité et de nécessité

104. Selon les plaignants, IAB Europe collecte les préférences des utilisateurs du TCF via la TC String dans un but vague, inaccessible et abusif, alors que les données à caractère personnel traitées sont insuffisantes et non pertinentes pour cette finalité.

105. En outre, le traitement en lui-même serait tout sauf proportionné, ce qui signifie qu'IAB Europe enfreint les articles 5, paragraphe 1, points *(b)* et 5(1)*(c)* du RGPD, ainsi que son devoir de responsabilité en tant que responsable du traitement, prévu à l'article 5, paragraphe 2 du RGPD. En outre, les plaignants considèrent qu'avec la conception du TCF, IAB Europe ne fournit pas les garanties nécessaires au respect des exigences du RGPD et à la protection

[38] Voir para. 133 et s. de cette décision.

des droits des personnes concernées ; par conséquent, la défenderesse enfreint l'article 25 RGPD.

La finalité du traitement de la TC String n'est ni spécifiée ni explicitement définie pour les personnes concernées, et n'est pas non plus justifiée.

106. Selon les plaignants, IAB Europe ne fournit pas d'informations aux personnes concernées concernant le traitement de leurs données à caractère personnel dans le TCF.

107. L'objectif de la TC String dans le cadre de l'objectif général du TCF est de saisir les informations fournies aux utilisateurs et leurs préférences de traitement. En d'autres termes, IAB Europe traite bien des données à caractère personnel (en particulier la TC String) dans le cadre du TCF parce qu'elle prétend que cela pourrait rendre le traitement sous-jacent lié au marketing conforme au RGPD. Selon les plaignants, c'est donc cette finalité qui doit être appréciée au regard de sa licéité, et à la lumière de cette finalité, il convient d'apprécier la proportionnalité et la nécessité du traitement effectué par la TC String dans le cadre du TCF.

La TC String est inadéquate et non pertinente pour l'objectif visé

108. Les plaignants prétendent en outre que les opérations de traitement de la TC String au sein du TCF sont insuffisantes et non pertinentes pour assurer la conformité au RGPD lorsque les données à caractère personnel sont traitées par le protocole OpenRTB.

109. Le protocole OpenRTB contient un problème de sécurité inhérent qui rend impossible pour un système tel que le TCF de garantir, entre autres, la transparence et la responsabilité nécessaires en ce qui concerne les données à caractère personnel, y compris les catégories spéciales de données à caractère personnel, traitées dans une bid request après que celle-ci a été envoyée.

110. L'idée centrale du TCF est que les participants recueillent les préférences des utilisateurs et les transmettent sous la forme de la TC String, afin que les autres participants prennent note du contenu (c'est-à-dire lisent le signal TCF) et puissent ainsi respecter les préférences des utilisateurs. Cependant, selon les plaignants, il n'y a rien dans le TCF, ou dans tout système ou mécanisme connexe, qui garantisse effectivement que les participants au protocole OpenRTB sont liés par le signal TCF. Le signal TCF n'est donc rien de plus qu'une simple notification.

111. Compte tenu de la nature intrinsèquement illégale du traitement des données à caractère personnel dans le protocole OpenRTB, d'une part, et de la nature intrinsèquement imparfaite d'un système purement basé sur les signaux tel que le TCF sans contrôle efficace, d'autre part, l'utilisation du eTCF, y compris le traitement de la TC String, ne pourra jamais donner aux participants l'assurance d'être en conformité avec le RGPD. En effet, le TCF n'offre aucune garantie que les participants au TCF se conformeront à leurs obligations

de responsabilité (article 5.2 du RGPD). Il ne peut pas non plus assurer une protection adéquate des données à caractère personnel partagées par le protocole OpenRTB (article 5.1.*f*RGPD).

IAB Europe a mis en place le TCF de telle manière que la protection des données n'est pas garantie dès la conception.

112. Les plaignants font valoir que la conception du TCF, en raison de son caractère disproportionné, ne peut garantir le niveau de protection des données requis par l'article 25 RGPD, notamment au regard de l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, en principe, seules les données à caractère personnel qui sont nécessaires à chaque finalité spécifique du traitement sont traitées.

113. Le traitement des données à caractère personnel au sein du TCF, en particulier la TC String, n'est donc pas nécessaire pour la finalité spécifique car, selon les plaignants, cette finalité ne peut pas et ne sera pas atteinte en tout état de cause.

114. En outre, les plaignants font valoir que la TC String, en tant que donnée personnelle indépendante qui identifie de manière unique les utilisateurs, est partagé avec de nombreux participants par le biais de divers mécanismes, y compris par le mécanisme propre à IAB Europe du cookie de *consentement global* partagé sur son domaine Internet « *consensu.org* ».

b. Violation des principes de traitement équitable, licite et transparent (articles 5, 6, 12, 13 et 14 du RGPD).

115. Les plaignants allèguent que les personnes concernées ne sont en aucune façon informées du fait que leurs données à caractère personnel (y compris la TC String) sont systématiquement et largement traitées par IAB Europe au sein du TCF.

116. Selon les plaignants, le traitement des données à caractère personnel des plaignants et d'autres personnes concernées par IAB dans le TCF est en fin de compte :

- tout sauf légal puisqu'il n'existe pas de base légale ;
- ni approprié ni transparent, puisqu'il se déroule entièrement « dans le dos » des personnes concernées, sans aucune forme de notification.

Les traitements effectués par IAB Europe n'ont pas de base légale et sont donc illégaux.

117. IAB Europe ne peut pas se fonder sur le consentement des personnes concernées (article 6.1.*a* RGPD), selon les plaignants, car elle n'a jamais demandé ni obtenu un tel consentement. De même, les *TCF Policies*, les *Technical specifications* et les TCF Terms

and Conditions ne mentionnent nulle part un mécanisme par lequel IAB Europe demanderait aux personnes concernées la permission de générer une chaîne de caractères d'identification unique qui partagerait leurs préférences en matière de confidentialité avec une masse de destinataires, même dans les cas où ces personnes indiquent dans une CMP qu'elles ne souhaitent pas partager leurs données à caractère personnel avec qui que ce soit.

118. Selon les plaignants, IAB Europe ne peut pas non plus invoquer la nécessité du traitement de la TC String au sein du TCF pour l'exécution d'un contrat avec les plaignants et d'autres personnes concernées (article 6.1.*b*), car il n'y a pas de contrat entre les personnes concernées et IAB Europe.

119. En outre, les plaignants font valoir que la défenderesse ne peut pas non plus invoquer la nécessité du traitement de la TC String au sein du TCF pour servir ses intérêts légitimes, ou ceux d'un tiers (article 6.1.*f* RGPD). L'équilibre exigé entre les intérêts serait toujours en faveur des personnes concernées.

120. Tout d'abord, le traitement de la TC String ne profite en rien aux personnes concernées, car le TCF n'est pas en mesure de garantir la sécurité, la responsabilité ou la transparence. En outre, il n'y a pas d'intérêt légitime, car cet intérêt n'est nulle part suffisamment clairement formulé et il n'est pas possible de le mettre en balance avec les intérêts et les droits fondamentaux des personnes concernées.

121. Ensuite, dans la mise en balance des intérêts, le responsable du traitement doit en principe tenir compte de plusieurs facteurs : les effets du traitement sur la personne concernée, la nature des données à caractère personnel traitées, la manière dont ces données à caractère personnel sont traitées, les attentes raisonnables de la personne concernée et le statut du responsable du traitement et de la personne concernée.

122. Selon les plaignants, les conséquences du traitement de la TC String sont particulièrement lourdes pour les personnes concernées. Les opérations de traitement d'IAB Europe conduiraient les participants au TCF à supposer qu'ils informent correctement les personnes concernées du traitement des données à caractère personnel par le protocole OpenRTB, alors que tel n'est pas le cas. Cela conduirait alors au partage et à la distribution illicites de données à caractère personnel, même sensibles, à une échelle considérable via le protocole OpenRTB.

123. Le traitement de la TC String par IAB Europe entraînerait le partage d'un identifiant en ligne unique avec un nombre incalculable de parties, à l'instar de ce qui se passe avec les identifiants uniques dans les cookies publicitaires des grandes sociétés de publicité. Il permettrait donc de suivre facilement les utilisateurs sur le web et sur différents appareils (« *web and cross-device tracking* »). De plus, les plaignants soutiennent que la TC String peut être combiné avec les données distribuées via le protocole OpenRTB, car la TC String est intégré dans une *bid request*.

124. Compte tenu du manque d'information des personnes concernées sur les opérations de traitement au sein du TCF et du partage sans restriction de la TC String avec un groupe presque illimité de destinataires, il est clair pour les plaignants que ces opérations de traitement dépassent le cadre des attentes raisonnables des personnes concernées. En outre, les personnes concernées, telles que les plaignants, ne s'attendent pas à ce que le traitement des données à caractère personnel dans le cadre du TCF entraîne le partage de leurs données à caractère personnel, parfois sensibles, et de leurs profils détaillés avec de nombreuses entreprises par l'intermédiaire du protocole OpenRTB, sans aucun contrôle réel et effectif sur ce que ces entreprises feront des données à caractère personnel obtenues.

125. Les plaignants dans cette affaire sont des personnes physiques et des groupes d'intérêt représentant les intérêts des personnes physiques en matière de protection des données. Ils n'ont aucun contrôle sur le traitement des données à caractère personnel dans le cadre du TCF (qui a lieu de toute façon, que le consentement soit donné ou refusé dans une CMP). Ils n'ont pas non plus de contrôle sur ce qu'il advient de leurs données à caractère personnel partagées par le protocole OpenRTB. Selon les plaignants, les personnes concernées ne peuvent pas vérifier si les participants à OpenRTB respectent effectivement les règles du TCF.

IAB Europe traite des données à caractère personnel dans le cadre du TCF de manière clandestine, sans aucune forme de notification, et le traitement n'est donc ni approprié ni transparent.

126. Malgré la vaste documentation qu'IAB Europe met à la disposition des participants au TCF sur son site web, il n'est indiqué nulle part que le TCF lui-même implique également le traitement de données à caractère personnel, selon les plaignants. En outre, la documentation ignore expressément, en ce qui concerne les participants au TCF que le TCF lui-même implique le traitement de données à caractère personnel.

127. Les lignes directrices de mise en œuvre du TCF semblent suggérer qu'il existe des hypothèses dans lesquelles la participation au TCF n'implique pas le traitement de données à caractère personnel. En fin de compte, les annonceurs et les DSP, qui participent déjà au TCF sont informés qu'ils doivent s'enregistrer en tant que *fournisseurs adtech* s'ils traitent des données à caractère personnel. Selon les plaignants, cela implique qu'ils n'auraient pas à le faire s'ils ne traitaient pas de données à caractère personnel. Or, cette dernière situation est tout à fait impossible, selon les plaignants, car le TCF exige par nature le traitement de données à caractère personnel.

128. Selon les plaignants, les déclarations contenues dans les directives d'IAB Europe sont trompeuses pour les centaines de *fournisseurs adtech* qui utilisent le TCF. Étant donné qu'IAB Europe n'informe pas les participants au TCF du traitement des données à caractère

personnel qu'implique nécessairement la mise en œuvre d'un TCF, aucun de ces participants n'est informé ou ne réalise qu'il a une obligation de transparence. De cette manière, les personnes concernées - telles que les plaignants - ne sont informées par aucun participant du traitement des données à caractère personnel au sein du TCF.

129. IAB Europe ne respecte pas non plus sa propre obligation de transparence. Ni sur son propre site Internet ni dans d'autres sources, la défenderesse ne communique les informations exigées par les articles 13 et 14 aux personnes concernées, telles que les plaignants. Cela comprendrait les informations suivantes : qu'IAB Europe est le responsable du traitement des données du TCF et ses coordonnées ; les coordonnées de son délégué à la protection des données ; quelles sont les finalités de son traitement et la base juridique du traitement ; quelles sont les catégories de données à caractère personnel traitées (en particulier la TC String) ; qui reçoit les données à caractère personnel (au moins tous les participants au TCF reçoivent la TC String) ; qu'IAB Europe a l'intention de transférer les données à caractère personnel à des destinataires dans des pays tiers ; combien de temps les données à caractère personnel sont conservées ; quels sont ses intérêts légitimes pour le traitement ; quels sont les droits des personnes concernées ; que les personnes concernées peuvent déposer une plainte auprès de l'autorité de protection des données ; que les personnes concernées peuvent retirer le consentement qu'elles ont donné ; et enfin, quelle est la source des données à caractère personnel.

130. Dans le même temps, IAB Europe ne peut invoquer aucune des exceptions prévues à l'article 14.5 du RGPD pour ne pas avoir à fournir ces informations, puisque :

    a. les personnes concernées ne sont pas encore en possession de l'information, puisque le traitement les concernant a jusqu'à présent été effectué en secret (article 14.5.*a* RGPD) ;

    b. il n'est pas impossible de porter ces informations à la connaissance des personnes concernée et cela ne nécessite un effort disproportionné, compte tenu de l'influence que IAB Europe exerce sur le fonctionnement du TCF (article 14.5.*b* RGPD) ;

    c. l'acquisition de ces données n'est pas prescrite par la loi (article 14.5.*c* du RGPD) ; et

    d. les données à caractère personnel ne doivent pas rester confidentielles pour des raisons de secret professionnel (article 14.5.*d* RGPD).

La référence d'IAB Europe à l'affaire Vectaury en France n'est pas pertinente.

131. Selon les plaignants, IAB Europe croit à tort qu'elle peut se fonder sur la décision de l'autorité de contrôle française CNIL dans l'affaire Vectaury. En effet, IAB Europe affirme à tort qu'il serait étrange que le Service d'inspection relève des infractions liées au traitement des données à caractère personnel dans le TCF, alors que la CNIL n'aurait, selon la

défenderesse,relevé aucun problème par rapport à la légitimité de ces traitements. Les plaignants affirment qu'IAB Europe fait des hypothèses et tire des conclusions qui ne peuvent absolument pas être déduites de l'affaire Vectaury :

- Tout d'abord, l'affaire Vectaury concernait la mise en œuvre spécifique d'une CMP par Vectaury qui aurait permis de mettre en œuvre le TCF. Le rôle d'IAB Europe ne faisait pas l'objet de cette procédure et la CNIL n'a donc pas statué, ni enquêté, sur le rôle d'IAB Europe dans la fourniture du TCF.
- Deuxièmement, cette affaire concernait spécifiquement la question de savoir si la mise en œuvre du TCF par Vectaury pouvait mettre le traitement sous-jacent des systèmes d'enchères en temps réel en conformité avec le RGPD. Le verdict de la CNIL a été clairement négatif, comme en témoigne le fait que Vectaury elle-même indique sur son site web qu'elle a créé une toute nouvelle méthode en dialogue avec la CNIL. Selon les plaignants, il est donc trompeur de la part d'IAB Europe de prétendre que la CNIL aurait légitimé le TCF en soi comme suffisant pour permettre la conformité avec le RGPD des systèmes d'enchères en temps réel.
- Troisièmement, les plaignants font valoir que l'enquête de la CNIL n'a pas porté sur la légitimité du traitement des données à caractère personnel au sein du TCF. La CNIL n'a pas considéré la génération et la distribution de la TC String comme un traitement autonome et n'a donc pas fait de déclaration à ce sujet.

132. Selon les plaignants, les décisions de la CNIL dans l'affaire Vectaury ne sont donc pas pertinentes, car il s'agissait d'un cas clairement différent, dirigé contre une partie différente, impliquant des traitements différents et sous une législation qui a été remplacée depuis. La Chambre Contentieuse suit le point de vue des plaignants et ne discute pas l'affaire Vectaury, qui concerne un cas différent du présent.

c. Violation des principes d'intégrité et de confidentialité (articles 5.1.f et 32 du RGPD).

133. Selon les plaignants, IAB Europe viole les obligations d'intégrité et de confidentialité du RGPD car elle facilite l'échange de données à caractère personnel dans le TCF, en particulier l'échange de la TC String, avec de nombreuses parties, sans vérifier si tous les destinataires de ces données à caractère personnel respectent les règles du RGPD.

134. Il est certain que la TC String est partagée avec des milliers d'entreprises. La TC String doit donc être protégée par des mesures appropriées conformément aux articles 5.1.*f* et 32 RGPD. Cependant, IAB Europe n'a pas intégré de mécanisme de protection approprié : Comme pour tout autre traitement dans le protocole OpenRTB, il n'existe aucun moyen de vérifier que les destinataires traitent effectivement la TC String conformément au RGPD. En effet, les plaignant affirment qu'aucun des mécanismes présentés par IAB Europe n'est basé sur un contrôle réel et proactif de la conformité au TCF.

135. Les plaignants contestent l'argument d'IAB Europe selon lequel il n'est pas tenu de faire respecter le TCF, et en particulier les accords conclus dans le cadre du TCF. Les plaignants prétendent qu'il est effectivement de son devoir, en tant que responsable du traitement, d'appliquer les accords conclus dans le cadre du TCF et, au moins de cette manière, de fournir certaines garanties pour le traitement sécurisé de la TC String.

136. Deuxièmement, les plaignants soulignent les affirmations d'IAB Europe selon lesquelles, en tant qu'organisation de gestion, elle fait des « efforts substantiels » pour faire respecter les accords conclus dans le cadre du TCF. Selon les plaignants, il n'existe aucune preuve de ces prétendus « efforts substantiels ». Les plaignants affirment en outre qu'IAB Europe devrait vérifier le respect de tous les accords par chaque participant TCF enregistré, ce qui, compte tenu de l'ampleur du traitement des données, impliquerait une enquête de très grande ampleur. En outre, les plaignants se réfèrent à la réponse donnée par IAB Europe elle-même au Service d'inspection : « *L'obligation de déclaration elle-même n'est pas actuellement contrôlée. En outre, il est difficile de le contrôler car il serait difficile pour IAB Europe d'établir si et quand une CMP a (ou aurait dû avoir) une « croyance raisonnable » qu'une autre partie ne se conformait pas à la réglementation* »[39].

137. Troisièmement, les plaignants estiment qu'IAB Europe a tort d'essayer de se cacher derrière les arrangements contractuels. Selon les plaignants, la défenderesse prétend qu'il suffit que les participants soient contractuellement tenus de signaler toute non-conformité à IAB Europe.

138. Les plaignants font également valoir qu'IAB Europe, en tant que responsable du traitement des données du TCF, est lié par les articles 5.1.*f* et 32 du RGPD, bien qu'il soit pratiquement impossible de garantir la sécurité de la TC String traité lorsqu'il est partagé avec des milliers de sociétés destinataires. Selon les plaignants, ce dernier point signifierait qu'IAB Europe vérifie activement que tous les destinataires de la TC String respectent toujours les obligations du RGPD, de sorte que le traitement de la TC String reçu ne serait pas illégal.

139. De plus, selon les plaignants, la pratique prouve que presque tous les participants au TCF traitent illégalement la TC String, car pas une seule CMP, pas un seul éditeur et pas un seul vendeur ne fournit d'informations sur le traitement de la TC String, sa finalité, sa base juridique ou les catégories de destinataires. Cela impliquerait, selon les plaignants, que le transfert de la TC String à ces parties constitue en soi une violation des données à caractère personnel qui, étant donné son ampleur considérable, donne lieu à une obligation de notification aux autorités de contrôle.

140. L'impossibilité pratique de fournir les garanties nécessaires à la protection des données à caractère personnel (en particulier la TC String) des personnes concernées, lorsqu'elles sont partagées avec des milliers de destinataires au sein du protocole OpenRTB, démontre,

[39] Lettre d' IAB Europe au service d'inspection du 10 février 2020, p. 8.

selon les plaignants, qu'IAB Europe manque aux obligations qui lui incombent en vertu des articles 5.1.*f* et 32 du RGPD.

d. Le transfert systématique de la TC String vers des pays tiers sans protection adéquate (violation de l'article 44 du RGPD).

141. Les plaignants prétendent qu'IAB Europe a mis en place le TCF de telle sorte que les données à caractère personnel - y compris la TC String, car il est intégré dans les *demandes d'offres* - sont structurellement transférées dans le cadre d'OpenRTB à de nombreuses sociétés situées en dehors de l'Espace économique européen (EEE), sans qu'une protection adéquate soit assurée pour ces transferts.

142. Les plaignants font référence à l'Ad Exchange Xandr (basé aux États-Unis), qui est affilié au TCF d'IAB Europe et reçoit donc au moins la TC String des utilisateurs de l'EEE, y compris les plaignants. En tant que responsable du traitement des données à caractère personnel dans le TCF, IAB Europe doit fournir un mécanisme de transfert des données à caractère personnel afin que les Ad Exchanges établis en dehors de l'EEE puissent recevoir la TC String.

143. Les échanges de la TC String via des systèmes d'enchères en temps réel tels que OpenRTB sont de nature structurelle et se répètent continuellement en fractions de secondes. En effet, la TC String est envoyeé avec les *demandes d'offres*. Il serait donc impossible pour IAB Europe, selon les plaignants, d'invoquer l'une des exceptions prévues à l'article 49 du RGPD.

144. Des garanties appropriées seraient le seul moyen pour IAB Europe d'organiser les transferts de données à caractère personnel dans le cadre du TCF. Cependant, à l'heure actuelle, IAB Europe ne fournit aucune forme de garanties appropriées pour le transfert de la TC String par le biais de systèmes d'enchères en temps réel tels que OpenRTB.

145. Conformément à l'arrêt Schrems II, IAB Europe[40] aurait dû, en plus de choisir une forme de garanties adéquates, prendre des mesures supplémentaires pour empêcher que les données à caractère personnel ne soient traitées de manière non conforme dans des pays tiers. Cependant, ces mesures supplémentaires sont tout aussi insuffisantes que les garanties appropriées. La TC String est partagée en aveugle avec un nombre indéfini de participants au protocole OpenRTB, où qu'ils se trouvent dans le monde.

[40] Arrêt de la CJUE du 16 juillet 2020, C-311/18, *Facebook Ireland et Schrems*, ECLI:EU:C:2020:559.

A.7. - Résumé de la duplique de la défenderesse du 25 mars 2021

A.7.1. - Les organisations qui traitent des données à caractère personnel dans le cadre du système RTB sont tenues de se conformer au RGPD et à la directive « vie privée et communications électroniques ».

146. La défenderesse prétend d'abord que toute partie participant au RTB et utilisant le protocole OpenRTB peut intervenir dans les opérations techniques de stockage et/ou d'accès sur l'appareil d'un utilisateur (par exemple, le placement de cookies de site web) en vertu de la directive « vie privée et communications électroniques », et/ou agir en tant que responsable du traitement ou sous-traitant de données à caractère personnel (par exemple, à des fins de publicité numérique) en vertu du RGPD. Le cas échéant, toutes ces parties sont responsables du respect de leurs obligations en vertu du RGPD et de la directive « vie privée et communications électroniques » lorsqu'elles s'engagent dans le RTB.

147. En outre, selon la défenderesse, il existe des milliers de sociétés engagées dans le RTB et utilisant le protocole OpenRTB, qui ne participent cependant pas au TCF. De même, les parties peuvent utiliser le TCF à des fins autres que le RTB. IAB Europe souligne également que les publishers peuvent utiliser le TCF pour une série de scénarios de publicité en ligne autres que le protocole OpenRTB - y compris d'autres types de protocoles RTB, mais aussi la publicité en ligne qui n'implique pas du tout le RTB, comme la vente directe d'inventaire publicitaire.

148. La défenderesse réfute également les allégations des plaignants selon lesquelles le RTB est intrinsèquement illégal en se référant au rapport de l'autorité de contrôle britannique (ICO) qui a simplement déclaré que le RTB « exige que les organisations assument la responsabilité de leur propre traitement des données, et que le secteur réforme collectivement le RTB ». L'ICO aurait également souligné les efforts déployés de bonne foi par des parties prenantes telles que IAB UK pour contribuer à ce processus de réforme dans une publication plus récente[41].

149. En outre, la défenderesse indique que plusieurs autorités de contrôle ont demandé des moyens d'accroître la transparence pour les personnes concernées en identifiant clairement les responsables du traitement avec lesquels les données à caractère personnel seront partagées, en précisant les finalités du traitement et en permettant aux personnes concernées d'exercer un contrôle sur leurs données à caractère personnel. C'est précisément ce type de mesure de transparence qu'IAB Europe et le TCF entendent soutenir.

[41] Information Commissioner's Office - Adtech - la réforme des enchères en temps réel a commencé et va se poursuivre, 17 janvier 2020, https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

150. Dans le cadre du TCF, les personnes concernées ont la possibilité de donner leur accord préalable à un certain nombre de tiers identifiés (*fournisseurs adtech*) et de finalités de traitement. Selon IAB Europe, cette transparence et ce contrôle préalable constituent un substitut approprié, du point de vue de la conformité juridique, au consentement en *temps réel*, *à la volée* et un par un pour l'accès, le stockage et le traitement des données par les responsables du traitement.

A.7.2. - IAB Europe ne peut être tenue responsable des pratiques illégales présumées des participants au RTB, car le TCF est totalement distinct du RTB.

151. La défenderesse souligne que le TCF n'est qu'une des nombreuses approches optionnelles que les responsables du traitement peuvent choisir pour aider à assurer la conformité avec les exigences de transparence et de consentement lors du traitement des données à caractère personnel personnelles pour le RTB ou d'autres fins publicitaires. Par conséquent, la responsabilité de la conformité et des décisions effectives sur les objectifs et les moyens de ces opérations de traitement des données à caractère personnel incombe entièrement aux parties engagées dans le RTB, et non à IAB Europe.

152. La défenderesse indique également qu'IAB Europe a eu des contacts avec plusieurs autorités de surveillance après le déploiement de la première version du TCF, ainsi qu'avec plusieurs *publishers*. À la suite de ces discussions, la deuxième version du TCF a été élaborée, dans laquelle plusieurs finalités de traitement ont été regroupées sous un seul titre dans des « piles », et l'intérêt légitime a été introduit comme base juridique possible. En outre, le TCF v2 introduit des objectifs supplémentaires et des « *contrôles d'éditeur* » qui permettent aux publishers de restreindre l'accès à un objectif particulier à un sous-ensemble de *fournisseurs adtech*.

153. Enfin, la défenderesse précise qu'IAB Europe a toujours eu l'intention de faire adopter le TCF en tant que code de conduite transnational.

154. Dans son conclusion initial, la défenderesse avance des arguments procéduraux concernant la compétence de l'APD et la manière dont les plaintes et l'enquête ont été traitées. Ces arguments en défense sont exposés ci-dessous à la section A.9.

155. Dans ses conclusions de synthèse, la défenderesse affirme également que la manière dont l'APD a mené la procédure n'est pas conforme à l'article 57 du RGPD. Toutefois, les plaignants n'ayant pas été en mesure de répondre, les débats ont été rouverts à la demande de la Chambre Contentieuse.

A.8. - audience et réouverture des débats

156. Conformément à l'article 51 du règlement de procédure de l'Autorité de protection des données, une audience a été organisée, à laquelle toutes les parties ont été invitées. L'audience a eu lieu le 11 juin 2021.

157. Un compte rendu écrit de l'audience est établi afin de donner les détails et les informations complémentaires qui ont été apportés lors de l'audience, sans répéter les éléments exposés dans les conclusions. Les parties ont également eu la possibilité de soumettre leurs commentaires écrits sur le dossier. Un certain nombre d'éléments mentionnés ci-dessous sont pertinents pour la présente décision.

158. Dans le cadre de l'audience, le Service d'inspection confirme tout d'abord sa position selon laquelle IAB Europe agit en tant que responsable du traitement des données à caractère personnel dans le cadre du Cadre de transparence et de consentement , mais pas pour OpenRTB.

159. Le Service d'inspection précise également que des données à caractère personnel sont collectées comme prévu dans les *TCF Policies*, dans les *conditions générales*[42] et dans la politique de confidentialité, ainsi que dans le contexte des valeurs TC String stockées dans un cookie *euconsent-v2*, ces dernières en tant qu'expression des préférences d'un utilisateur devant également être considérées comme des données à caractère personnel. Le Service d'inspection souligne également que la TC String en tant que tel ne contient aucune information relative directement ou indirectement à la taxonomie du site web auquel la TC String fait référence. Ce dernier aspect concerne une distinction essentielle entre les préférences de l'utilisateur qui sont collectées dans le contexte du TCF, et les données à caractère personnel de ce même utilisateur qui sont collectées et distribuées au sein du protocole OpenRTB. En conclusion, le Service d'inspection déclare que les valeurs TC String et le cookie *euconsent-v2* ne permettent pas en soi d'identifier un utilisateur individuel. Bien que les deux éléments contiennent des données à caractère personnel, dans le sens où les informations concernent une personne physique, le Service d'inspection confirme également qu'il n'est pas possible d'identifier la personne concernée spécifique sur la base de ces seules informations.

160. Au cours de l'audience, l'avocat de la défenderesse a soulevé un point de procédure, à savoir que la Chambre Contentieuse n'est pas autorisée à se prononcer sur les éléments présentés par les plaignants avant qu'une analyse ait été effectuée sur la cohérence de leurs conclusions avec l'ensemble des plaintes. La défenderesse demande également à la Chambre Contentieuse de se prononcer sur la nécessité de demander une enquête complémentaire au Service d'inspection, comme l'exigerait l'article 57.1.*f* RGPD. La

[42] Conditions générales du cadre de transparence et de consentement d'IAB Europe (« Conditions générales ») (pièce 33), p.7.

Chambre Contentieuse se prononcera sur ce point de procédure dans la présente décision[43].

161. Les plaignants ont répondu oralement aux arguments procéduraux de la défenderesse au cours de l'audience.

162. En ce qui concerne le moment auquel la TC String est générée, la défenderesse souligne que la notification de ce moment ne peut conduire à l'unicité d'une TC String, car il existe une chance que deux utilisateurs non identifiés puissent donner les mêmes préférences au même moment. De plus, cette durée ne suffit pas pour parler d'une chaîne unique, puisque les valeurs de la TC String ne sont pas persistantes et peuvent varier dans le temps ou en fonction des sites web visités.

163. La défenderesse indique également que le scénario des cookies de *consentement global*, dans lequel les préférences stockées dans une TC String s'appliquent à plusieurs sites web, n'est pas pertinent compte tenu de son champ d'application limité au moment de l'audience[44], ainsi que de l'intention d'IAB Europe, suite à la constatation qu'un consentement global ne répond pas à l'exigence d'un consentement spécifique[45], de ne plus soutenir cette fonctionnalité et de la supprimer progressivement dans les semaines suivant l'audience.

164. En ce qui concerne la question de savoir si l'attribution d'un sous-domaine de *consensu.org* à une CMP au moyen d'une délégation DNS peut être considérée comme une détermination des moyens de traitement, la défenderesse fait valoir que, en raison de la délégation DNS, chaque sous-domaine renvoie aux serveurs des CMP, qui sont d'ailleurs les seuls à pouvoir lire les TC Strings des appareils des utilisateurs. En outre, la défenderesse fait valoir que l'enregistrement d'un sous-domaine de *consensu.org* est purement facultatif et, en tant que tel, ne constitue pas un moyen essentiel de traitement.

165. Les plaignants soulignent, d'autre part, qu'une délégation DNS peut toujours être annulée par le défendeur, et qu'il est sans importance que le défendeur n'ait pas accès aux cookies *euconsent-v2*. Les plaignants soulignent également que la délégation DNS peut être considérée comme un moyen essentiel de traitement, puisque la délégation DNS est utilisée pour distribuer la TC String plus loin dans l'écosystème TCF.

166. Concernant l'existence d'interfaces entre le TCF et l'OpenRTB, les plaignants soulignent que les deux systèmes sont intrinsèquement imbriqués en raison du lien entre, d'une part, la TC String que les CMP génèrent selon les instructions du TCF et, d'autre part, les

[43] Voir para. 174 et s. de cette décision.

[44] Selon la défenderesse, le nombre de cookies de consentement global était au maximum de 0,5 % de tous les consentements et préférences collectés dans le monde.

[45] Article 4.11 RGPD : « consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ;

demandes d'offres, qui sont régulées par l'OpenRTB. En d'autres termes, ces derniers sont utilisés comme véhicules pour diffuser la TC String à travers l'écosystème OpenRTB.

167. La défenderesse affirme que les deux systèmes peuvent fonctionner indépendamment et que le TCF a été développé avec l'OpenRTB comme point de départ et pourrait être utilisé dans ce contexte, l'OpenRTB étant la norme la plus largement utilisée dans le secteur. Selon la défenderesse, cela ne signifie pas que le TCF soit un moyen essentiel pourutiliser l'OpenRTB.

168. La défenderesse prétend que l'élaboration par la défenderesse d'un futur code de conduite en relation avec le TCF ne peut être considérée comme une preuve de sa responsabilité (partagée) en matière de traitement des données à caractère personnel dans le cadre du TCF. Les plaignants ajoutent qu'il est impossible de vérifier le respect du GDPR par les organisations participantes, même si les règles sont clairement définies dans une politique d'application.

169. À cet égard, la défenderesse fait référence à l'élaboration et à la mise en œuvre progressive de programmes de conformité automatisés pour contrôler dans quelle mesure les CMP et les annonceurs (ainsi que d'autres *fournisseurs adtech*) se conforment aux *TCF Policies*, y compris les futurs audits internes des processus des parties susmentionnées. Le défendeur souligne également que le TCF prévoit déjà des mesures de sanction à l'encontre des *fournisseurs adtech* qui n'adhèrent pas au cadre, telles que la suspension temporaire de leur participation au TCF.

170. En ce qui concerne le lien entre la TC String et l'utilisateur individuel, la défenderesse estime que le TCF ne détermine pas comment cela se fait, ni comment la TC String est ensuite communiqué aux *fournisseurs adtech*, ces éléments étant entièrement soumis au protocole OpenRTB.

171. La défenderesse précise que l'utilisation du domaine *consensu.org* est purement facultative, et qu'en outre, ce domaine n'a pas été développé dans le but de traiter ou de stocker les logs relatifs au TC Strings.

172. Enfin, la défenderesse souligne sa position selon laquelle la TC String ne constitue une donnée à caractère personnel qu'après avoir été lié dans le cadre de l'OpenRTB à une *bid request* qui contient déjà des données à caractère personnel.

173. Le 9 août 2021, après délibération, la Chambre Contentieuse décide de rouvrir les débats sur les arguments procéduraux spécifiques d'IAB Europe.

174. Le 23 août 2021, la Chambre Contentieuse a reçu les premières conclusions de la défenderesse. La défenderesse affirme que l'autorité de contrôle Belge (APD) a violé l'article 57.1.*a* et 57.1.*f* du RGPD et l'article 94(3) de la LCA. L'APD n'aurait pas non plus respecté le principe de bonne administration et les droits de la défense du défendeur.

175. En ce qui concerne l'article 57.1.*f* RGPD, la défenderesse fait tout d'abord valoir que les plaignants ont présenté de nouvelles allégations dans leur conclusions, qui sont donc plus étendues que les plaintes initiales. De plus, selon la défenderesse, l'APD n'a pas enquêté de manière proactive sur ces nouvelles allégations en chargeant le Service d'inspection d'une enquête nouvelle ou complémentaire. En conséquence, la défenderesse considère que l'APD a manqué à ses obligations au titre de l'article 57.1.*f* RGPD.

176. En outre, défenderesse fait valoir que, en demandant une enquête initiale au Service d'inspection, la Chambre Contentieuse s'est liée *de facto* à une procédure dans laquelle chaque allégation ou défense doit être examinée par le Service d'inspection. Selon la défenderesse, la décision de la Chambre Contentieuse de ne pas demander un complément d'enquête après une première enquête et la présentation des moyens de défense a conduit à une violation de l'article 94(3) de la LCA.

177. La défenderesse indique également qu'en l'absence d'une enquête du Service d'inspection sur de supposées nouvelles allégations dans les défenses des plaignants et d'une qualification juridique de ces allégations, elle n'a pas été en mesure de se défendre de manière adéquate contre les plaintes déposées contre IAB Europe. Ainsi, la procédure devant la Chambre Contentieuse pourrait être considérée comme ayant évolué d'une procédure *inquisitoire* à une *procédure contradictoire* dans laquelle la Chambre Contentieuse n'aurait plus agi comme un organe administratif de règlement des litiges, prenant principalement en compte les prétentions et les documents des plaignants, de sorte que les droits de la défense d'IAB Europe auraient été violés, selon la défenderesse.

178. Le 6 septembre 2021, la Chambre Contentieuse a reçu les conclusions des plaignants. Les plaignants considèrent, tout d'abord, que les nouveaux moyens du défendeur ont dépassé le cadre limité des débats rouverts.

179. Deuxièmement, les plaignants prétendent que la nature de la procédure n'a en rien changé, puisque la procédure a été entamée en raison de plaintes déposées auprès de l'APD, en d'autres termes, comme une *procédure contradictoire*, et qu'elle l'est restée tout au long de la procédure.

180. Troisièmement, les plaignants se réfèrent aux articles 63, paragraphe 2, et 94 de la LCA, comme contre-argument à l'affirmation selon laquelle la Chambre Contentieuse aurait dû faire examiner par le Service d'inspection chacun des moyens soulevés par les plaignants. En effet, ces dispositions confèrent à la Chambre Contentieuse un pouvoir discrétionnaire pour décider si une enquête (supplémentaire) par le Service d'Inspection est nécessaire ou non.

181. En outre, les plaignants soutiennent qu'il est impossible pour la Chambre Contentieuse de faire procéder à une enquête ou à une enquête complémentaire par le Service d'Inspection après les conclusions et pièces des parties, compte tenu des délais limités de 30 jours après

que la Chambre Contentieuse a été saisie par le Service de première ligne après le dépôt de la plainte, ou par le Service d'Inspection après la réception du rapport d'enquête initial.

182. En ce qui concerne l'argument de la défenderesse selon lequel la manière dont la Chambre Contentieuse a traité le dossier viole l'article 57.1.*f* RGPD, les plaignants soulignent que, tout d'abord, cette disposition n'a pas d'effet direct en ce sens que la défenderesse pourrait en tirer des droits. Les plaignants prétendent également que cette disposition ne peut pas affecter la structure interne et le fonctionnement des autorités de contrôle, qui, en ce qui concerne l'APD et, plus précisément, la répartition des compétences entre son Service d'inspection et sa Chambre Contentieuse, sont soumis au droit administratif (procédural) belge.

183. En outre, les plaignants indiquent que l'article 57.1.*f* RGPD ne fait pas référence à une obligation pour la Chambre Contentieuse de demander une enquête du Service d'Inspection sur les plaintes, mais au pouvoir des autorités de contrôle de classer l'affaire.

184. En outre, les plaignants affirment que la décision de la Chambre Contentieuse de demander une enquête au Service d'inspection ne l'empêche nullement de se fonder sur les conclusions et pièces soumises par les parties, contrairement à la position de la défenderesse.

185. En ce qui concerne le prétendu manquement de la défenderesse au principe de diligence, les plaignants soutiennent que la Chambre Contentieuse est tenue, en vertu de ce principe, d'étudier correctement toutes les pièces du dossier afin que sa décision soit fondée sur une présentation correcte et complète des faits. Toutefois, ce principe n'implique en aucun cas que la Chambre Contentieuse doive faire procéder à une enquête (complémentaire) par le Service d'inspection pour chaque pièce à conviction.

186. En ce qui concerne les droits de la défense de la défenderesse, les plaignants soutiennent que, sur la base des différents rapports d'enquête du Service d'inspection et des mémoires et pièces présentés par les plaignants, la défenderesse a été suffisamment informée des faits et des violations du droit allégués. De plus, selon les plaignants, la défenderesse a eu suffisamment d'occasions de se défendre par écrit contre les allégations juridiques et factuelles faites par les plaignants, étant donné que la défenderesse peut soumettre deux jeux de conclusions.

187. Enfin, les plaignants se réfèrent à l'absence d'exemples concrets, dans les dernières conclusions de la défenderesse, de prétendues nouvelles allégations sur lesquelles la défenderesse n'a pas été en mesure de conclure ou qui n'ont pas fait l'objet d'une enquête par le Service d'inspection.

188. Le 13 septembre 2021, la Chambre Contentieuse a reçu la réponse de la défenderesse.

189. Selon la défenderesse, seul le rapport d'inspection détermine l'étendue des allégations, à condition que le rapport d'inspection soit significatif et fondé sur un examen complet des

faits. En outre, la défenderesse fait valoir que la décision de la Chambre Contentieuse de demander une enquête au Service d'inspection a eu pour effet de transformer l'ensemble de la procédure en une procédure « *inquisitoire* », indépendamment du fait que la procédure trouve son origine dans les plaintes déposées auprès de l'APD. Selon la défenderesse, la décision de la Chambre Contentieuse de ne pas demander ultérieurement un complément d'enquête et de fonder la suite de la procédure uniquement sur les conclusions et pièces des parties constitue une violation de ses droits de la défense.

190. En outre, la défenderesse est d'avis que le délai de trente jours prévu à l'article 96, alinéa 1, de la LCA ne s'applique pas à la demande de la Chambre Contentieuse de faire procéder à une enquête complémentaire par le Service d'inspection.

191. La défenderesse fonde ce raisonnement sur la distinction faite en droit administratif général entre les délais de péremption et les délais d'ordre. En particulier, la défenderesse estime que, en l'absence de dispositions formelles dans la LCA selon lesquelles le dépassement du délai de 30 jours entraîne une perte de compétence de la Chambre Contentieuse, les délais prévus à l'article 96 doivent être respectés, mais pas à peine de nullité de la décision rendue trop tard. Selon la défenderesse, la Chambre Contentieuse reste donc compétente pour prendre une décision d'instruction complémentaire même après l'expiration du délai d'ordre de 30 jours. Cette interprétation, selon la défenderesse, est en fait le résultat de la plus grande importance du droit à la défense par rapport au droit à une procédure rapide devant la Chambre Contentieuse.

192. En ce qui concerne l'effet direct de l'article 57.1.*f* RGPD, la défenderesse affirme que l'existence d'une marge d'appréciation pour les États membres n'exclut pas l'effet direct d'une disposition, mais implique d'examiner si cette disposition vise à offrir une garantie aux parties. La défenderesse estime que l'article 57.1. *f* RGPD répond à cette exigence et précise que son argument pour demander un complément d'enquête se limite en outre à une appréciation en fait et en droit des éléments justificatifs de la procédure.

193. En conclusion, la défenderesse déclare qu'elle n'a pas reçu d'exposé clair de la nature et de la portée des accusations, à l'exception des allégations formulées dans les mémoires en défense des plaignants. À cet égard, la défenderesse affirme que les rapports de contrôle technique ne contiennent que des descriptions techniques, dans lesquelles, en outre, la TC String n'est mentionnée nulle part. Dans la section A.9.- Objections de procédures soulevées par la défenderesse, la Chambre Contentieuse indique les raisons pour lesquelles les garanties procédurales, y compris concernant la nature et portée des accusations, ont été respectées.

A.9. - Objections de procédure soulevées par la défenderesse

A.9.1. - Infractions aux règles de procédure applicables au rapport d'inspection et aux droits et libertés fondamentaux d'IAB Europe

a. Irrecevabilité des plaintes

194. La défenderesse fait tout d'abord valoir que certaines des plaintes ont été déposées en anglais et qu'elles ne remplissent donc pas les conditions formelles de recevabilité prévues à l'article 60 de la LCA.

195. En outre, la défenderesse estime que certaines des personnes ayant déposé des plaintes ne peuvent être considérées ni comme des « plaignants » ni comme des « parties » au sens des articles 93, 95, 98 et 99 APD, de sorte que leurs conclusions doivent être exclues des débats et ne peuvent être prises en compte.

196. Enfin, la défenderesse affirme que les mesures que l'APD peut imposer en vertu de l'article 100 de la LCA n'apportent aucun avantage à ces plaignants.

197. IAB Europe considère donc que l'affaire a été illégalement engagée - notamment sur la base de plusieurs plaintes irrecevables - de sorte que les griefs formulés à son encontre doivent être rejetés et ne peuvent conduire à l'imposition d'une sanction ou d'une mesure corrective valide à IAB Europe.

Position de la Chambre Contentieuse

198. La Chambre Contentieuse se réfère à l'article 77.1 du RGPD, selon lequel les personnes concernées ont le droit de déposer une plainte dans l'État membre où elles résident habituellement, ont leur lieu de travail ou dans lequel l'infraction présumée a été commise. Les quatre plaintes en anglais mentionnées par le défendeur n'ont pas été déposées directement auprès de l'APD, mais auprès des autorités de contrôle compétentes pour chacun des plaignants, conformément à la législation linguistique applicable localement. *In casu*, les quatre plaintes ont été déposées respectivement auprès de l'autorité de contrôle polonaise, de la SA slovène, de la SA italienne ainsi que de la SA espagnole, qui ont ensuite transmis ces plaintes à l'APD belge en tant qu'autorité de contrôle principale, conformément à la procédure de coopération prévue à l'article 56 du GDPR.

199. Les conditions formelles de recevabilité prévues à l'article 58 de la LCA, et plus particulièrement l'obligation de rédiger la plainte dans une des langues nationales, ne s'appliquent qu'aux plaintes déposées directement auprès de l'APD. Tout autre point de vue nuirait au bon fonctionnement du droit de porter plainte, l'un des éléments fondamentaux du RGPD. En effet, on ne peut attendre d'un plaignant qui soumet sa plainte à une autorité d'un État membre qu'il la soumette dans la langue de l'État membre de l'autorité principale, si celle-ci est différente de l'autorité à laquelle il soumet sa plainte. Il s'ensuit que les quatre plaintes en question ont été valablement déposées auprès de l'APD.

200. En ce qui concerne le défaut d'intérêt de *Fundacja Panoptykon*, ainsi que d'autres plaignants, pour les plaintes déposées par le biais du mécanisme européen de « guichet unique », soulevé par la défenderesse, la Chambre Contentieuse note que *Fundacja Panoptykon* a déposé la plainte auprès de l'autorité de contrôle polonaise au nom de Mme Katarzyna Szymielewicz, conformément à l'article 80.1 RGPD. Sur la base de cette disposition, la plaignante a le droit de charger *Fundacja Panoptykon* de déposer la plainte en son nom.

201. La Chambre Contentieuse note qu'IAB Europe n'explique absolument pas pourquoi *Fundacja Panoptykon* ne devrait pas être considérée comme une plaignante et une partie dans la présente procédure. En outre, en l'absence de doutes sur la recevabilité des autres plaintes, l'argument de la défenderesse ne ferait aucune différence quant à l'issue de cette décision.

202. Cet argument doit donc être rejeté.

b. Le rapport d'inspection n'est pas correctement motivé

203. La défenderesse s'attaque ensuite à la motivation insuffisante du rapport d'inspection. En raison de l'absence d'une motivation clairement formulée dans le rapport d'inspection - notamment l'absence d'un responsable du traitement des données clairement identifié en relation avec une activité de traitement des données clairement définie - la défenderesse fait valoir que le rapport d'inspection non seulement enfreint l'obligation d'APD de motiver expressément et suffisamment ses décisions, mais constitue également une violation manifeste des droits de la défense d'IAB Europe. Par conséquent, le rapport d'inspection porte atteinte aux droits de la défense d'IAB Europe tels qu'ils sont énoncés à l'article 6 de la CEDH et à l'article 47 de la Charte des droits fondamentaux.

Position de la Chambre Contentieuse

204. L'affirmation d'IAB Europe selon laquelle le rapport du Service d'inspection du 13 juillet 2020 n'est pas suffisamment motivé est incorrecte. Comme le montre également le reflet de ce rapport d'inspection dans la présente décision, le rapport d'inspection contient un raisonnement détaillé.

205. En outre, IAB Europe ignore le fait que, outre le rapport du 13 juillet 2020, le Service d'inspection a produit d'autres rapports techniques très complets et détaillés (pièces 24 et 53). Enfin, la Chambre Contentieuse souligne les nombreux échanges de vues écrits et oraux entre les parties devant elle. La simple affirmation d'IAB Europe d'un non-respect de ses droits de la défense est donc sans fondement, comme cela est exposé dans les paragraphes suivants.

c. Caractère incomplet et partialité du rapport d'inspection

206. La défenderesse se réfère à l'article 58.4 GDPR, qui prévoit que la procédure devant l'APD doit être menée dans le respect des « *garanties appropriées, y compris*[...] *le respect de la légalité* ». Selon la défenderesse, ce principe s'applique aussi bien à l'enquête menée par le Service d'inspection qu'aux constatations figurant dans le rapport d'inspection.

207. Se référant aux similitudes avec le rôle et les devoirs d'un procureur dans une procédure pénale ordinaire, la défenderesse affirme que les principes fondamentaux de loyauté, d'impartialité et d'indépendance s'appliquent également au Service d'inspection. La défenderesse se réfère à la section IV de ses conclusions et considère que des éléments à décharge pertinents, dont le Service d'inspection avait ou aurait dû avoir connaissance, sont absents du rapport d'inspection.

208. La défenderesse, soulignant que l'APD est tenue de maintenir la présomption d'innocence d'un défendeur à tout moment, y compris pendant la phase d'enquête d'une procédure pouvant aboutir à des sanctions de nature pénale au sens de l'article 6 de la CEDH, estime que sa présomption d'innocence a été violée et que les demandes contre IAB Europe doivent donc être rejetées.

Position de la Chambre Contentieuse

En ce qui concerne l'autonomie de la Chambre Contentieuse par rapport aux autres organes de l'APD, y compris le Service d'inspection

209. La Chambre Contentieuse relève tout d'abord que la défenderesse semble confondre le rôle et les prérogatives de la Chambre Contentieuse avec ceux des autres organes de l'APD.

210. Comme indiqué ci-dessus, la Chambre Contentieuse est l'organe administratif de résolution des litiges de l'APD, conformément à l'article 33(1) de la LCA. Les dispositions régissant la procédure devant la Chambre Contentieuse (voir les articles 92 à 100 de la LCA) ne montrent pas qu'elle est liée de quelque manière que ce soit par les conclusions d'un autre organe de l'APD. Par conséquent, la Chambre Contentieuse n'est pas liée par les conclusions du Service d'inspection.

211. Il est également rappelé que le Service d'inspection a présenté non pas un mais plusieurs rapports détaillés et techniques exposant clairement les déficiences imputables à la défenderesse et étayant sa position à l'aide de sources législatives, jurisprudentielles et factuelles, comme le soulignent les plaignants. La défenderesse avait accès à ces rapports. De plus, la défenderesse a répondu en détail aux rapports du Service d'inspection.

212. La défenderesse soutient en outre que le rapport du Service d'inspection du 13 juillet 2020 ne serait pas à décharge, mais simplement à charge, car ce rapport ne contiendrait pas « certains éléments à décharge » d'IAB Europe. La défenderesse renvoie également, sans autre précision, à la section IV de ses conclusions, dans laquelle elle expose ses arguments

sur le fond. En l'absence d'informations plus détaillées sur les éléments à décharge qui ont été omis dans le rapport précité du Service d'inspection, cette plainte doit être rejetée.

213. La Chambre Contentieuse note que même si l'on devait suivre l'argument de la défenderesse, quod non, on pourrait néanmoins conclure, comme l'a déjà indiqué la Cour des Marchés, que la procédure devant la Chambre Contentieuse n'était pas illégale dans la mesure où les deux parties ont eu la possibilité de faire valoir leurs arguments dans leurs conclusions[46]. Compte tenu de la complexité du système, la Chambre Contentieuse n'a pas été en mesure de préciser chaque aspect technique du système contre lequel des accusations ont été portées à l'encontre de la défenderesse au début de la procédure devant la Chambre Contentieuse, le 13 octobre 2020, c'est-à-dire au moment où les parties ont été invitées à soumettre leurs conclusions (art. 98 LCA). Toutefois, afin de garantir les droits procéduraux des parties, la Chambre Contentieuse a veillé, d'une part, à ce que la défenderesse ait suffisamment de possibilités de présenter ses arguments devant elle et, d'autre part, à ce qu'elle reste dans le cadre des plaintes initiales et des rapports du Service d'inspection, communiqués aux deux parties avant leurs conclusions écrites.

Concernant le cadre juridique des enquêtes du Service d'inspection

214. Il convient également de rappeler que le Service d'inspection peut mener toute enquête, procéder à toute audition et recueillir toute information qu'il juge utile dans le cadre de ses missions afin de veiller au respect des principes fondamentaux de la protection des données à caractère personnel[47].

215. La Chambre Contentieuse rappelle également que l'intervention du Service d'inspection dans la procédure consiste à enregistrer des constatations et qu'il n'a pas le pouvoir d'imposer des sanctions.

216. Contrairement à ce que soutient la défenderesse, le Service d'inspection n'est pas une autorité administrative de droit pénal au sens de l'article 6 de la Convention européenne des droits de l'homme (ci-après : « CEDH »), car il n'a pas de pouvoir de sanction et sa tâche se limite à effectuer des constatations et à les transmettre à la Chambre Contentieuse dans son rapport. Comme indiqué ci-dessus[48], les conclusions du Service d'inspection ne sont que des éléments sur lesquels la Chambre Contentieuse fonde sa décision à un stade ultérieur de la procédure. Néanmoins, la Chambre Contentieusesouligne que l'enquête du Service d'inspection dans la présente affaire a été menée de manière impartiale, conformément aux exigences de l'article 6 de la CEDH et de l'article 47 de la Charte. Elle

[46] Cour des Marchés, 2019/AR/741, 12 juin 2019, p. 12, disponible sur le site de l'APD.

[47] Cf. Art. 64 de la loi APD : « L'inspecteur général et les inspecteurs exercent les compétences visées dans le présent chapitre en vue du contrôle tel que prévu à l'article 4, § 1er, de la présente loi. » Voir également l'art. 72(1) de la loi DPA : « Sans préjudice des dispositions du présent chapitre, l'inspecteur général et les inspecteurs peuvent procéder à toute enquête, tout contrôle et toute audition, ainsi que recueillir toute information qu'ils estiment utile afin de s'assurer que les principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel, sont effectivement respectées. » (soulignement ajouté).

[48] Voir para. 209-210 de cette décision.

s'oppose aux suggestions de la défenderesse dans la mesure où elles mettent en cause l'impartialité du Service d'inspection.

Concernant le respect du droit à un procès équitable, y compris le droit à la défense devant la Chambre Contentieuse

217. La Chambre Contentieuse partage l'avis de la défenderesse sur l'importance d'appliquer les garanties procédurales relatives au respect de la légalité dans les litiges dont elle est saisie. Il est également établi que ces principes sont effectivement appliqués devant la Chambre Contentieuse.

218. Ainsi qu'il a été exposé ci-dessus[49], le grief de la défenderesse concernant le prétendu manque de motivation et d'impartialité du rapport du Service d'inspection, sur lequel la défenderesse se fonde pour conclure à la violation de son droit à un procès équitable, doit être rejeté.

219. Par souci d'exhaustivité, la Chambre Contentieuse rappelle également que la Cour des Marchés a déjà jugé que — dans l'hypothèse où les garanties procédurales dans la phase antérieure de la procédure n'étaient pas assurées, *quod non* — les parties disposent d'un recours adéquat contre les décisions des organes administratifs, notamment par la possibilité d'un recours devant la Cour des Marchés[50].

220. La Cour des marchés a ajouté qu'un manque d'impartialité de la part d'une autorité administrative ne constitue pas nécessairement une violation de l'article 6.1 CEDH si une autorité judiciaire dotée d'un plein pouvoir de contrôle, qui respecte elle-même les garanties de l'article 6.1 CEDH, peut contrôler la décision en question.

221. Selon la Cour des marchés, une violation du principe d'impartialité de l'administration à un stade antérieur n'entraîne pas nécessairement une violation du droit à un procès équitable si cette violation peut être réparée à un stade ultérieur. La possibilité d'un recours devant une juridiction qui respecte les garanties de l'article 6 de la CEDH vise précisément à permettre de telles corrections[51].

222. Concernant spécifiquement la Chambre Contentieuse, la Cour des marchés a statué comme suit :

[49] Voir para. 204 et s. de cette décision.

[50] « Le législateur a donné au citoyen une voie de recours probante contre le comportement des organes administratifs (en l'occurrence l'APD) en prévoyant précisément le recours au tribunal du marché », Cour d'appel de Bruxelles, section de la Cour des marchés, 19e chambre A, section de la Cour des marchés, 2019/AR/741, 12 juin 2019, p. 9.

[51] « Un manque d'impartialité objective ou structurelle de la part d'une autorité administrative ne constitue pas nécessairement une violation de l'article 6.1 de la CEDH si la décision de cette autorité peut être ultérieurement contrôlée par une juridiction pleinement compétente et qui offre toutes les garanties prévues à l'article 6.1. En conséquence, une violation du principe d'impartialité à un stade antérieur n'entraîne pas nécessairement une négation du droit à un procès équitable si cette violation peut encore être corrigée à un stade ultérieur. L'organisation d'un recours auprès d'une instance qui répond à toutes les garanties de l'article 6 de la CEDH sert à rendre ce recours possible », Cour d'appel de Bruxelles, section Cour des marchés, 19e chambre A, Chambre de la Cour des marchés, 2019/AR/741, 12 juin 2019, p. 10.

> « [...] *même dans ce cas, cette protection juridique par le sujet de droit n'est juridiquement opposable que devant un juge (qui fait partie du pouvoir judiciaire) [...]. La possibilité légale d'introduire une action/un recours devant la Cour des marchés vise à offrir au justiciable la garantie de l'article 6.1 de la CEDH et, plus particulièrement, le recours prévu à l'article 47 de la CDFUE [Charte des droits fondamentaux de l'Union européenne]* ».[52]

223. Dès lors, en l'absence d'impartialité de la part de la Chambre Contentieuse, *quod non* en l'espèce, et dans la mesure où la Cour des marchés exerce un contrôle juridictionnel complet des décisions de la Chambre Contentieuse, il ne pourrait être conclu, *ipso facto*, à une violation du droit à un procès équitable dans la procédure.

224. Dans un souci de clarté et d'information, la Chambre Contentieuse relève que si les droits de la défense font partie des droits fondamentaux qui constituent l'ordre juridique de l'Union et sont consacrés par la Charte[53], il n'en demeure pas moins que, comme l'a jugé la CJUE, les différentes composantes du droit à un procès équitable, dont les droits de la défense, n'ont pas un caractère absolu et que toute restriction peut être possible pour un motif d'intérêt général. Cette appréciation doit être faite *in concreto* :

> « *La Cour a toutefois déjà considéré que les droits fondamentaux, tels que le respect des droits de la défense, n'apparaissent pas comme des prérogatives absolues, mais peuvent comporter des restrictions, à condition que celles-ci répondent effectivement à des objectifs d'intérêt général poursuivis par la mesure en cause et ne constituent pas, au regard du but poursuivi, une intervention démesurée et intolérable qui porterait atteinte à la substance même des droits ainsi garantis (...)* [...].
>
> *34. En outre, la question de savoir si les droits de la défense ont été violés doit être appréciée à la lumière des circonstances spécifiques de chaque cas* [...] »[54].

A.9.2. - Atteintes aux droits et libertés fondamentaux d'IAB Europe en ce qui concerne le caractère général de la procédure de l'APD

a. Sanctions administratives et articles 6 et 7 de la CEDH et article 47 de la Charte des droits fondamentaux de l'Union européenne

225. La défenderesse soutient que les mesures et les amendes que l'APD est autorisée à imposer dans le cadre des articles 100 et 101 de la LCA, lus conjointement avec l'article 83 du RGPD, doivent être qualifiées de sanctions de nature pénale au sens des conventions internationales en matière de droits de l'homme telles que la CEDH et la Charte des droits fondamentaux, eu égard à la nature même des infractions ainsi qu'à la nature et à la sévérité des sanctions qui peuvent être imposées à une partie. Par conséquent, selon la

[52] Cour d'appel de Bruxelles, section du tribunal du marché, 2020/AR/329, 2 septembre 2020. Les arrêts de la Cour des Marchés sont disponibles sur le site de l'APD en leur langue originelle (néerlandais ou français).
[53] À cet égard, voir CJUE, 18 juillet 2013, *Commission et autres c/ Kadi*, C- -584/10 P, C- -593/10 P et C- -595/10 P, ECLI:EU:C:2013:518, para. 98 et 99.
[54] CJUE, 10 septembre 2013, C-383/13 PPU, *Affaire G. et R.*, ECLI:EU:C:2013:533, para. 33 et suiv.

défenderesse, les articles 6 et 7 de la CEDH et l'article 47 de la Charte des droits fondamentaux sont applicables aux sanctions que l'APD peut imposer à IAB Europe.

226. La défenderesse considère ensuite que la grande marge entre le montant minimal et le montant maximal des sanctions administratives de nature pénale, qui, en outre, selon la défenderesse, met toutes les infractions sur un pied d'égalité tout en omettant de préciser la sévérité des sanctions dans la loi elle-même, est contraire aux principes fondamentaux de légalité matérielle et de proportionnalité. Le même raisonnement s'applique aux articles 100 et 101 de la LCA, *lus conjointement avec* l'article 83 du RGPD, qui, en raison de leur formulation imprécise et ambiguë, ne permettent pas à une partie d'évaluer de manière appropriée les conséquences pénales d'un certain comportement avant sa survenance.

227. Il s'ensuivrait par conséquent que les articles 100 et 101 de la LCA, lus conjointement avec l'article 83 du RGPD, seraient contraires aux principes fondamentaux de légalité matérielle et de proportionnalité énoncés aux articles 6 et 7 de la CEDH et à l'article 47 de la Charte des droits fondamentaux. Pour ces raisons, la défenderesse considère que les articles 100 et 101 de la LCA, lus conjointement avec l'article 83 du RGPD, ne pourraient constituer une base juridique valable pour que l'APD impose une sanction à IAB Europe.

Position de la Chambre Contentieuse

228. Tout d'abord, le pouvoir d'imposer une amende administrative et les modalités de son application sont prévus par l'article 83 du RGPD, d'effet direct. Conformément à la jurisprudence de la Cour des marchés, la Chambre Contentieuse considère que les amendes administratives, ainsi que les autres mesures correctives prévues à l'article 58 RGPD, constituent une partie puissante des outils d'exécution dont dispose l'APD[55].

229. Si l'APD constate une ou plusieurs infractions au règlement, elle doit déterminer la ou les mesures correctives les plus appropriées pour remédier à cette infraction. Les mesures disponibles à cette fin sont énumérées à l'article 58.2 *.b* à 58.2*.j* du RGPD. En particulier, l'article 58.2*.i* RGPD prévoit que l'autorité de contrôle a le pouvoir, selon les circonstances de chaque cas, d'imposer, en plus ou à la place des mesures visées dans ce paragraphe, une amende administrative conformément à l'article 83 RGPD. Cela signifie qu'une amende administrative peut être à la fois une mesure autonome (corrective) et une mesure prise conjointement avec d'autres mesures correctives (et constitue donc une sorte de mesure complémentaire). Les dispositions pénales des articles 83.4 à 83.6 du RGPD permettent l'imposition d'une amende administrative pour la plupart des infractions. Néanmoins, l'autorité de surveillance a la responsabilité de toujours choisir la ou les mesures les plus appropriées[56].

[55] Cour d'appel de Bruxelles, section du tribunal du marché, 2021/AR/320, 7 juillet 2021, p. 38.
[56] *Ibidem*.

230. Outre les dispositions pertinentes du RGPD et de la LCA sur le niveau des amendes administratives que la Chambre Contentieuse peut imposer, la Chambre Contentieuse s'appuie également sur la jurisprudence de la Cour des marchés[57], qui formule des exigences sur la prévisibilité et la motivation des amendes administratives imposées par la Chambre Contentieuse. Cette jurisprudence a par exemple conduit à ce qu'un formulaire notifiant l'intention d'imposer une sanction soit soumis à la partie concernée, qui peut y réagir et envoyer ses commentaires à la Chambre Contentieuse avant qu'elle ne prenne une décision. En conséquence, dans la présente procédure, ce formulaire a été envoyé et le défendeur a soumis une réaction[58].

231. La Chambre Contentieuse se réfère également à la jurisprudence de la Cour des marchés, qui a constaté que le RGPD ne prévoit pas de fourchette d'amende spécifique pour des infractions spécifiques, mais seulement une limite supérieure ou un montant maximal. En pratique, cela signifie que l'APD peut décider non seulement de ne pas imposer d'amende au contrevenant, mais aussi que, si elle décide d'imposer une amende, celle-ci sera comprise entre le minimum, à partir de 1 EUR, et le maximum prévu. L'amende est décidée par l'APD en tenant compte des critères énumérés à l'article 83, paragraphe 2, du RGPD.[59].

232. En outre, la Chambre Contentieuse suit également les lignes directrices du Groupe de travail Article 29 sur la protection des données concernant l'application et la fixation des amendes administratives en vertu du RGPD, approuvées par l'EDPB[60], qui détaillent les critères de l'article 83(2) RGPD qu'une autorité de contrôle doit appliquer lorsqu'elle évalue l'opportunité d'imposer une amende, ainsi que le montant de l'amende.

233. En outre, ces lignes directrices contiennent également une explication de l'article 58 du RGPD relatif aux mesures qu'une autorité de surveillance peut choisir de prendre, étant donné que les remèdes sont par nature différents et ont essentiellement des objectifs différents. Enfin, il précise que certaines mesures au titre de l'article 58 RGPD peuvent être cumulatives et constituer ainsi une action réglementaire fondée sur plusieurs recours.

234. La Cour des marchés, statuant en pleine juridiction, effectue un contrôle de légalité et de proportionnalité de la sanction et réduira ou annulera (seulement) l'amende en cas de circonstances graves et avérées que la Chambre Contentieuse ne prendrait pas ou pas suffisamment en compte.

235. En résumé, ce système garantit suffisamment le respect des principes juridiques fondamentaux découlant de l'article 6 de la CEDH et de l'article 47 de la Charte.

---

[57] Entre autres, les arrêts du 19 février 2020 (2019/AR/1600), du 24 janvier 2021 (2020/AR/1333) et du 7 juillet 2021 (2021/AR/320).

[58] Voir para. 272-273.

[59] Cour d'appel de Bruxelles, section Cour des marchés, 2021/AR/320, 7 juillet 2021, p. 38.

[60] EDPB - Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679, WP253, publiées sur http://www.edpb.europa.eu.

Cadre juridique des amendes administratives

Dispositions pertinentes de la LCA

236. En vertu de l'article 100(1)(13) de la LCA, la Chambre Contentieuse a le pouvoir d'imposer des amendes administratives. La Chambre Contentieuse peut décider d'imposer une amende administrative aux parties poursuivies selon les modalités générales prévues à l'article 83 RGPD.

237. Conformément à l'article 103 de la LCA, si un contrevenant a commis plusieurs infractions par un même acte, seule l'amende administrative la plus lourde des infractions concernées s'applique. En cas de chevauchement d'infractions, les taux des amendes administratives s'additionnent sans que le montant total ne puisse dépasser le double du montant le plus élevé de l'amende applicable aux infractions commises.

Dispositions pertinentes du RGPD

238. Dès lors qu'une infraction au règlement a été établie, sur la base de l'appréciation des faits de l'espèce, l'autorité de contrôle compétente devrait déterminer les mesures correctives les plus appropriées pour remédier à l'infraction. Les dispositions de l'article 58(2)(b)-(j)[61] définissent les outils que les autorités de contrôle peuvent utiliser pour remédier au non-respect des règles par un responsable du traitement ou un sous-traitant.

    a. avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ;

    b. rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement ;

    c. ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement ;

    d. ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ;

    e. ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel ;

    f. imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;

[61] L'article 58, paragraphe 2, point a), dispose qu'un avertissement peut être émis. En d'autres termes, dans le cas auquel la disposition se rapporte, une sanction corrective ne sera pas imposée..

g. ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 RGPD et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19 RGPD ;

h. révoquer une certification ou ordonner à l'organisme de certification de révoquer une certification délivrée en application des articles 42 et 43 RGPD, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites ;

i. en fonction des caractéristiques propres à chaque cas, imposer une amende administrative en application de l'article 83 RGPD, en complément ou à la place des mesures visées au présent paragraphe ; et

j. ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

239. Le pouvoir d'imposer une amende administrative est régi par l'article 83 du RGPD, qui dispose :

> *Conditions générales pour imposer des amendes administratives*
>
> *1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.*
>
> *2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :*
>
> *a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;*
>
> *a) le fait que la violation a été commise délibérément ou par négligence ;*
> *b) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;*
> *c) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;*
> *d) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;*
> *e) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;*
> *f) les catégories de données à caractère personnel concernées par la violation ;*
> *g) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;*
> *h) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;*

i) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et
j) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

3. Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :
b) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43 ;
c) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43 ;
d) les obligations incombant à l'organisme chargé du suivi des codes de conduite en vertu de l'article 41, paragraphe 4.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :
a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 ;
b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 ;
c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49 ;
d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX ;
e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

7. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58, paragraphe 2, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

8. L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

9. […] »

240. La lecture de l'article 83, paragraphe 2, RGPD, points *(a)* à *(k)*, ainsi que des explications complémentaires figurant aux paragraphes 3 à 6 de cette même disposition, suffit à réfuter

l'argument de la défenderesse selon lequel les différentes infractions énumérées à l'article 83 RGPD sont placées sur un pied d'égalité.

241. Les différents critères permettant d'évaluer la sévérité des sanctions sont clairement énoncés à l'article 83 lui-même et aux considérants 148 à 150 du RGPD. L'article 83.2 précise également qu'une analyse doit être faite « en fonction des circonstances de l'espèce ».

242. La Chambre Contentieuse a déjà fait référence aux Lignes directrices sur l'application et la fixation des amendes administratives en vertu du RGPD, approuvées par l'EDPB. Ces lignes directrices fournissent des conseils sur l'interprétation des faits individuels du cas à la lumière des critères énoncés à l'article 83.2 du RGPD. Les lignes directrices lient la Chambre Contentieuse en tant qu'organe de l'APD, membre de l'EDPB.

243. Afin de renforcer l'application des règles du RGPD, le considérant 148 du RGPD précise que des sanctions y compris des amendes administratives devraient être infligées pour toute violation du règlement, en complément ou à la place des mesures appropriées imposées par les autorités de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

244. Contrairement à ce que soutient la défenderesse, le RGPD n'impose donc pas un montant minimal d'amende, mais seulement des montants maximaux qui, en fonction des infractions commises, peuvent s'élever à 2 % ou 4 % du chiffre d'affaires d'un responsable de traitement, soit respectivement 10 000 000 ou 20 000 000 euros. Ces montants ont un caractère dissuasif et il appartient à la Chambre Contentieuse de moduler le montant de l'amende en fonction des circonstances de l'espèce, en tenant compte de l'exigence de proportionnalité et en vue d'assurer l'effectivité des dispositions du RGPD.

245. Dès lors que les différentes infractions énumérées à l'article 83 RGPD ne sont pas traitées de la même manière et que les différents critères d'appréciation de la sévérité des sanctions sont clairement énoncés, il convient de rejeter l'argument de la défenderesse selon lequel la lecture combinée de l'article 83 RGPD et des articles 100 et 101 de la LCA

viole les principes de légalité et de proportionnalité, et donc les articles 6 et 7 CEDH et 47 de la Charte des droits fondamentaux de l'Union européenne, en raison de son imprécision.

246. L'article 83 RGPD est une disposition à effet direct d'un règlement de l'UE et il appartient à la Chambre Contentieuse de veiller au bon fonctionnement de ce règlement. Il n'appartient pas à la Chambre Contentieuse, en tant qu'organe d'une autorité administrative nationale, de se prononcer sur l'éventuelle illégalité de cette disposition.

247. Par ailleurs, la Cour constitutionnelle a jugé dans son arrêt n°25/2016, du 18 février 2016 (p24-28) qu'une marge unique et large pour une amende administrative, permettant à l'autorité administrative d'adapter l'amende administrative à la gravité de l'infraction, ne viole pas le principe de légalité :

> « *B.18.2.*
>
> *« B.18.2. En outre, le principe de légalité en matière pénale qui découle des dispositions constitutionnelles et conventionnelles précitées procède de l'idée que la loi pénale doit être formulée en des termes qui permettent à chacun de savoir, au moment où il adopte un comportement, si celui-ci est ou non punissable et, le cas échéant, de connaître la peine encourue. (...)*
>
> *Toutefois, le principe de légalité en matière pénale n'empêche pas que la loi attribue un pouvoir d'appréciation au juge. Il faut en effet tenir compte du caractère de généralité des lois, de la diversité des situations auxquelles elles s'appliquent et de l'évolution des comportements qu'elles répriment.*
>
> *De même, afin de déterminer si les fourchettes des peines retenues par le législateur ordonnanciel sont à ce point larges qu'elles méconnaîtraient le principe de prévisibilité de la peine, il faut tenir compte des spécificités des infractions auxquelles ces peines se rattachent. (...)*
>
> *B.20.1. L'appréciation de la gravité d'une infraction et de la sévérité avec laquelle l'infraction peut être punie relève du pouvoir d'appréciation du législateur compétent. Il peut imposer des peines particulièrement lourdes dans des matières où les infractions sont de nature à porter gravement atteinte aux droits fondamentaux des individus et aux intérêts de la collectivité. C'est dès lors au législateur compétent qu'il appartient de fixer les limites et les montants à l'intérieur desquels le pouvoir d'appréciation du juge et celui de l'administration doivent s'exercer. La Cour ne pourrait censurer un tel système que s'il était manifestement déraisonnable.*
>
> *B.20.2. Il ne saurait être reproché au législateur ordonnanciel d'avoir voulu rationnaliser et simplifier le droit pénal environnemental en vigueur dans la Région. En vue d'atteindre cet objectif, il a pu prévoir une fourchette de peines unique et suffisamment large, aussi bien en ce qui concerne les sanctions pénales que les amendes administratives alternatives, afin de permettre au juge ou à l'autorité administrative d'adapter la peine ou l'amende administrative alternative à la gravité de l'infraction.*

B.20.3. En ce qui concerne spécifiquement l'infraction de dépassement des normes de bruit fixées par le Gouvernement, les dispositions attaquées s'adressent à des justiciables professionnels qui peuvent évaluer avec suffisamment de précision la gravité de l'infraction qu'ils commettent et l'importance corrélative de la sanction à laquelle ils s'exposent. Par ailleurs, le choix de la sanction doit être motivé, soit par le juge, soit par l'autorité administrative. Dans ce dernier cas, un recours juridictionnel est ouvert contre la décision.

B.20.4. Il résulte de ce qui précède que les dispositions attaquées n'attribuent pas au juge ou à l'autorité administrative un pouvoir d'appréciation qui excéderait les limites de ce qu'admet le principe de prévisibilité de la peine. »

248. Il convient donc de rejeter l'argument de la défenderesse selon lequel les articles 100 et 101 de la LCA, *lus conjointement avec* l'article 83 du RGPD, qui constituent le fondement du pouvoir de la Chambre Contentieuse d'imposer des sanctions administratives et des amendes, violent les principes de légalité et de proportionnalité et, partant, le droit à un procès équitable.

b. Le règlement intérieur de l'APD ne respecterait pas le principe fondamental de la légalité formelle des sanctions pénales, consacré par les articles 12 et 14 de la Constitution belge.

249. Le principe de légalité formelle, consacré par les articles 12 et 14 de la Constitution belge, exige que les éléments essentiels des règles relatives aux infractions réprimées, à la nature et au niveau de la sanction, ainsi qu'à la procédure garantissant la sauvegarde des droits de la défense, soient fixés par la Chambre des représentants selon la procédure législative prévue par la Constitution belge.

250. Ce principe s'appliquant non seulement aux sanctions pénales *stricto sensu*, mais aussi aux sanctions administratives de nature pénale, il serait pleinement applicable à la procédure de sanction de l'APD.

251. À cet égard, la défenderesse prétend que plusieurs aspects de la procédure de sanction de l'APD ne sont pas fixés dans un texte législatif - en particulier, non pas dans la LCA, mais dans le règlement d'ordre intérieur du 15 janvier 2019 (ROI).

252. En conséquence, la défenderesse considère que la présente procédure a été menée sur la base de règles de procédure contraires aux articles 12 et 14 de la Constitution belge et qu'elle est donc dépourvue de base légale valable, de sorte que les plaintes contre IAB Europe devraient être rejetées.

Position de la Chambre Contentieuse

253. Le principe de légalité signifie que les éléments essentiels d'une infraction, tels que sa nature, le niveau de la sanction et les garanties procédurales y afférentes, doivent être déterminés par le législateur.

254. La Chambre Contentieuse relève que les seuls éléments relatifs à l'imposition d'une sanction qui ne figurent ni dans le RGPD, ni dans la LCA, ni dans la loi du 30 juillet 2018, mais dans le Règlement d'ordre intérieur (ROI) de l'APD auquel se réfère la défenderesse, ne sont en aucun cas des éléments essentiels pour l'imposition d'amendes. En effet, ce n'est pas la nature de l'amende, ni la sanction, qui sont en cause, mais des éléments de nature secondaire ou organisationnelle, par exemple quant à la procédure à suivre en l'absence du président de la Chambre Contentieuse (article 44 ROI), ou le nombre de membres siégeant par affaire (article 43 ROI).

255. La Chambre Contentieuse souligne également que l'indépendance d'une autorité de contrôle en vertu de l'article 51 et suivants du RGPD signifie que l'organisation de ses processus, y compris par exemple l'affectation des membres à une procédure, est à la discrétion de l'Autorité de protection des données, bien entendu dans les limites des principes généraux de bonne administration et de la législation nationale pertinente.

256. L'argument de la défenderesse selon lequel la procédure devant la Chambre Contentieuse violerait le principe de légalité est donc rejeté.

c. La nomination des membres de l'APD violerait l'article 53 du RGPD

257. La défenderesse prétend que l'article 39 de la LCA, qui règle la nomination des membres de la Chambre Contentieuse, ne précise nullement les modalités de la procédure de nomination. En particulier, il ne précise nulle part comment l'audition des candidats doit se dérouler, et la loi sur la protection des données n'exige pas de compte rendu écrit de l'audition. En outre, la nomination a lieu sur la base d'un vote secret et il n'existe aucune garantie quant à l'adéquation des informations sur les candidats fournies aux membres de la Chambre des représentants.

258. Selon la défenderesse, la nomination des membres de l'APD, y compris des membres de la Chambre Contentieuse, ne répondrait donc pas aux exigences de l'article 53 RGPD, qui prévoit que la nomination doit être effectuée « au moyen d'une procédure transparente ».

259. Au vu de ce qui précède, la défenderesse considère que les membres de la Chambre Contentieuse ne seraient pas en mesure de prendre une décision juridiquement valide à l'égard de IAB Europe dans cette affaire. Pour ces raisons également, les demandes contre IAB Europe devraient être rejetées.

Position de la Chambre Contentieuse

260. Tout d'abord, la Chambre Contentieuse rappelle que les éventuelles imperfections de la procédure de désignation des membres de l'APD ne peuvent faire partie de cette procédure et que les parties ne peuvent invoquer un intérêt procédural pour remettre en cause la procédure de désignation.

261. La Chambre Contentieuse rappelle que les membres de la Chambre Contentieuse sont nommés par la Chambre des Représentants et ne peuvent être démis de leurs fonctions que par celle-ci. Ainsi, ni la Chambre Contentieuse ni la Cour des marchés ne sont compétentes pour statuer sur leur nomination. En outre, les parties n'ont aucun intérêt à demander une telle décision.

262. Par conséquent, la Chambre Contentieuse juge que cette allégation n'est pas fondée.

d. La manière dont l'APD a traité cette procédure ne serait pas conforme à ses obligations et à ses pouvoirs en vertu de l'article 57 du RGPD.

263. En conclusion, la défenderesse indique, tant dans son conclusion initial que dans le cadre de la réouverture des débats, que la manière dont l'APD, en plus de la plainte initiale, examine également les plaintes et griefs supplémentaires formulés par les plaignants, sans que la pertinence de ces allégations supplémentaires ait été examinée par le Service d'inspection, rend la défense d'IAB Europe considérablement plus difficile.

264. IAB Europe considère que cette approche est non seulement fondamentalement incompatible avec les devoirs et les responsabilités d'une autorité de surveillance tels que définis à l'article 57 du RGPD, mais a également pour effet qu'IAB Europe n'est tenue de se défendre que contre les allégations contenues dans le rapport d'inspection, et non contre les allégations ultérieures formulées par les plaignants dans leurs présentations d'arguments ultérieures.

Position de la Chambre Contentieuse

265. La Chambre Contentieuse souligne tout d'abord qu'à aucun moment la défenderesse n'a expliqué quelles nouvelles allégations font l'objet de ses arguments en défense et violeraient ainsi ses droits de la défense. Pour cette seule raison, la Chambre Contentieuse s'estime fondée à déclarer le moyen de la défenderesse non fondé.

266. En second lieu, la Chambre Contentieuse relève que la LCA ne prescrit nullement que la Chambre Contentieuse serait liée par un rapport d'enquête suite à une enquête demandée au Service d'inspection. En effet, il ne résulte d'aucune disposition de la LCA que la Chambre Contentieuse serait privée de la possibilité de prendre en compte des éléments supplémentaires ou complémentaires au rapport du Service d'inspection, pour autant que l'enquête et la prise en compte de ces éléments supplémentaires soient suffisamment justifiées dans la décision et que les droits de la défense soient suffisamment garantis.

267. Le Service d'inspection peut en tout état de cause décider de ne pas enquêter sur certains points litigieux, conformément à la prérogative que lui confère l'article 64 (2) de la LCA. Dans un tel cas, il serait toutefois contraire à l'article 57 RGPD ainsi qu'à l'autonomie et à l'indépendance de la Chambre Contentieuse, telles que mises en œuvre par les articles 92 à 100 de la LCA, de lier purement et simplement la Chambre Contentieuse par les

conclusions du Service d'inspection, sans tenir compte des éléments avancés dans les débats par les parties en cours de procédure et conformément au droit d'être entendu.

268. Troisièmement, la Chambre Contentieuse décide que la prétendue obligation de fonder les débats sur le seul rapport d'inspection à la suite d'une enquête du Service d'inspection n'est pas applicable. La LCA ne prévoit nulle part que la Chambre Contentieuse devrait fonder sa décision uniquement sur le rapport d'inspection ou sur les conclusions des parties. Il convient qu'une autorité de contrôle consulte également d'autres organes et sources afin de pouvoir étayer ses décisions si nécessaire.

269. Pour ce qui est de l'appréciation du Service d'inspection en vue d'une enquête complémentaire, et notamment la nature des délais prévus à l'article 96 de la LCA, la Chambre Contentieuse n'est pas convaincue par les arguments avancés par la défenderesse. En l'espèce, les parties ont eu amplement l'occasion de faire connaître leur point de vue à la Chambre Contentieuse et à lapartie adverse concernant les allégations et les charges, y compris le fonctionnement du TCF, le traitement des préférences et des permissions des utilisateurs dans la TC String, ainsi que l'interrelation entre le TCF et l'OpenRTB.

270. En outre, la Chambre Contentieuse estime qu'il n'y a aucun doute sur l'importance cruciale de la TC String pour le fonctionnement du TCF. Par conséquent, la défenderesse pouvait s'attendre, dès le début de la procédure, à ce que les débats se concentrent sur le traitement des données dans le cadre de la TC String. Ainsi, il ne saurait être question d'allégations nouvelles - pour autant qu'elles existent, compte tenu de l'absence d'exemple concret avec lequel la défenderesse a étayé son moyen - dans les conclusions des plaignants, puisqu'elles constituent une explication du fonctionnement du TCF, dont il n'est pas contesté qu'il est au cœur des plaintes contre IAB Europe.

271. Compte tenu de ce qui précède, la Chambre Contentieuse juge que ce moyen est insuffisant tant en fait qu'en droit.

A.10. – Formulaire de sanction, procédure de coopération européenne, et publication de la décision

272. La procédure devant la Chambre Contentieuse comprend un échange d'conclusions écrites ainsi qu'une audition orale des parties concernées, comme étapes usuelles dans le cadre d'une décision. Si la Chambre Contentieuse propose, après délibération, d'imposer une sanction (punitive), la Cour des Marchés exige que la Chambre Contentieuse donne à la défenderesse l'opportunité de répondre aux sanctions envisagées, par le biais d'un formulaire standard couvrant également les infractions retenues et les critères de détermination du montant de l'amende. Cette possibilité de contradictoire, ou droit d'être entendu, ne concerne que les sanctions proposées et n'est donc communiquée qu'au défendeur.

273. Un formulaire de sanction a été envoyé le 11 octobre 2021 au défendeur, informant ce dernier de ses infractions au RGPD ainsi que de l'intention de la Chambre Contentieuse d'imposer des mesures correctives et une amende administrative. IAB Europe a soumis sa réponse le 1er novembre 2021. La défenderesse conteste le calcul de l'amende administrative, en affirmant que la Chambre Contentieuse n'a pas pris en compte tous les éléments pertinents pour déterminer le montant de l'amende administrative en vertu de l'article 83.2 GDPR. En outre, la défenderesse conteste la prise en compte par la Chambre Contentieuse du chiffre d'affaires annuel mondial total d'Interactive Advertising Bureau Inc. (IAB Inc.) pour le calcul de l'amende administrative, puisque cette dernière n'a aucune participation dans la défenderesse ni aucun droit de regard sur le déploiement des activités d'IAB Europe. La défenderesse précise qu'IAB Europe obtient la licence du nom de marque "IAB" auprès de l'IAB Inc. et que les différentes organisations IAB en Europe sont des organisations séparées et distinctes.

274. Le 8 novembre 2021, les plaignants soumettent une requête à la Chambre Contentieuse, demandant à recevoir une copie du formulaire de sanction ainsi que la réaction du défendeur, en se basant sur l'hypothèse erronée que le défendeur aurait également reçu des informations supplémentaires sur le projet de décision de la Chambre Contentieuse. La Chambre Contentieuse répond le 9 novembre 2021 qu'elle ne divulguera pas le formulaire de sanction aux plaignants. La notification du formulaire de sanction au défendeur a lieu dans le cadre d'un contrôle objectif de la légalité et dans le but précis de respecter les droits de la défense du défendeur, conformément à la jurisprudence de la Cour des Marchés. Le défendeur est ainsi informé à l'avance de la nature et de la sévérité de la sanction qu'il risque et a la possibilité de soumettre ses dernières conclusions sur ce point à la Chambre Contentieuse. La notification du formulaire de sanction aux plaignants ne pourrait pas contribuer au même objectif, puisque la sanction envisagée ne serait infligée qu'au défendeur, et non aux plaignants, et n'affecterait donc pas directement les intérêts de ces derniers. Ni les droits de la défense ni aucune autre règle de droit n'exigent que les plaignants puissent présenter des conclusions supplémentaires en rapport avec la sanction que le défendeur est susceptible de se voir infliger.

275. Le 23 novembre 2021, la Chambre Contentieuse a soumis son projet de décision aux autres autorités de contrôle concernées (ci-après, "CSAs"), comme le prévoit l'article 60.3 du RGPD.

276. Le 18 décembre 2021, la Chambre Contentieuse a reçu une lettre des plaignants en réponse à la décision de la Chambre Contentieuse de ne pas divulguer le contenu du formulaire de sanction aux plaignants. Plus précisément, les plaignants ont fait valoir qu'ils devraient être informés si le défendeur a apporté de nouveaux éléments à la procédure. La Chambre Contentieuse constate que les débats étaient déjà clos à ce moment-là, et que la réaction de la défenderesse au formulaire de sanction ne portait que sur des éléments concernant la sanction.

277. Le 20 décembre 2021, la Chambre Contentieuse est informée par le système d'information sur le marché intérieur (IMI) d'une objection pertinente et motivée (RRO) soumise par l'Autorité néerlandaise (Autoriteit Persoonsgegevens, « AP »). L'objection porte sur l'absence de raisonnement de la Chambre Contentieuse concernant l'affirmation de l'ONG néerlandaise Bits of Freedom selon laquelle le TCF rend impossible l'exercice de leurs droits par les personnes concernées. La Chambre Contentieuse a abordé cette objection dans son projet de décision révisé[62].

278. Le 21 décembre 2021, la défenderesse soumet une lettre à la Chambre Contentieuse, demandant la suspension de l'exécution provisoire de la décision, que l'APD ne rende pas la décision publique jusqu'à ce que tous les recours soient épuisés, et que l'APD s'abstienne de toute communication publique sur la décision avant une telle décision finale. Une fois encore, la Chambre Contentieuse note que les débats étaient déjà clos à ce moment-là.

279. Le 21 décembre 2021, la Chambre Contentieuse est notifiée d'une objection pertinente et motivée introduite par l'Autorité portugaise (Comissão Nacional de Proteção de Dados , « CNPD »). L'objection porte sur l'absence de sanction prise par la Chambre Contentieuse à l'égard du traitement de TC Strings en l'absence d'une base légale prévue à l'article 6 RGPD. La CNPD estime que le projet de décision doit imposer à la défenderesse l'effacement immédiat de toutes les données à caractère personnel collectées illégalement à ce jour. La Chambre Contentieuse a abordé cette objection dans son projet de décision révisé[63].

280. En plus des deux objections pertinentes et motivées, la Chambre Contentieuse a reçu des commentaires d'autres CSAs concernant la co-responsabilité établie par la Chambre Contentieuse, l'utilisation de l'intérêt légitime pour certains traitements, la portée des mesures correctives, ainsi que l'amende administrative envisagée et la relation entre IAB Inc. et IAB Europe.

281. Le 13 janvier 2022, la Chambre Contentieuse a soumis son projet de décision révisé aux autres autorités de contrôle concernées, comme le prévoit l'article 60.5 du RGPD.

282. Le 17 janvier 2022, la Chambre Contentieuse a notifié aux parties le dépôt du projet de décision révisé et la date limite du 27 janvier 2022 pour les CSAs. Elle a également précisé que les échanges écrits avec les conseils de la défenderesse, concernant le formulaire de sanction, ne comportaient pas de nouveaux arguments qui nécessiteraient de rouvrir les débats avec les deux parties. Dès lors, et vu que tant ces échanges que le formulaire de sanction feront partie du dossier administratif, la Chambre Contentieuse a rejeté la demande des plaignants d'avoir accès au formulaire de sanction et aux échanges écrits qui ont suivi avec la défenderesse.

[62] Voir para. 504-506
[63] Voir para. 535.

283. Le 20 janvier 2022, la Chambre Contentieuse a reçu une lettre des plaignants, dans laquelle ils réaffirment avoir le droit d'obtenir une copie du formulaire de sanction et des échanges subséquents avec le défendeur, afin de vérifier par eux-mêmes qu'aucun élément nouveau n'ait été soulevé par ce dernier. Les plaignants font également valoir que si le formulaire de sanction et les échanges ultérieurs feront partie du dossier administratif, et seront donc accessibles en cas de recours, il n'y a aucune raison de ne pas leur accorder l'accès pendant la procédure en cours. Les plaignants prétendent en outre, sur la base d'un communiqué de presse de la défenderesse datant du 5 novembre 2021, que la Chambre Contentieuse a accepté d'approuver un Code de conduite soumis par la défenderesse 6 mois après sa décision. Les plaignants soutiennent que ceci n'a pas fait l'objet de débats au cours de la procédure, et demandent donc l'accès à tous les échanges écrits avec la défenderesse suite à la fiche de sanction, ainsi que la réouverture des débats sur la compétence de la Chambre Contentieuse pour approuver un code de conduite ou valider un plan d'action.

284. Le 27 janvier 2022, la Chambre Contentieuse a accusé réception de la lettre du conseil des plaignants, et a répondu que leurs arguments seront pris en considération dans sa délibération.

Position de la Chambre Contentieuse

285. La Chambre Contentieuse constate avant tout qu'elle n'est pas responsable et ne peut être tenue pour responsable des déclarations publiques faites en dehors de la procédure par l'une ou l'autre partie concernée en cours de délibéré sur le fond par la Chambre Contentieuse.

286. Deuxièmement, la Cour des Marchés a déclaré que les plaignants n'ont pas leur mot à dire dans la détermination des sanctions imposées par la Chambre Contentieuse[64]. À cet égard, l'article 58.2.d du RGPD accorde aux autorités de contrôle le pouvoir d'ordonner à un responsable de traitement ou à un sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du RGPD, le cas échéant, d'une manière et dans un délai déterminés. Cette disposition, lue en conjonction avec l'article 100, § 1, 9° de la LCA, doit être interprétée dans le sens qu'un plan d'action et le suivi intrinsèque de ce plan d'action par l'APD, doivent être considérés comme l'une des sanctions qui peuvent être imposées à un responsable de traitement ou à un sous-traitant. Le plan d'action doit donc être considéré comme une mesure corrective, à l'égard de laquelle les plaignants n'ont aucun intérêt à faire valoir leurs moyens.

287. En ce qui concerne la demande de la défenderesse de ne pas publier la décision, la Chambre Contentieuse rappelle l'impact significatif de l'affaire, compte tenu du grand nombre de

[64] Cour des Marchés, 1er décembre 2021, FOD Financiën c. GBA, nr. 2021/AR/1044, para. 7.3.4: " Il n'appartient (certainement) pas à un plaignant de s'immiscer de quelque manière que ce soit dans le caractère approprié, et encore moins dans l'étendue, d'une sanction. La plainte ne concerne (et ne peut concerner) qu'une infraction présumée de telle sorte que la décision prise par la Chambre Contentieuse de l'APD concernant la plainte - et imposant éventuellement une sanction à la personne concernée - ne peut jamais être considérée comme un jugement *ultra petita* du point de vue de la plainte. "

personnes concernées et d'organisations impliquées. En outre, la Chambre Contentieuse note que la demande des défendeurs a été soumise après la clôture des débats, et que la défenderesse elle-même a déjà publié sur l'affaire le 5 novembre 2021. Compte tenu de ces éléments, la Chambre Contentieuse décide de ne pas donner suite à la demande de la défenderesse dd. 21 décembre 2021 concernant la non-publication de la décision et l'absence de communications publiques sur la décision avant épuisement de toutes les voies de recours.

B. Raisonnement

B.1. - Traitement des données à caractère personnel dans le contexte du *Transparency and Consent Framework*

288. Dans cette section, la Chambre Contentieuse examine le concept de données à caractère personnel ainsi que la question de savoir si des données à caractère personnel existent dans le contexte du *Transparency and Consent Framework*, conçu et géré par IAB Europe[65], et si elles sont traitées[66].

289. Pour une bonne compréhension de cette décision, la Chambre Contentieuse souligne que les plaignants ont indiqué dans leurs conclusions écrites qu'ils souhaitaient se limiter aux violations alléguées du RGPD dans le traitement des données à caractère personnel « dans le TCF proprement dit »[67]. La Chambre Contentieuse ne se prononcera donc pas dans cette section sur la responsabilité quant aux opérations de traitement qui ont lieu dans le cadre du protocole OpenRTB.

B.1.1. – Présence de données à caractère personnel dans le TCF

290. La législation européenne sur la protection des données, y compris le RGPD, a toujours adopté une vision large des données à caractère personnel dans le but d'assurer un niveau élevé de protection des données et de sauvegarder les libertés et droits fondamentaux des personnes concernées. L'interprétation large du concept de données à caractère personnel et de la notion de traitement, entre autres, est un élément clé de la jurisprudence de la Cour de justice[68]. Le principe selon lequel les données à caractère personnel ne concernent pas seulement une personne physique *identifiée*, mais aussi une personne physique identifiable, a déjà été établi en 1981 par la Convention du Conseil de l'Europe pour la

[65] Voir titre B.1.1. – Présence de données à caractère personnel dans le TCF.
[66] Voir titre B.1.2. - Traitement de données à caractère personnel dans le TCF.
[67] Conclusions des plaignants du 18 février 2021, p. 2 : « *in het TCF op zich* ».
[68] C. DOCKSEY, H. HIJMANS, « The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law », *EDPL Review*, 2019, p. 300.

protection des personnes à l'égard du traitement automatisé des données à caractère personnel[69].

291. Le RGPD indique sans ambiguïté que toute information concernant une personne physique identifiée ou identifiable (« personne concernée ») constitue une donnée à caractère personnel. « Identifiable » doit donc s'entendre comme la possibilité d'identifier une personne physique directement ou indirectement au moyen d'un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs éléments spécifiques à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique[70].

292. En outre, le RGPD prévoit que, pour déterminer si une personne physique est identifiable, il convient de tenir compte de tous les moyens dont on peut raisonnablement supposer qu'ils seront utilisés soit par le responsable du traitement, *soit par toute autre personne*, pour identifier la personne physique directement ou indirectement, tels que des techniques de ciblage[71].

293. Pour déterminer si l'on peut raisonnablement prévoir que les ressources seront utilisées pour identifier la personne physique, il convient également de tenir compte de tous les facteurs objectifs, tels que le coût et le temps nécessaires à l'identification, compte tenu de la technologie disponible au moment du traitement et des évolutions technologiques[72].

294. Le considérant 30 du RGPD précise que les personnes physiques peuvent être liées à des identifiants en ligne par l'intermédiaire de leurs appareils, applications, outils et protocoles, tels que des adresses de protocole Internet (IP), des cookies d'identification ou d'autres identifiants. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.

295. L'ancien Groupe de travail «Article 29» a déjà abordé l'importance d'une définition large des données à caractère personnel, en particulier le fait qu'une personne physique peut être considérée comme identifiable lorsqu'elle peut être distinguée des autres membres du groupe et par conséquent traitée différemment[73].

296. Cette position est également adoptée par la Cour de justice. Il est de jurisprudence constante que le contenu des informations qualifiées de données à caractère personnel

---

[69] Article 2.*a* de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *B.S.*, 30 décembre 1993 (Convention 108).

[70] Article 4.1 RGPD

[71] Considérant 26 du RGPD ; le texte anglais fait explicitement référence à « *singling out* » comme l'un des moyens d'identifier une personne physique. Voir également l'arrêt de la CJUE C-582/14 du 19 octobre 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 46Fr. Zuiderveen Borgesius, « Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation », *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271.

[72] *Ibidem.*

[73] WP136 - Avis 4/2007 sur le concept de données à caractère personnel, p. 14 ; WP199 - Avis 08.2012 fournissant une contribution supplémentaire aux discussions sur la réforme de la protection des données, p. 5.

n'est pas important[74] et que le critère d'identifiabilité doit être interprété de manière souple. **Tant que des informations, en raison de leur contenu, de leur finalité ou de leur effet, peuvent être reliées à une personne physique identifiée ou identifiable par des moyens pouvant être raisonnablement mis en œuvre[75], et ce, que les informations à partir desquelles la personne concernée peut être identifiée soient détenues entièrement par le même responsable du traitement ou en partie par une autre entité, ces informations doivent être considérées comme des données à caractère personnel**[76].

297. Les plaignants font valoir dans leur conclusions en réponse que la TC String est une chaîne de caractères unique qui est également inscrite dans un cookie en tant qu'identifiant unique et qui est ensuite stockée sur l'appareil d'un utilisateur[77]. En outre, les plaignants estiment qu'IAB Europe collecte des informations supplémentaires sur les utilisateurs à l'aide de la TC String, y compris des données à caractère personnel sensibles au sens de l'article 9 du RGPD[78].

298. La défenderesse, en revanche, réfute les allégations et affirme que la TC String ne contient aucune donnée à caractère personnel[79] ni aucune information directement ou indirectement liée à la « *content taxonomy*[80] », qu'IAB Europe utilise comme « langage commun » pour décrire le contenu d'un site web[81]. En outre, la défenderesse estime que la TC String ne constitue pas un identifiant unique et qu'elle n'est pas conçue à cette fin[82].

299. Nonobstant ce qui précède, la défenderesse indique qu'il doit nécessairement être possible de relier la TC String à un utilisateur, mais sous réserve que ce lien entre les préférences conçues dans la TC String et l'utilisateur n'est établi qu'ultérieurement, à savoir dans le cadre de l'OpenRTB, et n'est donc pas couvert par le *Transparency and Consent Framework*[83].

300. Sur la base de la documentation technique d'IAB Europe et de l'IAB Tech Lab sur le protocole TCF, le Service d'Inspection conclut que la TC String en elle-même n'identifie pas *directement* les utilisateurs ou les appareils, car les éléments qui la composent ne font que refléter des informations techniques, à savoir si un utilisateur non identifié a consenti ou non

---

[74] Conclusions de l'avocat général Sharpston du 12 décembre 2013 dans les affaires jointes C-141/12 et C-372/12 *Y.S.*, para. 45.

[75] Arrêt de la CJUE C-434/16 du 20 décembre 2017, *Nowak t. Commissaire à la protection des données,* ECLI:EU:C:2017:994, para. 35.

[76] Voir également l'arrêt de la CJUE C-582/14 du 19 octobre 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 43 ; arrêt de la CJUE C-434/16 du 20 décembre 2017, *Nowak t. Commissaire à la protection des données*, ECLI:EU:C:2017:994, para. 31: voir aussi FR. ZUIDERVEEN BORGESIUS, « Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation », *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271; and FR. ZUIDERVEEN BORGESIUS, « The Breyer Case of the CJEU - IP Addresses and the Personal Data Definition », *EDPL*, 1/2017, pp. 130-137.

[77] Conclusions des plaignants du 18 février 2021, para. 25.

[78] Conclusions des plaignants du 18 février 2021, para. 26.

[79] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 48.

[80] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 51.

[81] https://iabtechlab.com/standards/content-taxonomy/

[82] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 53.

[83] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 54.

aux finalités Y ou Z, et si les *fournisseurs adtech* A et B peuvent traiter les données à caractère personnel aux fins acceptées.

301. Plus précisément, une TC String se compose des champs suivants :

i. des métadonnées générales ;

ii. une valeur binaire pour chacune des finalités du traitement pour lesquelles le consentement peut être donné ;

iii. une valeur binaire pour chacune des finalités du traitement permises par un intérêt légitime ;

iv. une valeur binaire pour chacun des fournisseurs adtech qui peuvent collecter et traiter les données à caractère personnel de l'utilisateur sur la base de son consentement ;

v. une valeur binaire pour chacun des fournisseurs adtech qui peuvent collecter et traiter les données à caractère personnel de l'utilisateur sur la base d'un intérêt légitime ;

vi. toute restriction de traitement ;

vii. des fonctionnalités spéciales *d'opt-in* en rapport avec les finalités du traitement ;

viii. un champ dédié aux finalités de traitement qui ne relèvent pas du TCF mais qui sont spécifiques à *l'éditeur* ;

ix. consentir au traitement sur des bases juridiques qui ne sont pas couvertes par le TCF.

Position de la Chambre Contentieuse

302. Bien que la Chambre Contentieuse comprenne qu'il n'est pas établi de manière concluante que la TC String, en raison des métadonnées et des valeurs limitées qu'elle contient, permette en elle-même une identification directe de l'utilisateur, la Chambre Contentieuse note que lorsque le pop-up de consentement est accédé, via un script, à partir d'un serveur géré par la CMP[84], celle-ci traite inévitablement aussi l'adresse IP de l'utilisateur, qui est explicitement classée comme une donnée à caractère personnel au sens du RGPD.

303. En effet, le considérant 30 du RGPD indique que les personnes physiques peuvent être liées à des identifiants en ligne par l'intermédiaire de leurs appareils, applications, outils et protocoles, tels que les adresses de protocole Internet (IP), les cookies d'identification ou d'autres identifiants tels que les étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes.

304. Dès qu'un CMP stocke ou lit la TC String sur l'appareil d'un utilisateur par le biais d'un cookie *euconsent-v2*, le consentement ou l'objection au traitement pour des raisons d'intérêt

[84] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 58.

légitime, ainsi que les préférences de cet utilisateur, peuvent être liés à l'adresse IP de l'appareil de l'utilisateur. En d'autres termes, les CMP disposent des moyens techniques de collecter les adresses IP (comme indiqué dans leur pop-up[85]) et de combiner toutes les informations relatives à une personne identifiable. La possibilité de combiner la TC String et l'adresse IP implique qu'il s'agit d'informations concernant un utilisateur identifiable[86].

305. En outre, l'identification de l'utilisateur est possible en établissant un lien avec d'autres données qui peuvent être utilisées par les organisations participantes dans le cadre du TCF, mais aussi dans le contexte du protocole OpenRTB. À cet égard, la Chambre Contentieuse souligne qu'il ne s'agit pas d'une seule et même partie, mais d'organisations participantes — les CMP et *fournisseurs adtech*— qui, comme examiné plus en détail ci-dessous[87], sont tenues de communiquer à la défenderesse, sur simple demande, les informations leur permettant d'identifier les utilisateurs.

306. Par conséquent, la Chambre Contentieuse constate que la défenderesse dispose de moyens raisonnables qu'elle peut utiliser à l'encontre des organisations inscrites qui participent au TCF, et avec lesquels la défenderesse est en mesure d'identifier directement ou indirectement l'utilisateur derrière une TC String.

307. La Chambre Contentieuse comprend également que le TCF est destiné à l'enregistrement de la combinaison de préférences de chaque utilisateur sous la forme d'une chaîne unique dans la TC String, afin de communiquer ces préférences à un grand nombre de fournisseurs adtech, et implique donc intrinsèquement l'enregistrement de ces données.

308. La Chambre Contentieuse a en effet constaté, sur la base des rapports d'enquête du Service d'Inspection, que les *fournisseurs adtech* ainsi que d'autres participants au sein de l'écosystème OpenRTB au sens large lisent le signal contenu dans une TC String afin de déterminer s'ils disposent de la base juridique requise pour traiter les données à caractère personnel d'un utilisateur, pour les finalités auxquelles ce dernier a consenti[88].

309. À cet égard, la Chambre Contentieuse souligne qu'il suffit que certaines informations soient utilisées afin d'individualiser une personne physique, pour pouvoir parler de données à caractère personnel[89]. De plus, la finalité de la TC String, à savoir la saisie des préférences d'un utilisateur *spécifique*, conduit *de facto* à considérer la TC String comme une donnée à caractère personnel.

---

[85] Voir les exemples dans le rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 99 et suivantes.

[86] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, « Consent Management Platforms Under the GDPR: Processors and/or Controllers? », in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51. La Chambre Contentieuse note à cet égard que, jusqu'à cet été, si une TC String « stockée globalement » était choisi, les CMP pouvaient accéder au domaine internet *consensu.org* géré par IAB Europe pour vérifier si un consentement à portée globale avait été donné par l'utilisateur, ce qui impliquait la divulgation des valeurs de la TC String couplées aux adresses IP des utilisateurs aux CMP, par IAB Europe. La défenderesse a annoncé lors de l'audition que la fonctionnalité des consentements à portée globale serait dépréciée.

[87] Voir les para. 358 et suivants de la présente décision.

[88] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 75.

[89] WP136 - Opinion 4/2007 on the concept of personal data, p. 14.

310. En d'autres termes, si la finalité du traitement est d'isoler des personnes, on peut supposer que le responsable du traitement ou une autre partie a ou aura à sa disposition les moyens par lesquels on peut raisonnablement prévoir que la personne concernée sera identifiée. Prétendre que les personnes ne sont pas identifiables, alors que le but du traitement est précisément de les identifier, serait une *contradictio in terminis*[90].

311. En outre, la Chambre Contentieuse est d'avis que l'utilisation de ces préférences a des conséquences indubitables sur les droits et intérêts des personnes concernées, puisque ces choix déterminent, entre autres, quels tiers recevront et traiteront les données à caractère personnel des utilisateurs dans le cadre du protocole OpenRTB[91].

312. Compte tenu des constatations qui précèdent ainsi que de l'interprétation large de la notion de données à caractère personnel, telle que confirmée par la jurisprudence de la Cour de justice[92], la Chambre Contentieuse conclut que les préférences des utilisateurs contenues dans une TC String constituent bien des données à caractère personnel, puisque ces préférences se rapportent à une personne physique individualisée et identifiable[93].

B.1.2. - Traitement de données à caractère personnel dans le TCF.

313. Le Service d'Inspection explique dans ses rapports d'enquête techniques que le TCF repose nécessairement sur trois éléments fondamentaux :

i. une interface utilisateur entièrement personnalisable qui permet aux *Consent Management Platforms* (CMP) inscrites au TCF de recueillir le consentement de l'utilisateur, ses éventuelles objections aux traitements fondés sur un intérêt légitime, et ses préférences concernant les finalités du traitement ainsi que les *fournisseurs adtech* autorisés ;

ii. une liste des fournisseurs adtech mondiaux qui comprend les partenaires approuvés par IAB Europe et des informations spécifiques concernant leurs finalités de traitement et leurs bases légales respectives ; et

iii. un mécanisme standardisé pour demander, enregistrer et éventuellement partager les *fournisseurs adtech* autorisés, les consentements, les objections et les préférences au moyen d'une API dédiée, un format standard pour stocker les partenaires/consentements, et une structure de données normalisée pour transférer le statut des partenaires/consentements[94].

[90] WP136 - Opinion 4/2007 on the concept of personal data, p. 14.
[91] Arrêt de la CJUE C-434/16 du 20 décembre 2017, *Nowak t. Commissaire à la protection des données*, para. 39.
[92] Voir para. 296 et suivants de la présente décision.
[93] Arrêt de la CJUE C-434/16 du 20 décembre 2017, *Nowak t. Commissaire à la protection des données*, para. 34.
[94] Plateforme de Gestion du Consentement API v2.0, août 2019 (pièce 34), p. 4 ; rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 58-59.

314. Les plaignants font valoir que la création de la TC String correspond à la génération automatisée d'une chaîne de caractères unique associée à un utilisateur spécifique, par laquelle ses préférences en matière d'échange de données sont saisies suite à l'intervention d'un CMP inscrit au TCF[95].

315. En outre, les plaignants mentionnent le partage de la TC String avec les CMP et les autres participants au TCF. Plus précisément, ils soutiennent que le stockage d'une TC String dans un cookie *euconsent-v2* spécifique, sur un système de stockage choisi par la CMP ou associé au domaine Internet *consensu.org* géré par IAB Europe, constitue également un traitement des préférences des utilisateurs.

316. La défenderesse, en revanche, fait valoir qu'il n'y a pas de traitement de données à caractère personnel au sens de l'article 4.2) du RGPD dans le cadre du TCF, étant donné son point de vue selon lequel la TC String en tant que telle ne peut être considéré comme une donnée à caractère personnel.

Appréciation par la Chambre Contentieuse

317. En premier lieu, la Chambre Contentieuse renvoie à la définition du traitement des données à caractère personnel comme étant toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction[96].

318. Le TCF fournit une approche standardisée pour la collecte et l'échange de données à caractère personnel — c'est-à-dire le consentement, les éventuelles objections et les préférences — d'utilisateurs bien définis, déjà identifiés ou au moins identifiables, d'une manière supposée conforme au RGPD. Le fait que les organisations participantes puissent identifier directement les personnes concernées à l'aide de données supplémentaires, telles qu'une adresse IP, à partir de la TC String qui saisit ces consentements, objections et préférences, signifie non seulement que la TC String peut être considérée comme une donnée personnelle[97], mais conduit aussi à que les organisations participantes (*fournisseurs adtech*), inévitablement, *traitent* des données à caractère personnel.

319. Compte tenu du lien entre le TCF et le protocole OpenRTB, la Chambre Contentieuse se réfère aux lignes directrices de l'ancien Groupe de travail « Article 29 » sur la publicité en ligne, dans lesquelles le Groupe de travail a noté que les méthodes de publicité basées sur

[95] Conclusions des plaignants du 18 février 2021, para. 27.
[96] Art. 4.2) RGPD.
[97] Voir la section antérieure B.1.1. – Présence de données à caractère personnel dans le TCF.

le comportement de navigation impliquent intrinsèquement le traitement de données à caractère personnel, car une telle publicité implique la collecte d'adresses IP et le traitement d'identifiants uniques, de sorte que les personnes concernées peuvent être suivies en ligne même si leur nom réel n'est pas connu[98].

320. La Chambre Contentieuse comprend que le *Transparency and Consent Framework* implique intrinsèquement la collecte, le traitement, le stockage et le partage ultérieur des préférences des utilisateurs avec d'autres parties, en combinaison ou non avec des données à caractère personnel supplémentaires dans le contexte de l'OpenRTB.

321. Par conséquent, la Chambre Contentieuse constate qu'il y a bien un traitement de données à caractère personnel au sens de l'article 4.2 du RGPD. Cette conclusion est également confirmée par la prise en compte de la possibilité que la TC String puisse à tout moment être reliée à des informations immédiatement identifiables, fournies ou non par la personne concernée.

B.2 . - Responsabilité d'IAB Europe pour les opérations de traitement dans le *Transparency and Consent Framework*

322. IAB Europe déclare qu'elle n'est pas responsable de traitement ni coresponsable de traitement des données à caractère personnel collectées par les organisations participantes dans le cadre du TCF.

323. La Chambre Contentieuse estime cependant que ce raisonnement ne peut être suivi, et ce, pour plusieurs raisons. Tout d'abord, il convient d'appliquer l'interprétation large par la Cour de justice de la notion de responsable du traitement (*B.2.1. - Interprétation large de la notion de responsable du traitement par la Cour de justice et l'EDPB*). Le fait qu'IAB Europe ait une influence décisive sur l'objectif (*B.2.2. - Détermination des finalités du traitement des données à caractère personnel au sein du TCF*) et des moyens (*B.2.3. - Détermination des moyens du traitement des données à caractère personnel au sein du TCF*) du traitement en imposant des paramètres TCF obligatoires doit également être prise en compte.

B.2.1. - Interprétation large de la notion de responsable du traitement par la Cour de justice et l'EDPB

324. Le RGPD définit le « responsable de traitement » comme l'entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel[99]. Cette définition doit être comprise à la lumière de l'objectif du législateur de placer la responsabilité principale de la protection des données à caractère personnel sur

[98] WP171 - Avis 2/2010 sur la publicité comportementale en ligne, 22 juin 2010, p. 10, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_nl.pdf.
[99] Art. 4.7) RGPD.

l'entité qui exerce effectivement un contrôle sur le traitement des données. Cela signifie qu'il faut tenir compte non seulement de la qualification juridique, mais aussi de la réalité effective[100].

325. L'EDPB *a* précisé *que la* notion *de responsable du traitement fait référence à l'influence du* responsable du traitement *sur le traitement, basée sur un pouvoir décisionnel ou de contrôle à l'égard des* activités de traitement*. Ce contrôle peut être fondé sur des dispositions légales, sur un pouvoir implicite ou sur l'exercice d'une influence de fait*[101]*. En substance, la détermination des finalités et des moyens correspond à décider respectivement du « pourquoi » et du « comment » du traitement : pour un traitement donné, le responsable du traitement est l'acteur qui exerce une telle influence sur le traitement des données à caractère personnel, déterminant ainsi la raison pour laquelle le traitement a lieu (c'est-à-dire « à quelle fin » ; ou « dans quel but ») et la manière dont cet* objectif *sera atteint (i.e. quels moyens seront utilisés pour poursuivre l'objectif)*[102]*.*

326. *Le pouvoir de déterminer les moyens et les fins des activités de traitement peut* d'abord *être lié au rôle fonctionnel d'une organisation*[103]*. La* responsabilité *peut également être attribuée sur la base de dispositions contractuelles entre les* parties *concernées, bien que celles-ci ne soient pas toujours décisives*[104]*, ou sur la base d'une appréciation du contrôle effectif d'une partie. La détermination des moyens et des finalités peut par exemple résulter d'une influence déterminante sur le traitement, en particulier sur la raison pour laquelle le traitement est effectué d'une certaine manière*[105]*.*

327. Dans son arrêt « Témoins de Jéhovah »[106], la Cour de justice donne une interprétation large à la notion de responsable du traitement. Cet arrêt est pertinent et applicable en l'espèce, car il précise que la définition de responsable du traitement doit être interprétée de manière large, afin d'assurer « une protection effective et complète des personnes concernées »[107], et qu'il n'est pas nécessaire d'avoir accès aux données à caractère personnel concernées pour être qualifié de responsable du traitement[108]. La Chambre Contentieuse cite ci-dessous les considérants pertinents de l'arrêt précité :

---

[100] L. A. BYGRAVE & L. TOSONI, "Article 4(7). Controller" in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 148.

[101] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 20 et seq.

[102] *Ibidem*, para. 35.

[103] D. DE BOT, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 362.

[104] D. DE BOT, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 362-365.

[105] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 20 et seq.

[106] Arrêt de la CJUE du 10 juillet 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551.

[107] Arrêt de la CJUE du 13 mai 2014, *Google Spain SL c. Agencia Española de protección de Datos (AEPD) et autres*, C-131/12, ECLI : EU:C:2014:317, paragraphe 34 ; voir également la discussion sur la portée du concept dans C. DOCKSEY et H. HIJMANS, « The Court of Justice as a Key Player in Privacy and Data Protection », *European Data Protection Law Review*, 2019, numéro 3, (300)304.

[108] Arrêt de la CJUE du 10 juillet 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551. EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 45.

> "65. *Ainsi que le prévoit expressément l'article 2, sous d), de la directive 95/46, la notion de « responsable du traitement » vise la personne physique ou morale qui, « seule ou conjointement avec d'autres », détermine les finalités et les moyens du traitement de données à caractère personnel. Cette notion ne renvoie, dès lors, pas nécessairement à une personne physique ou morale unique et peut concerner plusieurs acteurs participant à ce traitement, chacun d'entre eux devant alors être soumis aux dispositions applicables en matière de protection des données (voir, en ce sens, arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, point 29).*
>
> *66. L'objectif de cette disposition étant d'assurer, par une définition large de la notion de « responsable », une protection efficace et complète des personnes concernées, l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce (voir, en ce sens, arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, points 28, 43 et 44).*
>
> *67. À cet égard, ni le libellé de l'article 2, sous d), de la directive 95/46 ni aucune autre disposition de cette directive ne permettent de considérer que la détermination des finalités et des moyens du traitement doit s'effectuer au moyen de lignes directrices écrites ou de consignes de la part du responsable du traitement.*
>
> *68. En revanche, une personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement de données à caractère personnel et participe de ce fait à la détermination des finalités et des moyens de ce traitement, peut être considérée comme étant responsable du traitement, au sens de l'article 2, sous d), de la directive 95/46.*
>
> *69. En outre, la responsabilité conjointe de plusieurs acteurs pour un même traitement, en vertu de cette disposition, ne présuppose pas que chacun d'eux ait accès aux données à caractère personnel concernées (voir, en ce sens, arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, point 38).* »

328. Il apparaît donc clairement à la Chambre Contentieuse que la défenderesse ne doit pas nécessairement traiter elle-même les données à caractère personnel concernées, ni être en mesure de s'accorder un quelconque accès à ces données, pour qu'IAB Europe puisse être considérée comme un responsable du traitement de données[109] à l'égard d'un système pour lequel la défenderesse facture par ailleurs une redevance annuelle de 1.200 euros aux organisations participantes[110].

[109] Arrêt de la CJUE du 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI : EU:C:2017:796, para. 35 ; arrêt de la CJUE du 10 juillet 2018, *Tietosuojavaltuutettu* et *Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 69.
[110] https://iabeurope.eu/join-the-tcf/

329. En outre, l'impact ou les conséquences de certaines activités sur les droits et libertés des personnes concernées peuvent également être pris en compte pour déterminer la responsabilité d'une organisation. S'il apparaît qu'une organisation joue un rôle décisif dans la diffusion des données à caractère personnel[111] ou que les opérations de traitement effectuées sous l'influence de cette organisation peuvent affecter de manière substantielle les droits fondamentaux à la vie privée et à la protection des données à caractère personnel[112], cette organisation doit être considérée comme un responsable du traitement des données.

330. *Dans ce cas,* la Chambre Contentieuse conclut que les organisations participantes, c'est-à-dire les publishers et les *fournisseurs adtech*, ne seraient pas en mesure d'atteindre les objectifs fixés par IAB Europe sans le TCF. Le système développé par IAB Europe joue donc un rôle décisif en ce qui concerne la collecte, le traitement et la diffusion des préférences, des consentements et des objections des utilisateurs, indépendamment du fait que la défenderesse elle-même entre en contact avec les données susmentionnées.

B.2.2. - Détermination des finalités du traitement des données à caractère personnel au sein du TCF

331. La détermination des finalités du traitement est la première condition pour identifier le responsable du traitement de données à caractère personnel[113]. En outre, on considère généralement que la définition des finalités du traitement l'emporte sur celle des moyens lorsqu'il s'agit d'établir la responsabilité d'une organisation[114]. Au demeurant, une désignation erronée par un responsable du traitement, telle qu'une désignation en tant que sous-traitant contredite par la situation de fait, ne lie pas la juridiction ou l'autorité de contrôle[115].

332. Le Service d'Inspection précise que le *Transparency and Consent Framework* en soi ne constitue pas un traitement de données à caractère personnel, mais qu'il s'agit d'un ensemble de *Policies* et de technical specifications élaborées par IAB Europe et IAB Tech Lab[116]. La Chambre Contentieuse se rallie au Service d'Inspection sur ce point.

---

[111] Arrêt de la CJUE du 13 mai 2014, *Google Spain SL c. Agencia Española de protección de Datos (AEPD) et autres*, C-131/12 ; ECLI : EU:C:2014:317, para. 36.

[112] Arrêt de la CJUE du 13 mai 2014, *Google Spain SL c. Agencia Española de protección de Datos (AEPD) et autres*, C-131/12 ; ECLI: EU:C:2014:317, para. 38.

[113] Art. 4.7) RGPD ; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant » in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

[114] EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 20; L. A. BYGRAVE & L. TOSONI, « Article 4(7). Controller » in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 150; B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019, para 109-110; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant » in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 12.

[115] C. de TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD » in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

[116] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 9.

333. Toutefois, la Chambre Contentieuse a également constaté que des données à caractère personnel sont traitées dans le cadre du TCF, plus particulièrement les préférences des utilisateurs, que les CMP enregistrent via une interface utilisateur et stockent à l'aide de la *TC String*. Afin de permettre une approche standardisée au sein du TCF, IAB Europe fait usage à la fois de documents de politique (*policies*) et de technical specifications :

- Les *TCF Policies* consistent en des règles de participation qui s'appliquent aux *publishers*, aux *consent management platforms* (CMP) et aux autres *fournisseurs adtech*.
- Les technical specifications du TCF, qui fournissent un protocole technique avec lequel les organisations participantes peuvent échanger immédiatement le statut des informations fournies aux utilisateurs et les choix des personnes concernées. Ces technical specifications sont étroitement liées à la politique TCF (*policies*) afin de fournir la fonctionnalité technique requise pour rendre opérationnelle la norme TCF.

334. La défenderesse indique dans ses conclusions que le traitement de ces préférences, conformément aux règles imposées par le TCF aux organisations participantes, poursuit l'objectif de permettre tant aux publishers de sites web et d'applications (*publishers*) qu'aux partenaires *ad tech* qui prennent en charge le ciblage, la diffusion et la mesure de la publicité et des contenus (*fournisseurs adtech*) d'obtenir le consentement d'utilisateurs, de divulguer de manière transparente les finalités de leur traitement et d'établir une base juridique valable pour le traitement des données à caractère personnel dans le but de fournir entre autres de la publicité numérique[117]. Cet objectif est également reflété dans les *TCF Policies*[118]:

> « *ii. L'objectif du cadre est d'aider les acteurs de l'écosystème en ligne à satisfaire à certaines exigences de la directive « vie privée et communications électroniques » (et, par extension, de son successeur, le futur règlement « vie privée et communications électroniques ») et du règlement général sur la protection des données, en fournissant un moyen d'informer les utilisateurs, entre autres, du stockage et/ou de l'accès aux informations sur leurs appareils, le fait que leurs données à caractère personnel sont traitées, les finalités pour lesquelles elles sont traitées, les entreprises qui cherchent à traiter leurs données à caractère personnel à ces fins, en donnant aux utilisateurs le choix à ce sujet, et en signalant aux tiers, entre autres, quelles informations ont été divulguées aux utilisateurs et quels sont leurs choix*. »

335. Il ressort également de la documentation établie par la défenderesse que les objectifs de la TC String sont déterminés par IAB Europe :

[117] Conclusions en réponse de la défenderesse, para. 33.

[118] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

« *L'objectif principal d'une TC String est d'encapsuler et de coder toutes les informations divulguées à un utilisateur et l'expression de ses préférences pour le traitement de ses données à caractère personnel en vertu du RGPD. À l'aide d'une plateforme de gestion des consentements (CMP), les informations sont capturées dans une chaîne codée et compacte transférable par HTTP. Cette chaîne permet de communiquer des informations de transparence et de consentement aux entités, ou «* vendors *», qui traitent les données à caractère personnel d'un utilisateur. Les* vendors *décodent une TC String pour déterminer s'ils disposent des bases légales nécessaires pour traiter les données personnelles d'un utilisateur à leurs fins.* » [119]

336. Bien que la Chambre Contentieuse souligne que la finalité du traitement de la TC String doive être distinguée des finalités du traitement qui a lieu en dehors du TCF, tel que le traitement et l'échange des données à caractère personnel contenues dans une *bid request* dans le cadre de l'OpenRTB, elle constate que le TCF est proposé *dans le but de promouvoir indirectement l'utilisation de l'OpenRTB*. Dans cette optique, IAB Europe, en sa qualité de *Managing Organization*, sert de véritable charnière entre le TCF et l'OpenRTB, qui, par ailleurs, a été développé par IAB Tech Lab.

337. À l'appui de sa position, la Chambre Contentieuse se réfère à l'inventaire des finalités envisageables, que les organisations participantes peuvent poursuivre dans le cadre du TCF. Par exemple, les *TCF Policies* pour les CMP, les *publishers* et les autres *fournisseurs* stipulent respectivement une liste obligatoire [120] avec des finalités fixes et prédéfinies[121], des finalités spéciales[122], des fonctionnalités[123] ainsi que des fonctionnalités spéciales définies par IAB Europe :

- Finalité 1 — Stocker et/ou accéder à des informations sur un appareil
- Finalité 2 — Sélectionner les publicités de base
- Finalité 3 — Créer un profil de publicités personnalisé
- Finalité 4 — Sélectionner des publicités personnalisées
- Finalité 5 — Créer un profil de contenu personnalisé
- Finalité 6 — Sélectionner du contenu personnalisé
- Finalité 7 — Mesurer la performance des publicités

[119] Traduction libre, Chaîne de transparence et de consentement avec les formats de liste de fournisseurs et de CMP mondiaux v2.0, août 2019 (pièce 35), p. 8.

[120] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), pp. 26 et suivantes.

[121] Le terme « Objectif » fait référence à l'un des objectifs définis pour le traitement des données, y compris les données à caractère personnel des utilisateurs, par les participants au Cadre, qui sont définis dans les TCF Policies ou les Spécifications.

[122] Le terme « Objectif spécial » désigne l'un des objectifs définis pour le traitement des données, y compris les données à caractère personnel des utilisateurs, par les participants au Cadre, qui sont définis dans les TCF Policies ou les Spécifications pour lesquels les Fournisseurs déclarent une base juridique dans le GVL et pour lesquels les fournisseurs ne disposent d'aucun choix donné par une CMP.

[123] « Caractéristique » désigne l'une des caractéristiques de traitement des données à caractère personnel utilisées par les participants au Cadre qui sont définies dans les TCF Policies ou les Spécifications utilisées dans la poursuite d'une ou plusieurs objectifs pour lesquelles l'utilisateur n'a pas le choix séparément du choix offert concernant les objectifs pour lesquels elles sont utilisées.

- Finalité 8 — Mesurer la performance du contenu
- Finalité 9 — Appliquer une étude de marché pour générer des informations sur l'audience
- Finalité 10 — Développer et améliorer les produits
- Finalité spéciale 1 — Assurer la sécurité, prévenir la fraude et déboguer
- Finalité spéciale 2 — Diffuser techniquement des publicités ou du contenu.
- Fonctionnalité 1 — Faire correspondre et combiner les sources de données hors ligne
- Fonctionnalité 2 — Relier différents appareils
- Fonctionnalité 3 — Recevoir et utiliser les caractéristiques du dispositif envoyées automatiquement pour l'identification
- Fonctionnalité spéciale 1 — Utiliser des données de géolocalisation précises
- Fonctionnalité spéciale 2 — Analyse active des caractéristiques du dispositif pour l'identification.

338. La Chambre Contentieuse en conclut que la finalité de la TC String, et au sens plus large du traitement de la TC String au sein du TCF tel que décrit dans les *TCF Policies*, a été établi par IAB Europe.

B.2.3. - Détermination des moyens du traitement des données à caractère personnel au sein du TCF

339. Déterminer les moyens du traitement est la deuxième pierre angulaire de la responsabilité de traitement. En ce qui concerne les moyens de traitement, l'EDPB fait une distinction entre les moyens « essentiels » et les moyens « non essentiels ». Le choix des moyens non essentiels peut, en principe, être laissé à un sous-traitant sans que la responsabilité de l'entité qui a déterminé les finalités ne soit réduite[124].

340. Les « moyens essentiels » sont étroitement liés à la finalité et à la portée du traitement et sont par nature réservés au responsable du traitement. Des exemples de moyens essentiels concernent le type de données à caractère personnel traitées (« quelles données sont traitées ? »), la durée du traitement (« combien de temps sont-elles traitées ? »), les catégories de destinataires (« qui y a accès ? ») et les catégories de personnes concernées (« quelles données à caractère personnel sont traitées ? »). Les « moyens non essentiels », quant à eux, concernent principalement les aspects pratiques de la mise en œuvre, tels que le choix d'un type particulier de matériel ou de logiciel ou les mesures de sécurité détaillées qui peuvent être laissées à l'appréciation du sous-traitant[125].

[124] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 39-41.
[125] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 40.

341. Il est établi par la Chambre Contentieuse, et également confirmé par la défenderesse[126], que le *Transparency and Consent Framework* constitue un cadre de règles contraignantes pour les organisations participantes quant au traitement des préférences des utilisateurs. Les participants au TCF sont censés accepter les conditions générales du *Transparency and Consent Framework d'IAB Europe* (ci-après dénommées « *conditions générales* ») [127] pour s'inscrire. Ce faisant, la Chambre Contentieuse constate qu'IAB Europe ne fait pas *que* contrôler le respect des spécifications et des *TCF Policies*, en tant que *Managing Organization*. La défenderesse définit en outre également les règles applicables au traitement des *TC Strings* dans le cadre du TCF, et elle impose ces règles aux organisations participantes.

342. Dans les paragraphes suivants, la Chambre Contentieuse examinera dans quelle mesure les moyens essentiels de traitement de la *TC String* sont effectivement déterminés par IAB Europe.

343. Génération, modification et lecture de la *TC String* — En premier lieu, les *TCF Technical Specifications*[128], les *IAB Europe Transparency and Consent Framework Implementation Guidelines* (ci-après « *TCF Implementation Guidelines* »)[129] ainsi que les *TCF Policies*[130] décrivent comment les CMP sont tenues de recueillir l'approbation des utilisateurs, doivent générer une *TC String* unique et peuvent stocker la valeur de la *TC String*.

344. De plus, les CMP sont obligées de s'enregistrer auprès d'IAB Europe pour pouvoir générer une *TC String*[131] et ils doivent se conformer aux technical specifications, développées par IAB Europe en coopération avec IAB Tech Lab, concernant l'API[132] avec laquelle les CMP peuvent générer la *TC String* et par le biais de laquelle les *fournisseurs adtech* et *publishers* sont en mesure de lire la *TC String*[133]. Ces spécifications attestent par ailleurs du fait que l'API des CMP joue un rôle essentiel dans le TCF, car elle fournit un moyen standardisé pour les parties, telles que *l'éditeur* ou un *ad tech vendor*, d'accéder aux préférences des utilisateurs, qui sont gérées par la CMP[134]. La Chambre Contentieuse note que l'utilisation de cette API est obligatoire pour communiquer entre les CMP et les *fournisseurs*.

---

[126] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 35.

[127] Conditions générales du cadre de transparence et de consentement d'IAB Europe (« Conditions générales ») (pièce 33)

[128] Chaîne de transparence et de consentement avec les formats de liste de fournisseurs et de CMP mondiaux v2.0, août 2019 (pièce 35).

[129] TCF Implementation Guidelines du cadre de transparence et de consentement d' IAB Europe, août 2019 (pièce 36).

[130] TCF Policies d'IAB Europe v2019-08-21.3 (Pièce 32) ; TCF Policies d'IAB Europe v2019-04-02.2c (Pièce 38).

[131] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 76.

[132] Une API est une interface de programmation qui permet à une entité permet de se « brancher » sur une application afin d'échanger des données. Une API est ouverte et offerte par le propriétaire du programme. Les API sont utilisées dans divers domaines du marketing numérique pour permettre, par exemple, des passerelles automatisées pour l'échange de données entre des programmes tels que Adwords, AdExchange et une agence ou un fournisseur. Elles peuvent également être utilisées par les fournisseurs adtech, les agences ou les fournisseurs de logiciels pour automatiser les campagnes publicitaires.

[133] Consent Management Platform API v2.0, août 2019 (pièce 34), p. 4.

[134] Consent Management Platform API v2.0, août 2019 (pièce 34), p. 6.

345. En ce qui concerne le contenu de la *TC String*, les *TCF Technical Specifications* précisent quelles informations sont incluses, y compris les métadonnées telles que l'heure exacte à laquelle la *TC String* a été générée ou modifiée.

346. À cet égard, la Chambre Contentieuse renvoie à l'arrêt « Wirtschaftsakademie », dans lequel la Cour de justice a jugé que l'entité chargée de définir, et *a fortiori* d'imposer, les paramètres d'un traitement de données, participe ainsi à la détermination des finalités et des moyens de ce traitement et doit donc être considérée comme le responsable du traitement[135].

347. Emplacement de stockage — Dans leurs preuves écrites, les plaignants font valoir qu'IAB Europe est responsable de la gestion du domaine Internet « *consensu.org* », auquel renvoient les cookies de consentement[136] dits « à portée globale » (« *globally scoped* ») et qui, en tant que tel, permet aux CMP de consulter et de modifier les TC Strings partagées entre plusieurs sites internet ou applications.

348. En revanche, IAB Europe indique dans ses conclusions que, bien qu'elle ait enregistré le domaine *consensu.org*, il n'y a pas de stockage de la TC String sur les serveurs d'IAB Europe auquel ce domaine *consensu.org* renvoie. En effet, IAB Europe délègue un sous-domaine de *consensu.org* à chaque CMP[137] inscrit, qui stocke la TC String sur l'appareil de l'utilisateur à l'aide d'un cookie *euconsent-v2* et l'associe au domaine *consensu.org*. Selon la défenderesse, c'est donc uniquement la CMP qui génère et stocke la TC String et les propres serveurs de la CMP qui ont accès à la TC String.

349. Afin d'établir la responsabilité d'IAB Europe dans le traitement des TC Strings, il est nécessaire de déterminer dans quelle mesure la délégation d'un sous-domaine à une CMP par IAB Europe implique que la défenderesse établisse à tout le moins les moyens (et les éventuelles finalités) de ce traitement.

350. Les technical specifications du TCF prévoient que le partage de la TC String avec les CMP doit se faire de deux manières : soit en stockant la TC String dans un système de stockage choisi par la CMP, s'il s'agit d'un consentement spécifique à un service[138], soit en stockant la TC String dans un cookie de consentement partagé à portée globale, associé au domaine Internet *consensu.org* d'IAB Europe[139].

---

[135] Arrêt de la CJUE du 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI : EU:C:2017:796, para. 39 : « Dans ces conditions, il y a lieu de juger que l'administrateur d'une page fan sur Facebook, telle que Wirtschaftsakademie, en définissant des paramètres en fonction, notamment, de son public cible et des objectifs de gestion ou de promotion de ses activités, participe à la détermination des finalités et des moyens du traitement des données à caractère personnel des visiteurs de sa page fan ».

[136] Qui contiennent les TC Strings.

[137] Elle concerne plus particulièrement le sous-domaine <*nom de la CMP*>.mgr.consensu.org. Par exemple, pour Onetrust, il s'agit de https://cookies.onetrust.mgr.consensu.org/.

[138] Concrètement, cela signifie que le consentement de l'utilisateur n'est valide que pour le site web visité, et pour les fins acceptées et les fournisseurs approuvés.

[139] Chaîne de transparence et de consentement avec les formats de liste de fournisseurs et de CMP mondiaux v2.0, août 2019 (pièce 35).

351. Sur la base des rapports techniques et des déclarations des parties à l'audience, la Chambre Contentieuse conclut que le consentement spécifique au service est établi au moyen d'un cookie first-party *euconsent-v2*, et qu'il est donc stocké exclusivement sur le dispositif de l'utilisateur. Dans ce premier scénario, le cookie *euconsent-v2* en question ne sera donc pas lié au domaine *consensu.org*, ni au sous-domaine délégué au CMP par IAB Europe.

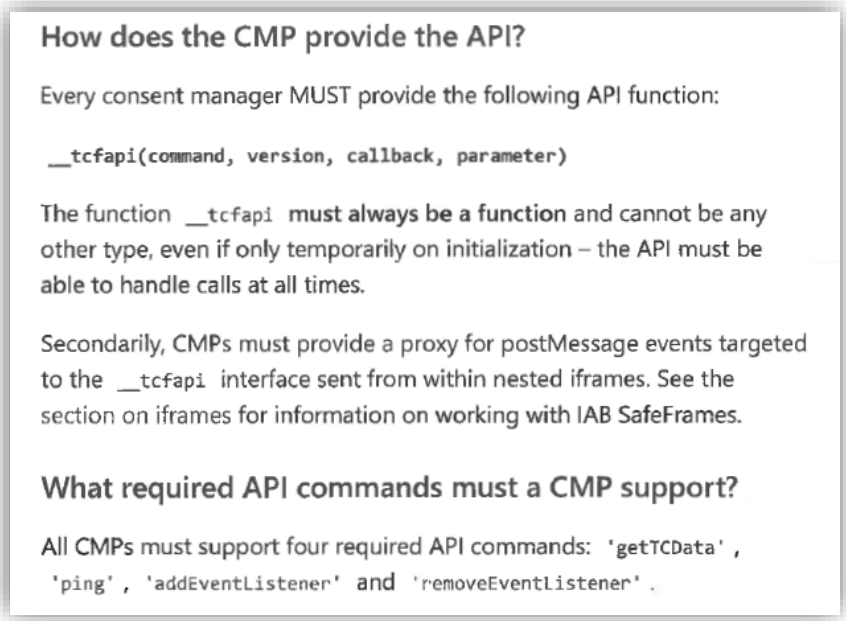
352. Toutefois, dans des cas exceptionnels où le consentement de l'utilisateur s'applique également à d'autres sites web, ce que l'on appelle les cookies de consentement à portée globale, les CMP sont tenus de stocker la TC String correspondante sur l'appareil de l'utilisateur au moyen d'un cookie *tiers*, associé au domaine *consensu.org*.[140] Seuls les CMP sont capables de lire les TC Strings sur les appareils d'utilisateurs.

353. Dans ce deuxième scénario, chaque CMP se voit alors attribuer un sous-domaine distinct, attribué par IAB Europe par délégation DNS, où le cookie de consentement et la TC String sont associés au domaine principal *consensu.org* et à ses sous-domaines. Concrètement, cela signifie que la portée du cookie de consentement à portée globale comprend à la fois le domaine *consensu.org* et les sous-domaines délégués aux CMP.

354. Selon la défenderesse, le consentement global n'a été appliqué que dans une mesure limitée et IAB Europe a cessé de l'utiliser et de le soutenir après l'audience. La Chambre Contentieuse en prend note, mais souligne que cette fonctionnalité démontre également que la responsabilité d'IAB Europe va au-delà de la simple conception d'un cadre.

355. La Chambre Contentieuse considère en outre que la défenderesse établit les moyens de traiter la TC String ainsi que le cookie *euconsent-v2*, tant pour les consentements spécifiques au service que pour les consentements à portée globale. Le fait que le TCF n'impose pas un mécanisme spécifique pour stocker le consentement des utilisateurs dans le navigateur mais recommande simplement aux CMP d'utiliser un cookie *first-party* n'empêche pas de constater que la défenderesse fournit une liste de mécanismes possibles pour relier la TC String à un utilisateur individuel, dont l'API des CMP est le plus courant. Plus précisément, la Chambre Contentieuse relève que, dans son document de politique intitulé « *Consent Management Platform API* », la défenderesse prescrit notamment la manière standardisée dont les différentes parties impliquées dans le TCF peuvent consulter les préférences, les objections et les consentements des utilisateurs[141] :

[140] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 79.
[141] Consent Management Platform API v2.0, août 2019 (pièce 34), p. 6.



How does the CMP provide the API?

Every consent manager MUST provide the following API function:

```
__tcfapi(command, version, callback, parameter)
```

The function `__tcfapi` **must always be a function** and cannot be any other type, even if only temporarily on initialization – the API must be able to handle calls at all times.

Secondarily, CMPs must provide a proxy for postMessage events targeted to the `__tcfapi` interface sent from within nested iframes. See the section on iframes for information on working with IAB SafeFrames.

What required API commands must a CMP support?

All CMPs must support four required API commands: `'getTCData'`, `'ping'`, `'addEventListener'` and `'removeEventListener'`.

356. Catégories de destinataires de la TC String — La Chambre Contentieuse juge également qu'IAB Europe détermine avec qui les préférences des utilisateurs doivent être partagées, notamment en mettant à disposition une liste de fournisseurs adtech inscrits au TCF, intitulée *Global Vendors List* (GVL)[142], ainsi qu'une liste de CMP agréés *(Global CMP List*)[143].

357. La documentation d'IAB Europe montre que les *publishers* qui souhaitent utiliser le TCF sont obligés de collaborer avec un CMP inscrit au TCF[144]. En outre, les *TCF Implementation Guidelines* énoncent que les CMP sont tenus de recueillir le consentement et les éventuelles objections pour toutes les finalités et les partenaires sélectionnés par l'éditeur, bien que cette sélection puisse être étendue à tous les *fournisseurs adtech* inclus dans la GVL[145].

358. Période de conservation de la TC String — Enfin, les deux versions des *TCF Policies* prévoient explicitement que les CMP et les *fournisseurs adtech* participants doivent conserver l'enregistrement du consentement ou de l'objection, qui est stocké dans la TC String, aussi longtemps que le traitement est en cours, et qu'ils sont tenus de le mettre à la disposition de la *Managing Organization*, c'est-à-dire la défenderesse, sur simple demande de celle-ci[146]:

> « *8. Record Keeping*

[142] https://iabeurope.eu/vendor-list/ et https://iabeurope.eu/vendor-list-tcf-v2-0/

[143] https://iabeurope.eu/cmp-list/

[144] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), pp. 26 et suivantes.

[145] TCF Implementation Guidelines du cadre de transparence et de consentement d'IAB Europe, août 2019 (pièce 36), p.13.

[146] IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Annexe 32); IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Annexe 32). Articles 8 et15.

1. A CMP will maintain records of consent, as required under the Policies and/or the Specifications, and will provide the MO access to such records upon request without undue delay.

2. A CMP will retain a record of the UI that has been deployed on any given Publisher at any given time and make this record available to its Publisher client, Vendors, and/or the MO upon request.

[…]

15. Record Keeping

1. A Vendor must maintain records of consent, as required under the Policies and the Specifications, and will provide the MO access to such records upon request without undue delay.

2. A Vendor must maintain records of user identification, timestamps, and received Signals for the full duration of the relevant processing. A Vendor may maintain such records of user identification, timestamps, and Signals beyond the duration of the processing as required to comply with legal obligations or to reasonably defend or pursue legal claims, and/or for other processing allowed by law, under a valid legal basis, and consistent with the purposes for which the data was collected. »

359. La Chambre Contentieuse estime donc qu'IAB Europe porte la responsabilité de définir les critères permettant de déterminer les périodes de conservation des TC Strings.

360. Il résulte de ce qui précède que, outre les finalités, c'est IAB Europe qui détermine en réalité les moyens de générer, de stocker et de partager la TC String par laquelle les préférences, les objections et le consentement des utilisateurs sont traités. Les éléments suivants sont déterminants selon la Chambre Contentieuse :

i. IAB Europe définit comment les CMP peuvent recueillir le consentement ou les objections des utilisateurs, générer une TC String unique et stocker la valeur de la TC String ;

ii. IAB Europe, en collaboration avec IAB Tech Lab[147] a développé les technical specifications de l'API avec laquelle les *fournisseurs adtech*, entre autres, peuvent accéder d'une manière standardisée aux préférences des utilisateurs, gérées par la CMP;

iii. IAB Europe détermine l'emplacement et la méthode de stockage des cookies de consentement, qu'ils soient spécifiques à un service ou de portée globale ;

iv. IAB Europe gère les listes des CMP et des *fournisseurs adtech* enregistrés et détermine donc à quels destinataires les données relatives à la TC String sont potentiellement communiquées ;

[147] IAB Europe a travaillé avec IAB Tech Lab pour déterminer les politiques des règles du cadre. IAB Europe a également confié à Tech Lab le développement ainsi que l'hébergement des implémentations techniques et des spécifications du TCF, en raison de leur expertise technologique.

v. IAB Europe détermine les critères selon lesquels les durées de conservation des TC Strings peuvent être établies, ainsi que la manière dont les organisations participant au TCF doivent mettre ces TC Strings à la disposition de *la Managing Organization*, c'est-à-dire la défenderesse.

361. Sur la base des explications précédentes, la Chambre Contentieuse estime que **la défenderesse doit être considérée comme responsable du traitement des données à caractère personnel quant à l'enregistrement du signal de consentement, des objections et des préférences des utilisateurs au moyen de la TC String, conformément aux TCF Policies et aux technical specifications du *Transparency and Consent Framework***.

B.3. - Responsabilité conjointe des publishers, des CMP et des fournisseurs adtech en ce qui concerne les moyens et les finalités du traitement des données à caractère personnel dans le contexte du TCF et de l'OpenRTB

362. La responsabilité d'IAB Europe n'exclut pas qu'il existe d'autres responsables du traitement des données mettant en œuvre le TCF et s'appuyant sur le protocole OpenRTB, endossant leur responsabilité propre ou une responsabilité partagée pour les opérations de traitement des données à caractère personnel qu'ils effectuent.

B.3.1. - Responsabilité conjointe de traitement

363. L'article 26.1 du RGPD dispose qu'il existe une responsabilité conjointe lorsque « deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement ». La Cour de justice de l'UE a précisé que « l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce »[148].

364. Là encore, l'EDPB a expliqué que l'appréciation de la responsabilité conjointe du traitement devait être fondée sur une analyse factuelle plutôt que formelle de l'impact concret sur les finalités et les moyens du traitement[149].

365. Tout d'abord, la Chambre Contentieuse souligne que l'existence de décisions *identiques* n'est pas nécessaire pour que l'on parle de responsabilité conjointe de traitement ; il suffit que les finalités définies soient complémentaires les unes des autres[150]. L'EDPB souligne

[148] CJUE Arrêt de 10 juillet 2018, *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 66 et CJUE Arrêt dy 29 Juillet 2019, *Fashion ID GmbH & Co. KG*, C-40/17, ECLI:EU:C:2019:629, para. 70.

[149] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 52.

[150] Conclusions de l'avocat général Bobek dans l'affaire *Fashion ID*, C-40/17, ECLI : EU:C:2018:1039, para. 105 : « Nonobstant le fait que les utilisations précises des données à des fins commerciales ne soient pas nécessairement les mêmes, tant la

également que la participation conjointe à la définition des moyens et des finalités peut prendre la forme d'une décision commune, mais aussi résulter de décisions différentes mais *convergentes* de deux ou plusieurs entités concernant les finalités et les moyens essentiels d'un traitement de données[151].

366. **Des décisions peuvent être considérées comme convergentes si elles sont complémentaires et nécessaires au traitement d'une manière qui confère une influence tangible sur la détermination des finalités et des moyens du traitement.** La question à se poser est de savoir si le traitement *envisagé* de données à caractère personnel serait impossible sans la participation de toutes les parties, ou plus précisément, si les activités de traitement effectuées par chaque partie sont indissociables et indivisibles.

367. Tant dans ses conclusions que lors de l'audition, IAB Europe a souligné que le TCF et le protocole OpenRTB sont complètement indépendants l'un de l'autre, en ce sens que même sans participation au TCF, les fournisseurs adtech peuvent traiter librement les données à caractère personnel dans le contexte de l'OpenRTB. D'autre part, les plaignants ont toujours fait référence à l'interconnexion inhérente entre l'OpenRTB et le TCF, que la défenderesse elle-même confirmerait — d'après les plaignants — dans les *TCF Implementation Guidelines*[152].

368. La Chambre Contentieuse constate que l'argument de la défenderesse ne peut être suivi, étant donné que la défenderesse indique à plusieurs reprises dans ses conclusions que la raison d'être du TCF est précisément de mettre les traitements de données à caractère personnel fondés sur le protocole OpenRTB, entre autres, en conformité avec la réglementation applicable, en ce compris le RGPD et la directive ePrivacy. Bien que la Chambre Contentieuse comprenne que le TCF puisse également être utilisé par les *publishers* pour d'autres applications[153], en collaboration ou non avec les CMP, il est également certain que le TCF n'a jamais été conçu pour être un écosystème autonome et indépendant.

369. Au contraire, la Chambre Contentieuse note que le *Transparency and Consent Framework* comprend des TCF Policies et des technical specifications qui devraient permettre aux publishers de sites web et d'applications (*publishers*) ainsi qu'aux partenaires adtech qui prennent en charge le ciblage, la diffusion et la mesure de la publicité et du contenu (*fournisseurs adtech*), de divulguer de manière transparente leurs finalités de traitement, d'établir une base juridique pour le traitement des données à caractère personnel pour la

---

défenderesse au principal que Facebook Ireland paraissent globalement poursuivre la même finalité d'une manière qui semble mutuellement assez complémentaire. À défaut d'identité, il y a donc une unité de la finalité : il y a une finalité commerciale et publicitaire. »

[151] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 54.

[152] https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md#how-does-the-tc-string-apply-to-non-openrtb-situations.

[153] Le TCF peut ainsi être également utilisé à des fins non liées au marketing, par exemple pour mesurer l'audience, les performances, etc.

fourniture de publicité numérique, et d'obtenir le consentement ou d'identifier les objections des utilisateurs[154].

370. **Partant, la Chambre Contentieuse constate que les décisions traduites par IAB Europe dans les dispositions des TCF Policies et des technical specifications du TCF, d'une part, et les moyens et les finalités déterminés par les organisations participantes concernant les traitements — dans le cadre ou non de l'OpenRTB — de données à caractère personnel des utilisateurs, d'autre part, doivent être considérées comme des décisions convergentes[155]. IAB Europe fournit un écosystème au sein duquel le consentement, les objections et les préférences des utilisateurs sont collectés et échangés non pas à des fins propres ou d'auto-préservation, mais pour faciliter le traitement ultérieur par des tiers (à savoir : les *publishers* et les *fournisseurs adtech*)**.

371. En conséquence, la Chambre Contentieuse juge qu'IAB Europe et les organisations participantes respectives doivent être considérées comme des responsables de traitement conjoints en ce qui concerne la collecte et la diffusion ultérieure du consentement, des objections et des préférences des utilisateurs, ainsi que pour le traitement connexe de leurs données à caractère personnel, sans que la responsabilité des CMP et des *fournisseurs adtech* participants ne réduise pour autant celle d'IAB Europe.

a. Plateformes de gestion des consentements (CMP)

372. Les CMP assurent la mise en œuvre technique des bannières de consentement par lesquelles les personnes concernées indiquent leurs choix concernant le traitement de leurs données à caractère personnel.

373. Plus précisément, les CMP ont pour fonction de stocker le consentement, les objections et les préférences des utilisateurs dans la TC String, puis de stocker cette valeur sous la forme d'un cookie *euconsent-v2* dans les navigateurs utilisés pour visiter le site web, et enfin de fournir une API aux *fournisseurs adtech* afin qu'ils puissent accéder aux valeurs de consentement, d'objection et de préférence pour chaque utilisateur individuel[156].

374. Les CMP qui souhaitent s'inscrire au TCF v2.0 d'IAB Europe sont tenus de mettre en place les finalités et fonctionnalités de traitement standardisées dans leur interface utilisateur, afin de recueillir et de stocker les préférences de la personne concernée à cet égard[157]. Ils doivent également respecter les principes légaux applicables, tels qu'ils sont définis dans le TCF v2.0 d'IAB Europe.

375. La Chambre Contentieuse a déjà établi que la TC String en elle-même ne permet pas d'identifier directement des personnes ou des dispositifs. Toutefois, dès lors que la TC

[154] Conclusions en réplique de la défenderesse du 25 mars 2021, para. 33.
[155] Voir para. 365-366.
[156] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, « Consent Management Platforms Under the GDPR: Processors and/or Controllers? », in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51.
[157] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 9 et suivantes.

String est placée sur le dispositif de l'utilisateur, un CMP peut attribuer un identifiant unique à cette TC String, *c'est-à-dire* l'adresse IP du dispositif sur lequel elle est placée sous la forme d'un cookie *euconsent-v2*.[158].

376. Pour fournir une interface CMP aux utilisateurs, les *publishers* doivent implémenter le code JavaScript CMP sur leur site web. Ce code est ensuite chargé directement depuis le serveur CMP ou via le sous-domaine délégué. Suite à cette requête HTTP(S), le serveur de l'éditeur et le serveur de la CMP ont accès à l'adresse IP de l'utilisateur qui visite le site web et voit l'interface de la CMP[159].

377. L'accès à cette adresse IP permet aux CMP d'enrichir le consentement, l'objection et les préférences contenus dans la TC String avec d'autres informations déjà en leur possession ou en possession de l'éditeur et liées à cette même adresse IP. Sur cette base, la Chambre Contentieuse conclut que les CMP sont en mesure de traiter un grand nombre de données à caractère personnel.

378. La Chambre Contentieuse évalue la mesure dans laquelle les CMP agissent en tant que sous-traitants ou en tant que responsables du traitement (conjoints) dans les paragraphes suivants.

379. Selon la défenderesse, et comme le prévoient ses TCF Policies, les CMP sont en principe considérées comme des sous-traitants[160]. La Chambre Contentieuse ne partage pas ce point de vue pour les raisons suivantes. La tâche principale des CMP est de développer et de fournir des interfaces qui peuvent avoir un impact direct sur le choix des personnes concernées. Les CMP jouent donc un rôle clé, non seulement dans le contexte du TCF, mais aussi en ce qui concerne le traitement des données à caractère personnel dans le cadre de l'OpenRTB. Elles sont donc tenues de respecter les principes de protection des données énoncés à l'article 5.1 du RGPD (licéité, loyauté et transparence du traitement des données à caractère personnel).

380. Bien que les *TCF Policies* interdisent aux CMP d'accorder une préférence à certains *fournisseurs adtech* de la *Global Vendors List*, et qu'ils sont donc en principe tenus de présenter aux utilisateurs tous les fournisseurs inscrits au TCF, sauf instruction contraire des *publishers*[161], quelques auteurs notent qu'un certain nombre de CMP ne respectent pas cette exigence. Soit parce que les CMP imposent aux *publishers* des fournisseurs présélectionnés, soit parce qu'elles leur refusent la possibilité de déroger à la liste complète des *fournisseurs adtech*, proposée par défaut[162].

---

[158] Voir les para. 302 et suivants de la présente décision. Voir également C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, « Consent Management Platforms Under the GDPR: Processors and/or Controllers? », in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 50.

[159] *Ibidem*, p. 5.

[160] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 9 et suivantes.

[161] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 9, § 8 et p. 10, § 11.

[162] C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, « Consent Management Platforms Under the GDPR: Processors and/or Controllers? », in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51.

381. Il convient également de noter que les CMP ont une grande marge d'appréciation en ce qui concerne l'interface qu'elles offrent aux utilisateurs. En effet, les *TCF Policies* n'imposent que des exigences d'interface minimales aux CMP participantes[163], avec pour conséquence qu'en pratique, les interfaces et le respect des principes d'équité et de transparence peuvent varier considérablement selon la CMP avec laquelle les *publishers* de sites web et d'applications collaborent[164].

382. Les constatations qui précèdent amènent la Chambre Contentieuse à conclure que les CMP jouent un rôle important et portent donc une responsabilité[165] (conjointe) en ce qui concerne les finalités et les moyens du traitement des données à caractère personnel des utilisateurs dans le cadre du TCF et du protocole OpenRTB.

383. La Chambre Contentieuse observe cependant que cette conclusion ne signifie pas pour autant que toutes les CMP doivent systématiquement être considérées comme des responsables du traitement conjointement avec IAB Europe et les *publishers*, ou que le champ d'application de cette responsabilité conjointe est sans limites. Comme expliqué plus haut dans cette décision[166], la liste des CMP mettant en œuvre le TCF est limitative[167] en raison de la procédure d'enregistrement et d'approbation obligatoire auprès d'IAB Europe, en tant que *Managing Organization*. La Chambre Contentieuse constate que la responsabilité conjointe du contrôle est établie en ce qui concerne, respectivement :

    a. l'éditeur du site ou de l'application,

    b. la CMP spécifique mise en place par l'éditeur et fournissant l'interface TCF aux utilisateurs,

    c. IAB Europe, en tant que *Managing Organization*.

    À cet égard, la Chambre Contentieuse souligne que des accords appropriés doivent être mis en place entre les différents responsables du traitement conjoints, conformément aux exigences prévues par l'article 26 du RGPD.

384. Les CMP sont en principe tenues, en vertu des *TCF Policies* — élaborées et administrées par la défenderesse — de présenter par défaut dans leur interface *l'ensemble* des *fournisseurs adtech* inscrits au TCF. Dans la mesure où les CMP mettent en œuvre les *TCF Policies*, la Chambre Contentieuse constate que la défenderesse est responsable des moyens essentiels du traitement, puisque IAB Europe détermine les destinataires des données à caractère personnel collectées, et est donc conjointement responsable de la

[163] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 61 et suivantes.
[164] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 99-103.
[165] Voir para. 360 de la présente décision sur la responsabilité de traitement d'IAB Europe pour la détermination des destinataires.
[166] Voir para. 102 ; 341 ; 344 ; 356-360 ; et 374 de la présente decision.
[167] En novembre 2021, la liste des CMP enregistrées comprend 76 entrées : https://iabeurope.eu/cmp-list/.

transmission des données à caractère personnel, en ce compris certaines données contenues dans la *bid request*.

385. Si, en revanche, les CMP s'écartent des *TCF Policies*, la Chambre Contentieuse considère que, cette fois, les CMP agissent elles-mêmes en tant que responsables du traitement des données à l'égard des destinataires des données à caractère personnel. Dans la mesure où les CMP ne respectent pas les instructions qui leur sont imposées, elles en sont elles-mêmes pleinement responsables[168], conformément à l'article 28.10 RGPD.

386. Enfin, lorsque les CMP déterminent la liste des destinataires conformément aux instructions des *publishers*, la Chambre Contentieuse constate que les *publishers* portent la responsabilité principale du transfert des données à caractère personnel aux fournisseurs, sans préjudice de la responsabilité d'IAB Europe, sans laquelle la liste globale des fournisseurs adtech participants n'existerait pas en premier lieu.

b. *Publishers*

387. Les *publishers* agissent généralement en tant que responsables du traitement dans le contexte du TCF, car ils sont censés décider de coopérer ou non avec une CMP enregistrée, et sont également en mesure de déterminer quels fournisseurs sont autorisés à fournir de la publicité sur leur site web ou dans leur application. En outre, les publishers peuvent exercer un contrôle sur la base juridique pour une finalité de traitement spécifique, et ils peuvent exclure certaines finalités de traitement[169].

388. Les *bid requests* sont envoyées par les *plateformes côté offre* (*supply-side platforms*, ou SSP), en leur qualité de représentants des publishers, aux plateformes *côté demande* (*demand-side platforms*, ou DSP), qui représentent les fournisseurs adtech. Le format et le contenu (ou « attributs ») de ces *bid requests* sont déterminés conformément aux technical specifications du protocole OpenRTB, indépendamment du TCF.

389. Comme le confirment les rapports du Service d'Inspection, IAB Europe ne participe pas à la détermination des attributs d'une *bid request* spécifique. Ce sont principalement les publishers de sites web et d'applications qui décident des attributs à inclure dans une *bid request* et à transmettre aux fournisseurs adtech.

390. Une *bid request* contient au moins un identifiant unique pour chaque *bid request* (*Bid ID*) et un identifiant unique pour l'espace publicitaire mis aux enchères (*Item ID*). En outre, une *bid request* contient généralement des informations sur l'appareil de l'utilisateur, les détails de l'utilisateur, le site web ou l'application, et des détails techniques sur l'espace publicitaire (*Impression*)[170].

[168] EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 150.
[169] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), pp. 21-22.
[170] Rapport d'analyse technique du Service d'Inspection, 4 juin 2019 (pièce 24), p. 12-13.

391. Sur la base de ce qui précède, la Chambre Contentieuse constate que la *bid request* contient le plus de données à caractère personnel, et que ces données ne sont pas traitées par la défenderesse, mais principalement par les *publishers*, les CMP et les différents *fournisseurs adtech* qui sont en principe tous tenus de respecter les valeurs de la TC String, conformément aux TCF Policies.

392. Dans la mesure où un *éditeur* s'appuie sur une CMP qui a mis en œuvre le TCF, la *bid request* contiendra également une TC String indiquant les préférences du visiteur du site web ou de l'utilisateur de l'application. La Chambre Contentieuse est d'avis que ceci peut être considéré non seulement comme une preuve additionnelle que la TC String est bien une donnée à caractère personnel, puisqu'il s'agit d'informations relatives à une personne physique *identifiable*[171], mais aussi comme une preuve que les préférences stockées dans la TC String ont un impact direct et significatif sur les activités de traitement ultérieures.

393. Par conséquent, lorsque un utilisateur donne sciemment ou non son consentement par le biais d'un bouton « *accepter tout* » dans une interface CMP, et que l'éditeur du site web et la CMP n'ont pas dérogé à la liste complète des fournisseurs adtech participants, cela signifie que les données à caractère personnel de la personne concernée seront partagées avec des centaines de parties tierces.

394. Dans la logique de ses conclusions précédentes concernant les CMP[172], la Chambre Contentieuse estime que les *publishers* agissent également en tant que responsables du traitement des préférences des utilisateurs dans une TC String ainsi que de leurs données à caractère personnel traitées dans une *bid request*.

395. En outre, la Chambre Contentieuse se réfère à l'article 23.5 des *TCF Policies*, qui interdit aux *publishers* de modifier les finalités du traitement, ou de donner aux CMP toute instruction à cet effet[173].

396. Par conséquent, dans la mesure où les *publishers* décident de ne pas s'écarter de la liste de *fournisseurs adtech* proposée par défaut et acceptent toutes les finalités de traitement proposées, la Chambre Contentieuse considère également qu'IAB Europe agit en tant que responsable conjoint du traitement des données avec les *publishers* en ce qui concerne les destinataires de la TC String ainsi que les finalités de traitement pour lesquelles les données à caractère personnel des utilisateurs seront traitées.

c. Fournisseurs adtech

397. La Chambre Contentieuse a déjà constaté qu'IAB Europe porte la responsabilité de la définition des différentes finalités de traitement dans le cadre du TCF[174].

[171] Voir les para. 291 et suivants de la présente décision.
[172] Voir para. 382 et s. de la présente décision.
[173] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), pp. 22-23.
[174] Voir para. 331 *et s.* de la présente décision.

398. Lorsqu'ils s'inscrivent au TCF v2.0, les fournisseurs adtech doivent également choisir les finalités de traitement envisagées et les bases juridiques possibles, au départ d'une liste fixe et prédéterminée de finalités.

399. En ce sens, la Chambre Contentieuse constate que les fournisseurs adtech ainsi que la défenderesse sont conjointement responsables des traitements qui ont lieu dans le contexte de l'OpenRTB, pour les finalités de traitement et conformément aux préférences, objections et consentements recueillis dans le cadre du TCF. Ce dernier aspect n'affecte toutefois pas le rôle que jouent les fournisseurs adtech lorsqu'ils précisent eux-mêmes les finalités pour lesquelles ils envisagent de traiter les données à caractère personnel contenues dans une *bid request*, ou à l'égard d'un traitement ultérieur des données non prévu par le TCF[175].

400. En outre, la Chambre Contentieuse précise que, comme pour les CMP, les fournisseurs adtech sont également tenus de s'inscrire au TCF afin d'en bénéficier. Cela signifie que la responsabilité conjointe du contrôle est limitée aux fournisseurs adtech inscrits[176].

d. Evaluation par la Chambre Contentieuse

401. Cette analyse factuelle du rôle des CMP, des publishers et des fournisseurs adtech montre que les décisions relatives à la détermination des finalités et des moyens des activités de traitement effectuées par la défenderesse dans le cadre du TCF (visant à mettre les activités de traitement effectuées par les organisations participantes précitées en conformité avec le RGPD et la directive ePrivacy) complètent les décisions relatives aux finalités et aux moyens des activités de traitement effectuées par les organisations participantes dans le cadre de l'OpenRTB et doivent par conséquent être considérées comme des décisions convergentes.

402. **Cela amène la Chambre Contentieuse à conclure que la défenderesse ainsi que les CMP, les publishers et les fournisseurs adtech participants doivent être considérés comme des responsables conjoints du traitement pour ce qui concerne la collecte et la diffusion des préférences, des objections et du consentement des utilisateurs, ainsi que pour le traitement ultérieur de leurs données à caractère personnel**.

B.4. Sur les violations alléguées du Règlement général sur la protection des données

B.4.1 - Licéité et loyauté du traitement (art. 5.1.a et 6 du RGPD)

403. En ce qui concerne la licéité et la loyauté du traitement, la Chambre Contentieuse distingue deux activités de traitement : d'une part, la saisie proprement dite du signal de

[175] WP171 - Avis 2.2010 sur la publicité comportementale en ligne, pp. 10-11.
[176] https://iabeurope.eu/vendor-list-tcf-v2-0/.

consentement, des objections et des préférences des utilisateurs dans la TC String par les CMP (a), et, d'autre part, la collecte et la diffusion des données à caractère personnel des utilisateurs par les organisations participantes (b).

a. Enregistrement du signal de consentement, des objections et des préférences des utilisateurs au moyen de la TC String.

404. La Chambre Contentieuse constate que les utilisateurs ne sont informés nulle part de la base juridique du traitement, par les CMP, de leurs préférences personnelles et individuelles concernant les finalités et les fournisseurs adtech autorisés.

405. Le raisonnement sous-jacent de la défenderesse à cet égard est que la TC String n'est pas une donnée à caractère personnel et que, par conséquent, aucune base juridique n'est exigée pour son traitement.

406. Comme déjà établi, la Chambre Contentieuse ne partage pas la position de la défenderesse[177]. La Chambre Contentieuse a établi que la génération et la diffusion de la TC String impliquent effectivement le traitement de données à caractère personnel.[178] Par conséquent, ce traitement doit en tout état de cause être fondé sur l'une des bases juridiques de traitement limitativement énumérés à l'article 6 du RGPD. Pour cette raison, la Chambre Contentieuse examinera la question de savoir si l'une des bases juridiques de l'article 6 RGPD peut être appliquée.

407. Tout d'abord, la Chambre Contentieuse constate que ni les *TCF Policies* ni les *TCF Implementation Guidelines* ne mentionnent une obligation pour les CMP d'obtenir le consentement sans équivoque des utilisateurs, avant d'enregistrer leurs préférences dans une TC String, qui est placée sur les appareils des utilisateurs au moyen d'un cookie *euconsent-v2*. En outre, les utilisateurs ne sont jamais informés du traitement de leurs préférences sous la forme d'une TC String, ni des parties avec lesquelles leurs préférences sont partagées, ni de la durée de conservation de leurs préférences. Le consentement des visiteurs n'étant jamais demandé, l'article 6.1.a ne s'applique *de facto* pas comme base juridique pour ce traitement.

408. De même, la Chambre Contentieuse souligne que l'article 6.1.*b* n'est *à première vue* pas applicable au traitement des préférences des utilisateurs et de la TC String. Dans la majorité des cas, même en l'existence d'une relation contractuelle entre les utilisateurs et les publishers, les traitements de données concernés par le TCF ne répondraient pas à l'exigence de nécessité objective pour la fourniture de services en ligne par les publishers

[177] Voir *supra* B.1.1. – Présence de données à caractère personnel dans le TCF ».
[178] Voir *supra* B.1.2. - Traitement de données à caractère personnel dans le TCF.

aux utilisateurs concernés (notamment en ce qui concerne les traitements à des fins de personnalisation des contenus et de publicité basée sur le comportement de navigation)[179].

409. En l'absence de toute relation contractuelle entre les personnes concernées et les CMP ou IAB Europe, et à défaut d'un consentement sans ambiguïté donné par les utilisateurs pour le placement d'un cookie *euconsent-v2*, la Chambre Contentieuse se doit d'examiner si l'intérêt légitime passe le triple test de la CJUE et, si tel est le cas, s'il pourrait servir de base juridique (6.1.*f* RGPD) pour ce traitement préliminaire des préférences des utilisateurs par les CMP, conformément aux moyens et aux objectifs tels que définis par IAB Europe dans ses *TCF Policies* et ses *TCF Implementation Guidelines*.

410. Afin de pouvoir invoquer l'article 6.1.f RGPD comme base juridique du traitement des données à caractère personnel, l'intérêt légitime du responsable du traitement (ou de tiers), étroitement lié au concept de finalité du traitement (même s'il en demeure distinct), doit être mis en balance avec les intérêts ou les droits et libertés fondamentaux des personnes concernées. Alors que la « finalité » fait référence à la raison spécifique pour laquelle les données sont traitées — en d'autres termes, le but ou l'intention du traitement des données —, la notion d'« intérêt » est liée à l'intérêt plus large qu'un responsable du traitement peut avoir dans le traitement, ou au bénéfice que le responsable du traitement — voire un tiers, qui ne doit pas nécessairement être qualifié de responsable conjoint à l'égard du traitement des données — pourrait retirer du traitement[180].

411. En application de l'article 6.1.*f* du RGPD et de la jurisprudence de la Cour de justice, trois conditions cumulatives doivent être réunies pour qu'un responsable du traitement puisse valablement se prévaloir de cette base juridique, « *à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas* » (arrêt Rigas[181]).

412. Afin de pouvoir invoquer le motif de licéité de « l'intérêt légitime » en vertu de l'article 6.1.*f* du RGPD, le responsable du traitement doit démontrer, en d'autres termes, que :

    1) les intérêts qu'il poursuit avec le traitement peuvent être reconnus comme légitimes (critère de « finalité ») ;

---

[179] EDPB - Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, v2.0, 8 octobre 2019, para. 23 *et s.*, para. 52 *et s.* et para. 57 *et s.*, https://edpb.europa.eu. Cette situation est différente de l'affaire pendante devant la Cour de justice C-446/21, Maximilian Schrems vs. Facebook Ireland Ltd.

[180] Arrêt de la CJUE du 11 décembre 2019, *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.

[181] Arrêt de la CJUE du 4 mai 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA « Rīgas satiksme »*, C-13/16; ECLI: EU:C:2017:336, para. 28-31. Voir également Arrêt de la CJUE du 11 décembre 2019, *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 40.

2) le traitement envisagé est nécessaire à la réalisation de ces intérêts (critère de « nécessité ») ; et

3) la mise en balance de ces intérêts avec les intérêts, libertés et droits fondamentaux des personnes concernées penche en faveur du responsable du traitement ou d'un tiers (critère de « mise en balance »).

413. Pour ce qui est de la première condition, la Chambre Contentieuse considère que l'enregistrement du consentement et des préférences des utilisateurs afin de s'assurer et de pouvoir démontrer que ceux-ci ont valablement consenti ou ne se sont opposés au traitement de leurs données à caractère personnel à des fins publicitaires, peut être considéré comme étant réalisé dans un intérêt *légitime*.

414. L'intérêt poursuivi par la défenderesse en tant que responsable du traitement des données peut, conformément au considérant 47 du RGPD, être considéré comme légitime en soi. Plus particulièrement, la possibilité de stocker les préférences des utilisateurs[182] est un élément essentiel du TCF et la Chambre Contentieuse note que cela se fait dans l'intérêt légitime de la défenderesse ainsi que des tiers concernés, tels que les *fournisseurs adtech* participants.

415. Dès lors, la première condition énoncée à l'article 6.1.*f* du RGPD est remplie.

416. Pour remplir la deuxième condition, il convient ensuite de démontrer que le traitement est *nécessaire* à la réalisation des finalités poursuivies. Cela signifie notamment qu'il faut se demander si le même résultat peut être obtenu par d'autres moyens, sans traitement de données à caractère personnel ou sans traitement inutilement contraignant pour les personnes concernées.

417. Compte tenu de l'objectif de permettre à la fois aux publishers de sites web ou d'applications et aux *fournisseurs adtech* participants de communiquer les finalités de leur traitement de manière transparente, d'établir une base juridique valide pour le traitement des données à caractère personnel afin de fournir de la publicité numérique, et de recueillir le consentement — ou d'identifier si une objection a, le cas échéant, été formulée quant au traitement des données fondé sur leur intérêt légitime[183] —, la Chambre Contentieuse se doit de vérifier si les données à caractère personnel comprises dans la TC String sont limitées à ce qui est strictement nécessaire pour enregistrer le consentement, les objections et les préférences d'un utilisateur spécifique.

418. Cette deuxième condition peut également être remplie par le respect du principe de minimisation des données (article 5.1.*c* du RGPD). La Chambre Contentieuse note que les

[182] Y compris la collecte d'un consentement valide avant le traitement des données personnelles, ou la possibilité pour les utilisateurs de s'opposer à un traitement fondé sur l'article 6.1.*f* RGPD au moment de la collecte des données à caractère personnel.

[183] IAB Europe *Transparency & Consent Framework - Policies*, Version 2020-11-18.3.2a, p. 5, https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

informations traitées dans une TC String[184] sont limitées aux données strictement nécessaires pour atteindre l'objectif visé. En outre, sur la base des pièces du dossier et des moyens de défense des parties, la Chambre Contentieuse n'a pas été en mesure d'établir que la TC String est conservée indéfiniment.

419. Afin de vérifier si la troisième condition de l'article 6.1.*f* du RGPD — le critère de « mise en balance » entre les intérêts du responsable du traitement, d'une part, et les libertés et droits fondamentaux de la personne concernée, d'autre part — peut être remplie, les attentes raisonnables de la personne concernée doivent être prises en compte conformément au considérant 47 du RGPD. En particulier, il convient d'évaluer si la personne concernée « peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée »[185].

420. C'est également ce que souligne la Cour dans son arrêt « *Asociaţia de Proprietari bloc M5A-ScaraA* »[186], dans lequel elle déclare :

> « *Sont également pertinentes aux fins de cette pondération les attentes raisonnables de la personne concernée à ce que ses données à caractère personnel ne seront pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci.* »

421. À cet égard, la Chambre Contentieuse trouve remarquable qu'aucune option ne soit offerte aux utilisateurs pour s'opposer complètement au traitement de leurs préférences dans le cadre du TCF. Quel que soit leur choix, la CMP générera une TC String avant de la lier au User ID unique de l'utilisateur, par le biais d'un cookie *euconsent-v2* placé sur l'appareil de la personne concernée.

422. En outre, dès lors que les utilisateurs ne sont pas informés de l'installation d'un cookie *euconsent-v2* sur leur dispositif, qu'ils soient ou non d'accord avec les finalités et les fournisseurs adtech proposés par la CMP, et qu'en outre ils ne sont pas informés de leur droit d'opposition à un tel traitement, la Chambre Contentieuse constate que la dernière condition de l'article 6.1.*f* du RGPD n'est actuellement pas remplie.

423. La gravité de la violation des droits et libertés de la personne concernée est également un élément essentiel de l'appréciation au titre de l'article 6.1.*f* RGPD. Le résultat de cette appréciation dépend des circonstances particulières du cas spécifique concerné[187]. Dans ce contexte, il convient selon la Cour de justice de tenir compte en particulier de « la nature éventuellement sensible de ces données, ainsi que de la nature et des modalités concrètes du traitement des données en cause, en particulier du nombre de personnes qui ont accès

[184] Voir para. 300 et 301 de la présente décision.
[185] Considérant 47 du RGPD.
[186] Arrêt CJUE du 11 décembre 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.
[187] *Ibidem*, para. 56.

à ces données et des modalités d'accès à ces dernières »[188]. Dans ce contexte, la Chambre Contentieuse souligne le grand nombre d'organisations participantes qui ont accès à la TC String, ainsi que le contrôle réduit des personnes concernées sur la nature et la portée du traitement de leurs données à caractère personnel par ces organisations.

424. **En l'absence de base juridique valide, la Chambre Contentieuse juge que le traitement des données dans le cadre du TCF dans son format actuel, par lequel les CMP enregistrent les préférences des utilisateurs dans une TC String, n'est pas conforme à l'article 6 du RGPD**.

425. **Il est donc indéniable pour la Chambre Contentieuse qu'IAB Europe, en tant que *Managing Organization* du TCF, n'a pas fourni de base juridique pour le traitement des préférences des utilisateurs sous la forme d'une TC String et a donc violé l'article 6 du RGPD.**

b. Collecte et diffusion de données à caractère personnel dans le cadre du RTB

426. Il n'est contesté par aucune des parties que le TCF vise à capter, au moyen des interfaces présentées par les CMP, le consentement des utilisateurs ou leur absence d'objection aux intérêts légitimes des fournisseurs adtech participants.

427. Pour mémoire, la Chambre Contentieuse souligne que ces deux bases concernent les activités de traitement qui ont lieu dans le cadre du RTB, conformément au protocole OpenRTB.

428. Cependant, la Chambre Contentieuse juge qu'aucune des bases proposées et mises en œuvre par le TCF ne peut être légalement invoquée par les participants au TCF. Tout d'abord, la Chambre Contentieuse estime que le consentement des personnes concernées obtenu par le biais des CMP n'est pas valide *(i)* et que la nécessité (pré)contractuelle n'est pas applicable *(ii)*. En outre, la Chambre Contentieuse estime que l'intérêt légitime ne répond pas au triple critère de la CJUE *(iii)*. L'article 6 du RGPD est donc enfreint.

(i) - Le consentement n'est pas une base valide pour les opérations de traitement dans l'OpenRTB telles que facilitées par le TCF

429. Afin de garantir que les *publishers* et les fournisseurs adtech se conforment aux exigences plus strictes en matière de transparence et de consentement prévues par le RGPD en ce qui concerne le traitement des données à caractère personnel dans le contexte de l'OpenRTB (ou du RTB en général), les CMP fournissent une interface relativement standardisée permettant aux utilisateurs de consentir ou de s'opposer au transfert de leurs données à caractère personnelles à des centaines de tiers en une seule fois, pour des finalités spécifiques.

[188] Arrêt CJUE du 11 décembre 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

430. Sur la base des pièces de ce dossier, la Chambre Contentieuse comprend que les participants peuvent poursuivre une ou plusieurs finalités parmi les 12 finalités standardisées que le TCF met à la disposition des fournisseurs adtech participants, et qui sont proposées aux utilisateurs au moyen des CMP[189].

431. Cependant, le système des CMP pose des problèmes à plusieurs niveaux, avec pour conséquence que le consentement obtenu par ces CMP (par l'intermédiaire du TCF), pour les traitements effectués dans le cadre de l'OpenRTB, n'est pas juridiquement valide au regard de l'article 7 RGPD.

432. Pour pouvoir être utilisé comme base juridique légitime, le consentement au titre de l'article 7 du RGPD doit répondre à des conditions strictes. Toutefois, pour les raisons exposées ci-dessous, la Chambre Contentieuse estime que le consentement recueilli par les CMP et les publishers dans la version actuelle du TCF est insuffisamment libre, spécifique, éclairé et dénué d'ambiguïté.

433. Tout d'abord, la Chambre Contentieuse constate que les finalités de traitement proposées ne sont pas décrites de manière suffisamment claire, et dans certains cas, sont même trompeuses[190]. À titre d'exemple, la Chambre Contentieuse constate que les finalités 8 (« *Measure content performance* ») et 9 (« *Apply market research to generate audience insights* »)[191] fournissent peu ou pas d'indications sur la portée du traitement, la nature des données à caractère personnel traitées, ou encore la durée de conservation des données à caractère personnel collectées tant que l'utilisateur ne retire pas son consentement.

434. En outre, sur la base des pièces du dossier, la Chambre Contentieuse comprend que *l'interface utilisateur* des CMP ne fournit pas un aperçu des catégories de données à caractère personnel collectées, ce qui rend impossible pour les utilisateurs de donner leur consentement éclairé.

435. La Chambre Contentieuse note également que le TCF rend particulièrement difficile pour les utilisateurs d'obtenir plus d'informations sur l'identité de tous les responsables du traitement des données auxquels ils donnent leur consentement pour traiter leurs données à certaines fins avant d'obtenir leur consentement. En particulier, les destinataires pour lesquels le consentement est recueilli sont si nombreux que les utilisateurs auraient besoin d'un temps disproportionné pour lire ces informations, ce qui signifie que leur consentement peut rarement être suffisamment éclairé.

436. En outre, les informations que les CMP fournissent aux utilisateurs demeurent trop générales pour refléter les opérations de traitement spécifiques de chaque fournisseur adtech, ce qui empêche la nécessaire granularité du consentement.

[189] Pour un aperçu de ces objectifs de la TCF, voir le paragraphe 337 de la présente décision.
[190] Voir para. 465 *et s*. de la présente décision.
[191] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), pp. 34-36.

437. En outre, la Chambre Contentieuse estime que l'enrichissement des données contenues dans une *bid request*, au moyen de données à caractère personnel déjà en possession des fournisseurs adtech et des CMP concernés, implique que les utilisateurs ne peuvent pas être adéquatement informés, puisque le TCF ne prévoit pas dans son format actuel que les organisations participantes indiquent quelles données à caractère personnel elles détiennent ni quelles opérations de traitement elles effectuent déjà avec ces données.

438. Enfin, la Chambre Contentieuse constate que le consentement, une fois obtenu par les CMP, ne peut être retiré par les utilisateurs aussi facilement qu'il a été donné, comme l'exige pourtant l'article 7 du RGPD. Tout d'abord, la Chambre Contentieuse observe qu'en vertu des *TCF Policies*, les fournisseurs adtech sont tenus de se conformer aux signaux de consentement d'un utilisateur en temps réel[192], alors qu'aucune mesure n'est mise en place pour garantir que les fournisseurs adtech ne puissent pas poursuivre leur traitement sur la base d'un signal de consentement reçu précédemment. Au demeurant, le TCF ne prévoit pas de transmission proactive des signaux de consentement mis à jour aux fournisseurs adtech. En outre, les *fournisseurs adtech* ne peuvent en principe plus accéder aux données à caractère personnel de l'utilisateur concerné après que celui-ci ait retiré son consentement, ce qui signifie également qu'ils ne peuvent pas identifier l'utilisateur pour lequel le consentement a été retiré en tant que tel, avec pour conséquence que les fournisseurs adtech continueront à traiter les données à caractère personnel de l'utilisateur en question[193].

439. En effet, la Chambre Contentieuse comprend que les CMP se trouvent à l'intersection entre les utilisateurs et les fournisseurs adtech participants, qui reçoivent leurs données à caractère personnel et les traitent ensuite à leurs propres fins. Une telle configuration signifie donc que le retrait d'un consentement par le biais d'un CMP ne prendra effet qu'à partir du moment où le fournisseur adtech concerné consultera les nouvelles valeurs dans la TC String modifiée via l'API de la CMP. En d'autres termes, le retrait du consentement n'est jamais immédiat et ne peut donc être considéré comme effectif.

440. Par conséquent, la Chambre Contentieuse conclut que l'article 6.1.*a* du RGPD ne constitue pas une base juridique valide pour le traitement et la diffusion de données à caractère personnel dans le cadre de l'OpenRTB, dans la mesure où ce consentement aurait été obtenu conformément au TCF dans son format actuel.

(ii) - L'intérêt légitime des organisations participantes ne l'emporte pas sur la protection des libertés et droits fondamentaux des personnes concernées.

441. La question est donc de savoir dans quelle mesure les organisations participant à la fois au TCF et à l'OpenRTB (fournisseurs adtech) peuvent légitimement se fonder sur l'article 6.1.*f*

[192] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a (Pièce 32), p.14

[193] Pour plus d'informations, voir : M. VEALE, FR. ZUIDERVEEN BORGESIUS, « Adtech and Real-Time Bidding under European Data Protection Law », *German Law Journal*, 31 July 2021, p. 26.

RGPD pour des finalités de traitement prédéfinies mettant en œuvre de la publicité ciblée ou le profilage des utilisateurs, par opposition à des finalités non liées au marketing, telles que la mesure d'audience et la mesure de performance.

442. Comme indiqué précédemment[194], l'appréciation des intérêts légitimes doit être effectuée sur la base de l'approche en trois étapes établie par la Cour de justice. Cette appréciation doit être effectuée par les responsables du traitement des données avant la mise en œuvre du traitement fondé sur l'article 6.1.f RGPD, étant donné qu'ils déterminent les moyens et les finalités des activités de traitement des données à caractère personnel envisagées et sont donc les seuls en mesure de mettre en place des garanties appropriées pour éviter un impact disproportionné sur les personnes concernées. Dans le cas où plusieurs responsables du traitement sont conjointement responsables, les principes de responsabilité et de transparence exigent que la mise en balance soit effectuée conjointement par tous les responsables du traitement des données impliqués dans le traitement.

443. Comme l'a indiqué le groupe de travail « Article 29 », les conséquences tant positives que négatives doivent être prises en considération pour évaluer l'impact du traitement, qui doit être nécessaire et proportionné à la réalisation des intérêts légitimes poursuivis par les responsables du traitement des données ou par un tiers. Ces conséquences peuvent inclure des « décisions ou de mesures éventuelles qui seront prises ultérieurement par des tiers et de situations où le traitement peut aboutir à l'exclusion de certaines personnes, à une discrimination à leur encontre, à de la diffamation ou, plus généralement, de situations qui comportent un risque de nuire à la réputation, au pouvoir de négociation ou à l'autonomie de la personne concernée.»[195]

444. En ce qui concerne le critère de finalité, en particulier la question de savoir si les intérêts poursuivis par les publishers et les fournisseurs adtech à travers le traitement des données à caractère personnel peuvent être reconnus comme légitimes, la Chambre Contentieuse comprend que les organisations participantes ont un intérêt à collecter et à traiter les données à caractère personnel des utilisateurs afin de pouvoir leur proposer des publicités sur mesure.

445. Sur la base de la jurisprudence de la Cour de justice et des lignes directrices de l'EDPB, la Chambre Contentieuse estime que la notion d'intérêt légitime peut avoir une portée large, étant entendu que l'intérêt invoqué par un responsable de traitement doit être suffisamment spécifique, existant, actuel et non hypothétique[196].

---

[194] Voir para. 411 *et s.*

[195] Groupe de travail Article 29 - Avis 06.2014 sur la notion d'intérêts légitimes du responsable du traitement des données au titre de l'article 7 de la directive 95-46-CE (WP217), p. 37.

[196] Arrêt de la CJUE du 11 décembre 2019, *TK c. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.

446. À cet égard, la Chambre Contentieuse ne peut que constater que, premièrement, les finalités de traitement proposées sont décrites en termes généraux, de sorte qu'il n'est pas aisé pour les utilisateurs d'apprécier dans quelle mesure la collecte, la diffusion et le traitement de leurs données à caractère personnel sont nécessaires aux finalités envisagées, pour autant que celles-ci soient d'ailleurs compréhensibles pour les utilisateurs.

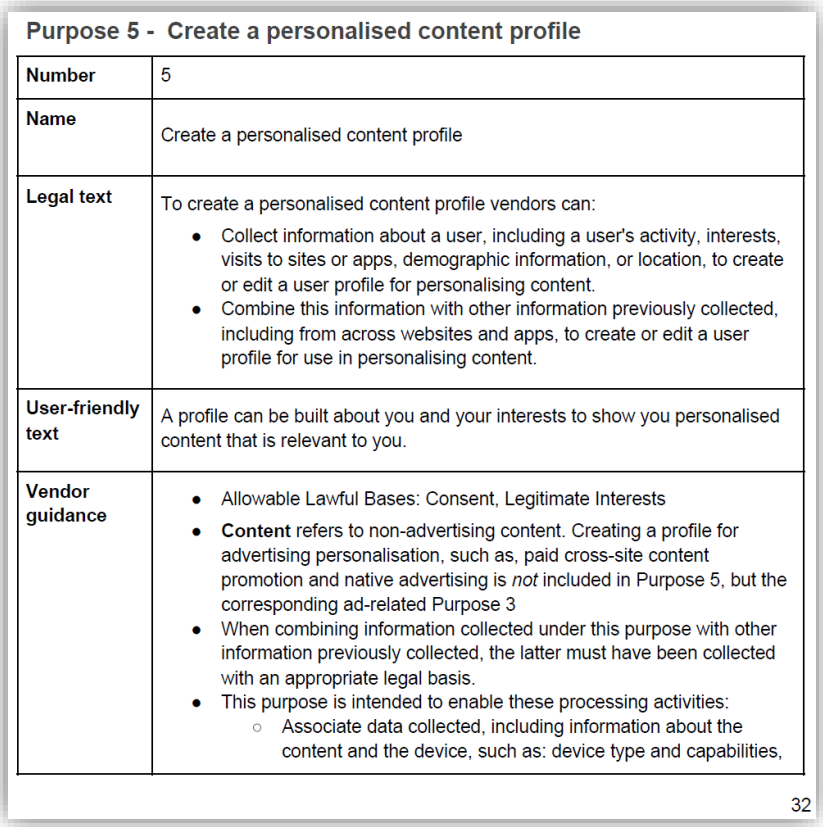
447. Pour être pertinent, un intérêt légitime doit être conforme au droit européen et national applicable, être suffisamment spécifique et formulé clairement de sorte qu'une mise en balance soit permise, et représenter un intérêt réel et actuel. Par conséquent, le simple fait d'invoquer un intérêt légitime dans le traitement des données à caractère personnel n'est pas suffisant ; le résultat du test de mise en balance déterminera si l'article 6.1.*f* RGPD peut être invoqué[197].

448. Les *TCF Policies* ne prévoient pas d'obligation pour les CMP d'expliquer en termes clairs aux utilisateurs les intérêts légitimes en jeu. Au lieu de cela, les exigences spécifiques pour les *Framework UIs* en rapport avec les intérêts légitimes contenues dans les *TCF Policies*[198] exigent seulement des CMP qu'elles mettent à disposition une couche d'information secondaire, permettant aux utilisateurs:

   a. d'obtenir des informations sur le fait que des données à caractère personnel sont traitées, ainsi que la nature des données à caractère personnel traitées (par exemple, des identifiants uniques, des données de navigation) ;
   b. d'obtenir des informations sur la portée du traitement fondé sur l'intérêt légitime et la portée de toute objection à ce traitement ;
   c. d'accéder aux paramètres dans l'interface CMP afin de s'opposer au traitement de leurs données à caractère personnel fondé sur un intérêt légitime ;
   d. d'examiner la liste des finalités de traitement, y compris leur intitulé standard et leur description standard complète, tels que définis à l'annexe A des *TCF Policies*, et de fournir aux utilisateurs un mécanisme pour voir quels fournisseurs adtech traitent leurs données pour chacune des finalités sur la base d'un intérêt légitime ;
   e. d'exercer leur droit d'opposition, soit à l'égard de chaque fournisseur adtech dont le traitement est fondé sur l'intérêt légitime, soit, de manière distincte, pour chaque finalité poursuivie par les fournisseurs adtech sur base d'un intérêt légitime;
   f. de consulter la liste nominative des fournisseurs adtech, ainsi que leurs objectifs et leurs bases juridiques, et d'accéder à un lien renvoyant vers la politique de confidentialité de chaque fournisseur adtech.

449. À titre d'exemple, la Chambre Contentieuse renvoie aux définitions de la finalité de traitement 5 (Create a personalised content profile), dans l'annexe A des *TCF Policies* [199]:

[197] *Ibidem*, p. 25.
[198] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a, pp.67-68.
[199] IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a, p. 32.



Purpose 5 - Create a personalised content profile

Number	5
Name	Create a personalised content profile
Legal text	To create a personalised content profile vendors can: • Collect information about a user, including a user's activity, interests, visits to sites or apps, demographic information, or location, to create or edit a user profile for personalising content. • Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalising content.
User-friendly text	A profile can be built about you and your interests to show you personalised content that is relevant to you.
Vendor guidance	• Allowable Lawful Bases: Consent, Legitimate Interests • **Content** refers to non-advertising content. Creating a profile for advertising personalisation, such as, paid cross-site content promotion and native advertising is *not* included in Purpose 5, but the corresponding ad-related Purpose 3 • When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis. • This purpose is intended to enable these processing activities: ○ Associate data collected, including information about the content and the device, such as: device type and capabilities,

32

450. Nonobstant le fait que les TCF Policies indiquent qu'elles établissent des exigences minimales en matière de langue, de conception et d'autres éléments dans l'interface utilisateur cadre (Framework UI), qui sont destinées à s'aligner sur les exigences juridiques de la réglementation européenne en matière de vie privée et de protection des données, la Chambre Contentieuse note par ailleurs que les règles et conditions générales pour les Framework UI précisent également que

> « *b. When providing transparency about Purposes and Features, the Framework UI must do so only on the basis of the standard Purpose, Special Purpose, Feature, and Special Feature names and definitions of Appendix A as they are published on the Global Vendor List or using Stacks*[200] *in accordance with the Policies and Specifications. UIs must make available the standard legal text of Purposes, Special Purposes, Features, and Special Features of Appendix A but may substitute or supplement the standard legal definitions with the standard user friendly text of Appendix A so long as the legal text remains available to the user and it is explained that these legal texts are definitive.* »

451. La Chambre Contentieuse interprète ces règles générales comme interdisant aux CMP et publishers participant au TCF d'expliquer davantage aux personnes concernées, de manière claire et conviviale, à la fois les intérêts légitimes poursuivis ainsi que les raisons

[200] Les « stacks » ou piles constituent, en substance, une combinaison de différents objectifs de traitement.

pour lesquelles ils estiment que leurs intérêts ne sont pas supplantés par les intérêts ou les droits et libertés fondamentaux des personnes concernées[201].

452. Bien que, dans le contexte de la présente affaire, la Chambre Contentieuse ne se prononce pas sur la question de savoir si un intérêt économique[202] peut être considéré comme un intérêt légitime au sens de l'article 6.1.*f* du RGPD, elle considère que le manque de spécificité des finalités déclarées a pour conséquence que la première condition d'un traitement licite *spécifique* n'est pas remplie au moyen des descriptions standardisées des finalités du traitement et des intérêts poursuivis, telles qu'imposées par les *TCF Policies*.

453. Dans le cadre du critère de nécessité, visant à déterminer si les traitements envisagés sont nécessaires à la réalisation des intérêts poursuivis, il convient de se demander si les intérêts légitimes poursuivis par le traitement des données ne pourraient raisonnablement pas être atteints de manière tout aussi efficace par d'autres moyens, entraînant une ingérence moindre dans les libertés et droits fondamentaux des personnes concernées, en particulier leur droit au respect de leur vie privée et leur droit à la protection des données à caractère personnel, tels que garantis par les articles 7 et 8 de la Charte[203].

454. La Cour de justice a également précisé que la condition de nécessité du traitement doit être examinée au regard du principe de minimisation des données énoncé à l'article 5.1.*c* du RGPD[204]. En d'autres termes, il est nécessaire selon l'EDPB d'examiner si d'autres moyens, moins invasifs, sont disponibles pour atteindre le même objectif.

455. Dans ce cas-ci, la Chambre Contentieuse comprend qu'aucune garantie n'est prévue pour s'assurer que les données à caractère personnel collectées et diffusées se limitent aux informations strictement nécessaires pour les finalités envisagées.[205]

456. En l'absence de mesures démontrant de manière adéquate qu'aucune donnée personnelle inappropriée n'est diffusée, la Chambre Contentieuse est contrainte de juger que la deuxième condition n'est pas remplie.

457. En ce qui concerne le critère de mise en balance, en particulier la question de savoir si les intérêts poursuivis par les fournisseurs adtech l'emportent sur les libertés et droits fondamentaux des personnes concernées, les attentes raisonnables des personnes

---

[201] Groupe de travail Article 29 - Avis 06.2014 sur la notion d'intérêts légitimes du responsable du traitement des données au titre de l'article 7 de la directive 95-46-CE (WP217), p. 47.

[202] Contrairement à l'intérêt poursuivi par la captation des choix des utilisateurs dans une TC String, tel qu'analysé aux para. 404 et suivants.

[203] Arrêt de la CJUE du 4 mai 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA « Rīgas satiksme »*, C-13/16; ECLI: EU:C:2017:336, para. 47.

[204] *Ibidem*, para. 48.

[205] À cet égard, certains auteurs affirment qu'il existe des alternatives au RTB, dans lesquelles seules des informations minimales sur l'utilisateur sont communiquées. Voir M. VEALE, FR. ZUIDERVEEN BORGESIUS, « Adtech and Real-Time Bidding under European Data Protection Law », German Law Journal, 31 juillet 2021, p. 19 et suivantes. Les auteurs mentionnent en particulier le plug-in de navigateur Adnostic, développé il y a dix ans, qui établit un profil sur la base du comportement de navigation de l'utilisateur afin de cibler les publicités, les informations quittant l'appareil de l'utilisateur étant minimales et le ciblage comportemental ayant lieu exclusivement dans le navigateur de l'utilisateur. En outre, les auteurs font référence au système de Google appelé *Federated Learning of Cohorts* (FLoC) pour le microciblage dans Chrome.

concernées devraient également être prises en compte, conformément au considérant 47 du RGPD, en plus des circonstances spécifiques au cas particulier[206].

458. Le critère de la gravité de la violation des droits et libertés de la personne concernée constitue un élément essentiel de l'appréciation au cas par cas exigée par l'article 6.1.*f* du RGPD[207]. Dans ce contexte, il convient selon la Cour de justice de tenir compte en particulier de « la nature des données à caractère personnel en cause, en particulier de la nature éventuellement sensible de ces données, ainsi que de la nature et des modalités concrètes du traitement des données en cause, en particulier du nombre de personnes qui ont accès à ces données et des modalités d'accès à ces dernières[208] ».

459. Une fois encore, la Chambre Contentieuse constate, premièrement, qu'en raison du grand nombre de partenaires TCF susceptibles de recevoir leurs données à caractère personnel, les personnes concernées ne peuvent pas raisonnablement s'attendre aux traitements découlant de cette transmission. À cela s'ajoute la quantité considérable de données qui, conformément aux préférences saisies dans le cadre du TCF, sont collectées par le biais d'une *bid request* et transmises aux fournisseurs adtech dans le cadre du protocole OpenRTB[209].

460. En outre, l'EDPB indique que l'intérêt légitime ne constitue pas une base juridique suffisante dans le contexte du marketing direct mettant en œuvre de la publicité comportementale[210]. De même, l'ICO a conclu dans un rapport récent que l'intérêt légitime n'est pas une base de licéité dans le contexte du RTB (malgré ceci de nombreux publishers fondent leurs traitement sur cette base juridique)[211]. En résumé, au vu de ce qui précède, la Chambre Contentieuse juge que la troisième condition imposée par l'article 6.1.*f* RGPD et la jurisprudence de la Cour n'est pas remplie *en l'espèce*.

461. À la lumière des considérations susmentionnées, la Chambre Contentieuse estime que **l'intérêt légitime des organisations participantes ne peut être considéré comme une base juridique adéquate pour les activités de traitement effectuées selon le protocole OpenRTB, conformément aux préférences et aux choix des utilisateurs saisis dans le cadre du TCF**.

---

[206] Arrêt CJUE du 11 décembre 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.

[207] *Ibidem*, para. 56.

[208] Arrêt CJUE du 11 décembre 2019, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

[209] Norsk Forbrukerrådet - « Out of Control. Comment les consommateurs sont exploités par l'industrie de la publicité en ligne », 14 janvier 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/, p. 36-37 ; voir également la recommandation CM/Rec(2021)8 du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, 3 novembre 2021 : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a46147.

[210] Groupe de travail Article 29 - Avis 03/2013 sur la limitation de la finalité (WP 203), 2 avril 2013, p. 46 : « le consentement devrait être exigé, par exemple, pour le suivi et le profilage à des fins de marketing direct, de publicité comportementale, de courtage de données, de publicité basée sur la localisation ou d'études de marché numériques basées sur le suivi ».

[211] Information Commissioner's Office - « Update report into adtech and real time bidding », 20 juin 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

(iii) - La nécessité contractuelle n'est pas une base valable pour le traitement des données à caractère personnel dans le contexte du TCF et de l'OpenRTB

462. Conformément aux lignes directrices de l'EDPB, la Chambre Contentieuse note que, de manière générale, la nécessité (pré)contractuelle du traitement n'est pas une base juridique applicable à la publicité comportementale[212].

463. De surcroît, la Chambre Contentieuse note que la version actuelle du TCF ne mentionne nulle part l'article 6.1.*b* RGPD comme une base juridique possible pour le traitement des données à caractère personnel au sein du TCF et de l'OpenRTB.

464. **Sur la base des éléments qui précèdent, la Chambre Contentieuse conclut donc que le traitement des données à caractère personnel dans le cadre de l'OpenRTB, sur la base des préférences capturées conformément à la version actuelle du TCF, est incompatible avec le RGPD en raison d'une violation inhérente du principe de licéité et de loyauté.**

B.4.2. - Obligation de transparence envers les personnes concernées (articles 12, 13 et 14 du RGPD)

465. Les plaignants soulèvent la question du manque de transparence, et plus particulièrement le fait que l'écosystème OpenRTB est si étendu qu'il est impossible pour les personnes concernées de donner un consentement éclairé au traitement de leurs données à caractère personnel, ou de s'opposer de manière éclairée au traitement de leurs données à caractère personnel sur la base d'un intérêt légitime.

466. La défenderesse, quant à elle, affirme que le TCF offre une solution pour recueillir le consentement valide des utilisateurs, lorsqu'applicable, conformément aux exigences énoncées dans le RGPD et la directive ePrivacy[213].

467. La Chambre Contentieuse estime que les informations fournies en vertu du format actuel du TCF aux personnes concernées, bien qu'aux fins du traitement de leurs données à caractère personnel dans le cadre de l'OpenRTB, ne répondent pas aux exigences de transparence prévues par le RGPD[214].

468. Tout d'abord, la Chambre Contentieuse indique qu'IAB Europe peut, dans certains cas, réclamer les « *records of consent* » que les CMP sont tenus de conserver, conformément aux *TCF Policies*[215], mais omet d'informer les personnes concernées de ce traitement potentiel par IAB Europe.

[212] EDPB - Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, v2.0, 8 octobre 2019, p. 14 et s., https://edpb.europa.eu.

[213] TCF Policies d'IAB Europe v2019-08-21.3 (Pièce 32) ; TCF Policies d'IAB Europe v2019-04-02.2c (Pièce 38).

[214] Voir para. 433 et suivants de la présente décision.

[215] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 11, 14 et 19.

469. En second lieu, la Chambre Contentieuse estime que la manière dont l'information est fournie aux personnes concernées, qui a été établie par IAB Europe, ne respecte pas l'exigence d'une « forme transparente, compréhensible et facilement accessible »[216]. L'ancien Groupe de travail « Article 29 » énonce dans ses lignes directrices sur la transparence que « L'exigence que la fourniture d'informations aux personnes concernées et que les communications qui leur sont adressées soient réalisées d'une manière «concise et transparente» signifie que les responsables du traitement devraient présenter les informations/communications de façon efficace et succincte afin d'éviter de noyer d'informations les personnes concernées »[217]. En outre, les personnes concernées doivent pouvoir déterminer à l'avance la portée et les conséquences du traitement et ne pas être surprises ultérieurement par d'autres façons d'utiliser leurs données à caractère personnel[218].

470. La Chambre Contentieuse estime que l'approche adoptée jusqu'à présent ne remplit pas les conditions de transparence et d'équité requises par le RGPD. Certaines des finalités de traitement annoncées sont en effet exprimées de manière trop générique pour que les personnes concernées soient correctement informées de la portée et de la nature exactes du traitement de leurs données à caractère personnel[219]. Cela est particulièrement problématique pour les finalités qui reposent sur le consentement des personnes concernées, car le consentement doit être spécifique et suffisamment informé pour être valable en tant que base juridique[220].

471. La Chambre Contentieuse se réfère également aux exemples de CMP précisés dans le rapport technique du Service d'Inspection, et constate que l'interface offerte aux utilisateurs ne permet pas, entre autres, d'identifier de manière simple et claire les finalités de traitement associées à l'autorisation d'un fournisseur adtech particulier ou d'identifier les fournisseurs adtech qui traiteront leurs données pour une finalité spécifique[221].

472. À cet égard, la Chambre Contentieuse souligne que le grand nombre de tiers, à savoir les fournisseurs adtech qui recevront et traiteront le cas échéant les données à caractère personnel des utilisateurs issues de la *bid request*, en fonction des préférences qu'ils ont saisies, n'est pas compatible avec la condition d'un consentement suffisamment éclairé, ni avec l'obligation de transparence plus large prévue par le RGPD.

---

[216] Art. 12.1 RGPD.

[217] WP260 - Orientations sur la transparence dans le cadre du GDPR, paragraphe 8.

[218] WP260 - Orientations sur la transparence dans le cadre du GDPR, paragraphe. 10.

[219] Voir le para. 4333 de cette décision pour des exemples ainsi que les para. 441-452 pour une analyse plus approfondie par la Chambre Contentieuse ; voir également C. MATT, C. SANTOS, N. BIELOVA, « Purposes in IAB Europe's TCF : which legal basis and how are they used by advertisers ? », in *Privacy Technologies and Policy*, APF 2020, LNCS, vol 12121, Springer, 2020, pp. 163-185.

[220] Voir para. 429-440 *et s*. de la présente décision.

[221] Rapport d'analyse technique du Service d'Inspection, 6 janvier 2020 (pièce 53), p. 99 *et s*.

473. Sur la base des éléments qui précèdent, la Chambre Contentieuse doit donc juger que le TCF, dans sa configuration actuelle, ne respecte pas les obligations découlant du principe de transparence, notamment les articles 12, 13 et 14 RGPD.

B.4.3. - Responsabilité (art. 24 RGPD), protection des données dès la conception et par défaut (art. 25 RGPD), intégrité et confidentialité (art. 5.1.f RGPD), et sécurité du traitement (art. 32 RGPD)

a. Principe de responsabilité et protection des données dès la conception et par défaut

474. L'article 24.1 RGPD impose au responsable du traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD règlement. Ces mesures doivent en outre être réexaminées et actualisées si nécessaire. Cet article reflète le principe de « responsabilité » » énoncé à l'article 5.2 du RGPD, selon lequel « le responsable du traitement est responsable du respect du paragraphe 1 (responsabilité) et est en mesure d'en apporter la preuve ». L'article 24.2 du RGPD dispose que, lorsqu'elles sont proportionnées par rapport aux activités de traitement, les mesures visées à l'article 24.1 du RGPD ci-dessous comprennent la mise en œuvre de politiques de protection des données appropriées par le responsable du traitement.

475. Le considérant 74 du RGPD ajoute qu' « il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte. Il importe, en particulier, que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec le présent règlement, y compris l'efficacité des mesures. Ces mesures devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci présente pour les droits et libertés des personnes physiques. »

476. Il incombe également au responsable du traitement, conformément aux articles 24 (responsabilité) et 25 du RGPD (protection des données dès la conception et par défaut), d'intégrer le respect nécessaire des règles du RGPD dans ses traitements et procédures (par exemple, s'assurer de l'existence et de l'efficacité des procédures de traitement des demandes des personnes concernées, et portant sur la vérification de l'intégrité et de la conformité de la TC String).

b. Les contours de l'obligation de sécurité

477. Conformément à l'article 32 RGPD, le responsable du traitement a la responsabilité de garantir la sécurité du traitement, « compte tenu de l'état des connaissances, des coûts de

mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ». La Chambre Contentieuse constate cependant un manque de respect de l'obligation d'assurer la sécurité du traitement de la part de la défenderesse, obligation qui fait partie du principe de responsabilité. Cette lacune est abordée dans les points suivants.

478. Ce manquement à l'obligation d'assurer la sécurité du traitement constitue un point fondamental de la présente décision et des sanctions qu'elle impose. L'absence de mesures techniques et organisationnelles visant à garantir l'intégrité de la TC String est considérée comme une infraction grave.

479. Selon l'article 5.1*f* RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. En l'absence de mesures appropriées pour sécuriser les données à caractère personnel des personnes concernées, l'effectivité du respect des droits fondamentaux à la vie privée et à la protection des données à caractère personnel ne peut être garantie, compte tenu notamment du rôle crucial joué par les technologies de l'information et de la communication dans notre société.

480. Comme indiqué dans la section précédente, l'absence d'obligation d'assurer la sécurité du traitement constitue un point important de la décision[222]. Compte tenu du très grand nombre de TC Strings générée chaque jour dans le cadre du TCF, il est essentiel que l'ensemble des règles régissant la participation au TCF soient observées et respectées par toutes les parties concernées, sous la supervision d'IAB Europe en tant que *Managing Organization*. La Chambre Contentieuse rappelle que la lecture combinée des articles 32 (sécurité du traitement), ainsi que 5.2 et 24 RGPD (principe de responsabilité) impose au responsable du traitement de démontrer son respect de l'article 32, en prenant des mesures techniques et organisationnelles appropriées, de manière transparente et traçable.

481. La Chambre Contentieuse rappelle également l'exigence de l'article 25 RGPD (protection des données par conception et par défaut), qui impose au responsable du traitement d'intégrer la nécessaire conformité aux règles du RGPD en amont de ses actions.

482. Il convient également de noter que le principe de sécurité, avec ses différentes composantes d'intégrité, de confidentialité et de disponibilité des données, est énoncé aux articles 5.1.*f* et 32 du RGPD et est désormais réglementé dans le RGPD au même titre que les principes fondamentaux de licéité, de transparence et de loyauté.

[222] Voir para. 448 et suivants de la présente décision.

483. IAB Europe propose le TCF pour rendre le protocole OpenRTB conforme au RGPD. En d'autres termes, l'objectif du TCF est de garantir que les traitements de données à caractère personnel dans le cadre du protocole OpenRTB se déroulent conformément au RGPD ainsi qu'à la directive ePrivacy. Par conséquent, IAB Europe, en tant que *Managing Organization* du TCF et responsable conjointe des opérations de traitement effectuées dans ce cadre[223], doit prendre des mesures organisationnelles et techniques pour garantir que les participants respectent au moins les TCF Policies.

484. Bien que dans le système TCF actuel d'IAB Europe, les fournisseurs adtech reçoivent les signaux de consentement dans le cadre d'une requête HTTP(S) ou via les API de navigateurs, certains auteurs estiment que les mesures en place dans le cadre du TCF sont insuffisantes pour garantir l'intégrité des signaux de consentement (en particulier leur validité) et pour s'assurer qu'un fournisseur adtech les a effectivement reçus (plutôt que générés lui-même)[224].

485. Toutefois, en l'absence de validation par IAB Europe, il devient théoriquement possible pour les CMP de falsifier ou de modifier le signal pour générer un cookie *euconsent-v2* et ainsi reproduire un « faux consentement » des utilisateurs à toutes fins et pour tous les fournisseurs adtech. Ce cas est en outre explicitement prévu par les *TCF Policies*:

> « *A Vendor must not create Signals where no CMP has communicated a Signal and shall only transmit Signals communicated by a CMP or received from a Vendor who forwarded a Signal originating from a CMP without extension, modification, or supplementation, except as expressly allowed for in the Policies and/or Specifications.* »[225]

486. La Chambre Contentieuse prend note du fait que la possibilité de falsification ou de modification de la TC String par les CMP est prévue dans le document *TCF Policies* de la défenderesse, qui établit les bases du TCF.

487. La Chambre Contentieuse s'appuie également sur le fait que la défenderesse indique sur son site web l'introduction du « *TCF Vendor Compliance Programme* », par lequel des audits des organisations participant au TCF (listées sur la *Global Vendors List*) auront lieu[226]. La Chambre Contentieuse encourage toutes les initiatives émanant de la défenderesse, qui visent à assurer le respect de l'obligation de traiter les données à caractère personnel en vertu du TCF de manière sécurisée. Néanmoins, compte tenu de l'absence de contrôle systématique par la défenderesse du respect des règles TCF par les organisations participantes, et compte tenu de l'impact significatif de telles violations (notamment, la

[223] Voir *supra*, titre B.2 . - Responsabilité d'IAB Europe pour les opérations de traitement dans le Transparency and Consent Framework.

[224] Voir à ce sujet, par exemple C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, « Consent Management Platforms Under the GDPR: Processors and/or Controllers? », in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 64.

[225] *Transparency and Consent Framework Policies*, Chapitre III 13 (6), https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/#13_Working_with_CMPs

[226] https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/

falsification ou la modification de la TC String), la Chambre Contentieuse considère que cette introduction du *TCF Vendor Compliance Programme* est insuffisante pour mettre la défenderesse en conformité avec l'obligation de sécurité.

488. En particulier, la Chambre Contentieuse s'appuie sur le fait que le régime de sanctions de ce nouveau programme, prévu par la défenderesse en cas de non-respect des règles du TCF, est permissif et non dissuasif. En effet, un fournisseur adtech peut se déclarer responsable d'un manquement jusqu'à trois reprises, sans aucune sanction, avant de bénéficier d'un délai de 28 jours pour se mettre en conformité. Ce n'est qu'en cas de non-conformité après l'expiration des 28 jours que le fournisseur adtech sera suspendu de la *Global Vendors List*. Il peut également être réintroduit dans la liste s'il se conforme aux règles par la suite. Le programme prévoit également qu'un fournisseur adtech puisse commettre une infraction jusqu'à quatre fois, avant de procéder à sa suspension immédiate pendant une brève période de 14 jours, jusqu'à ce que le fournisseur se mette en conformité. Le « *TCF Vendor Compliance Programme* » ne constitue donc pas une mesure suffisante pour assurer la sécurité des traitements de données à caractère personnel opérés dans le cadre du TCF.

489. La Chambre Contentieuse observe également qu'aucune mesure autre que le « *TCF Vendor Compliance Programme* » n'est prévue par la défenderesse pour surveiller ou empêcher la falsification ou la modification de la TC String.

490. En ce qui concerne l'allégation des plaignants selon laquelle IAB Europe enfreint également les articles 44 à 49 du GDPR, la Chambre Contentieuse reconnaît, au vu de la portée du TCF — qui implique un grand nombre d'organisations participantes — qu'il est évident que les données à caractère personnel inclues dans les TC Strings seront transférées à un moment donné en dehors de l'EEE par les CMP, et que la défenderesse agit en tant que responsable du traitement à cet égard (voir para. 356-357). La Chambre Contentieuse note cependant que le Service d'Inspection n'a pas inclus dans son rapport une appréciation d'un transfert international concret de données. Pour cette raison, la Chambre Contentieuse conclut qu'il y a une violation du RGPD, mais au vu de l'absence de preuve d'un transfert international systématique, ainsi que de la portée et de la nature de celui-ci, la Chambre Contentieuse estime qu'elle n'est pas en mesure de sanctionner la défenderesse pour une violation des articles 44 à 49 du RGPD. Nonobstant ce qui précède, la Chambre Contentieuse juge également que ces transferts internationaux de données à caractère personnel, le cas échéant, doivent être évalués en premier lieu par les publishers et les CMP qui mettent en œuvre le TCF. La Chambre Contentieuse constate que les publishers sont responsables et redevables de prendre les mesures nécessaires pour éviter que les données à caractère personnel collectées par le biais de leur site web et/ou application ne soient transférées en dehors de l'EEE sans mécanismes de transfert international adéquats.

491. Toutefois, la Chambre Contentieuse est également d'avis que la défenderesse devrait faciliter la diligence raisonnable (*due diligence*) incombant aux publishers et aux CMP, en

exigeant par exemple que les fournisseurs *adtech* indiquent clairement s'ils sont localisés en dehors de l'EEE ou s'ils envisagent de transférer ultérieurement des données à caractère personnel en dehors de l'EEE par l'intermédiaire de leurs sous-traitants. En outre, la Chambre Contentieuse note que, contrairement à l'obligation qui lui incombe en vertu des principes de responsabilité et de protection des données dès la conception et par défaut, IAB Europe n'a prévu aucun mécanisme permettant de s'assurer que les publishers et les CMP participants ont mis en place des mécanismes adéquats pour les transferts internationaux potentiels de la TC String, comme le prévoient les articles 44 à 49 du RGPD, tant au moment de sa création que lors de la transmission de la TC String aux fournisseurs adtech participants. Le préambule des *TCF Policies* indique simplement que le TCF « *is not intended nor has it been designed to facilitate [...] more strictly regulated processing activities, such as transferring personal data outside of the EU* ». La Chambre Contentieuse estime que cela ne répond pas aux exigences des articles 24 et 25 du RGPD.

492. La Chambre Contentieuse note, pour mémoire, qu'il n'est pas certain que, compte tenu de son architecture actuelle et de la prise en charge du protocole OpenRTB, le TCF puisse être concilié avec le RGPD.

493. En ce sens, la responsabilité d'IAB Europe est engagée à partir du moment où l'organisation conçoit et met à disposition un système de gestion du consentement ou des objections des utilisateurs, mais ne prend pas les mesures nécessaires pour garantir la conformité, l'intégrité et la validité de ce consentement ou de cette objection.

494. La Chambre Contentieuse constate donc que, dans le cadre de ses obligations de sécurité et d'intégrité, il incombe à IAB Europe de prendre des mesures effectives, tant organisationnelles que techniques, pour garantir et pouvoir démontrer l'intégrité du signal préférentiel transmis par les CMP aux fournisseurs adtech.

B.4.4 - Autres violations alléguées du RGPD

a. Limitation de la finalité et minimisation des données (art. 5.1.b et 5.1.c du RGPD)

495. Bien que dans cette décision, la Chambre Contentieuse ait déjà conclu que les opérations de traitement fondées sur le protocole OpenRTB ne sont pas conformes aux principes fondamentaux de limitation de la finalité et de minimisation des données[227] (dès lors qu'aucune garantie n'est prévue pour assurer que les données à caractère personnel collectées et diffusées dans le cadre de l'OpenRTB se limitent aux informations strictement nécessaires aux finalités poursuivies), la Chambre Contentieuse souligne que les plaignants ont explicitement indiqué dans leurs conclusions qu'ils limitent la portée de leurs allégations aux opérations de traitement au sein du TCF. Le Service d'Inspection a également précisé dans son rapport qu'IAB Europe n'agit pas en tant que responsable du traitement des

[227] Voir para. 455-456 de la présente décision

données pour les opérations de traitement qui ont lieu intégralement dans le cadre de l'OpenRTB.

496. Compte tenu de ces précisions, la Chambre Contentieuse conclut que, vu la quantité limitée de données relatives à un utilisateur qui sont stockées dans une TC String avant d'être sauvegardées au moyen d'un cookie *euconsent-v2*, il n'y a pas de violation des principes de limitation de la finalité et de minimisation des données dans le contexte du TCF.

497. Bien que des quantités plus importantes de données à caractère personnel soient traitées à un stade ultérieur, en ce compris des catégories particulières de données à caractère personnel, ce n'est pas le cas dans le contexte du TCF. Dans le cadre du TCF, il n'y a donc pas de violation des principes de limitation de la finalité et de minimisation des données.

b. Limitation du stockage (Art. 5.1.e RGPD)

498. Pour ce qui est du principe de limitation de la conservation et sur la base du rapport du Service d'Inspection, la Chambre Contentieuse estime qu'il n'y a pas de preuves suffisantes que la TC String et le stockage associé des données à caractère personnel des utilisateurs sont stockés pendant une période non autorisée, en violation de l'article 5.1.*e* du RGPD.

499. Par conséquent, la Chambre Contentieuse conclut qu'aucune violation de l'article 5.1.*e* du RGPD n'a pu être établie.

c. Intégrité et confidentialité (Art. 5.1.f RGPD)

500. Comme déjà expliqué ci-dessus[228], la Chambre Contentieuse estime que la version actuelle du TCF offre des garanties insuffisantes pour empêcher que les valeurs incluses dans une TC String ne soient modifiées de manière non autorisée, avec pour conséquence que les données à caractère personnel d'une personne concernée regroupées dans une *bid request* peuvent être traitées à de mauvaises fins, en violation du principe d'intégrité, et/ou peuvent aboutir chez les mauvais fournisseurs adtech ou des fournisseurs adtech refusés par l'utilisateur, en violation du principe de confidentialité. La Chambre Contentieuse juge donc que la version actuelle du TCF viole l'article 5.1.*f* du RGPD.

d. Traitement de catégories particulières de données à caractère personnel (Art. 9 RGPD)

501. Bien qu'un certain nombre de plaintes soient dirigées contre le système du RTB, y compris le protocole *Authorized Buyers* développé par Google ainsi que le protocole OpenRTB développé par IAB Tech Lab, le Service d'Inspection a déterminé dans son rapport, à titre préliminaire, que l'Autorité belge de protection des données n'était pas compétente pour le premier et que IAB Tech Lab n'agit pas en tant que responsable du traitement pour le second[229].

[228] Voir para. 477 *et s.* de la présente décision.
[229] Rapport d'enquête du Service d'Inspection, pp. 8-11.

502. La Chambre Contentieuse note que le Service d'Inspection signale l'absence de règles appropriées pour le traitement des catégories spéciales de données à caractère personnel au titre du TCF. Toutefois, cette observation n'est étayée par aucune analyse technique montrant que les catégories spéciales de données à caractère personnel sont effectivement traitées *au sein du TCF*. Au contraire, les analyses techniques du Service d'Inspection montrent que la TC String en elle-même ne contient aucune information pouvant être liée à la taxonomie des sites web visités, où, par exemple, des catégories spéciales de données à caractère personnel peuvent être impliquées.

503. Par conséquent, la Chambre Contentieuse juge que cette allégation n'est pas fondée et qu'il ne peut être conclu à une violation de l'article 9 du RGPD par la défenderesse.

e. Exercice des droits des personnes concernées (articles 15 à 22 du RGPD)

504. Tout d'abord, le Service d'Inspection note dans son rapport que certains plaignants ont fait état de l'impossibilité pour les personnes concernées de faire valoir leurs droits, même si l'enquête menée par le Service d'Inspection n'a pas permis de confirmer ces allégations. Compte tenu de l'absence de preuve d'une quelconque infraction, la Chambre Contentieuse limite son raisonnement à des conclusions générales relatives à l'exercice des droits des personnes concernées.

505. En second lieu, la Chambre Contentieuse prend en considération la portée des conclusions écrites des plaignants, dans lesquelles ils ont spécifiquement limité leurs griefs au traitement des données à caractère personnel des plaignants par la défenderesse dans le cadre particulier du TCF[230]. Par conséquent, la Chambre Contentieuse n'évaluera pas les circonstances dans lesquelles les personnes concernées peuvent exercer leurs droits concernant le traitement des données à caractère personnel contenues dans les *demandes d'offres*, en ce qui concerne les *fournisseurs adtech*, étant donné que ce traitement a lieu entièrement sous le protocole OpenRTB.

506. En ce qui concerne la version actuelle du TCF, la Chambre Contentieuse constate toutefois que le TCF ne semble pas faciliter l'exercice des droits des personnes concernées, dans la mesure où l'interface de la CMP ne peut pas être rappelée facilement et à tout moment par les utilisateurs, de manière à leur permettre de modifier leurs préférences et de retrouver l'identité des fournisseurs adtech avec lesquels leurs données à caractère personnel ont été partagées au moyen d'une *bid request*, conformément au protocole OpenRTB. À cet égard, la Chambre Contentieuse souligne l'importance d'une mise en œuvre et d'une application correctes des exigences en matière d'interface, telles que définies dans les *TCF Policies*, de manière à permettre aux personnes concernées d'exercer effectivement leurs droits vis-à-vis de chacun des responsables conjoints du traitement, et note que la responsabilité partagée à cet égard incombe principalement aux CMP et aux publishers.

[230] Conclusions des plaignants du 18 février 2021, p. 2.

Dans ces circonstances, néanmoins, la Chambre Contentieuse n'est pas en position de constater une infraction aux articles 15 - 22 RGPD.

f. Registre des activités de traitement (Art. 30 RGPD)

507. Le Service d'Inspection note dans son rapport qu'IAB Europe ne tient pas de registre de ses activités de traitement. La défenderesse estime, tout d'abord, qu'elle peut se prévaloir de l'exception prévue à l'article 30.5 du RGPD et qu'elle n'est donc pas soumise à l'obligation de conserver de tels enregistrements. Au cours de l'enquête, la défenderesse a néanmoins ajouté aux documents du dossier un résumé de ses activités de traitement[231].

508. La Chambre Contentieuse constate tout d'abord que le registre soumis par la défenderesse ainsi fourni ne contient aucune activité relative au TCF, à l'exception de la gestion des membres, y compris l'administration du TCF. Contrairement à l'affirmation de la défenderesse, à savoir que les registres n'ont pas besoin d'inclure les activités de traitement dans le contexte du TCF, la Chambre Contentieuse est d'avis que les registres doivent à tout le moins inclure l'accès aux signaux de consentement, aux objections et aux préférences des utilisateurs.

509. En effet, conformément à l'article 8 des *TCF Policies* (v1.1)[232] et à l'article 15 des *TCF Policies* (v2.0)[233], la défenderesse se réserve le droit, en tant que *Managing Organization*, d'accéder aux « *records of consent* ». La Chambre Contentieuse souligne également que le caractère accessoire de cet accès aux préférences des utilisateurs n'a pas été démontré ou soulevé par la défenderesse. La relation stable entre IAB Europe, en sa qualité de *Managing Organization*, et toutes les organisations participant à l'écosystème TCF, doit également être prise en compte. Compte tenu du grand nombre d'organisations participantes et de l'intention de la défenderesse de contrôler la conformité des différents CMP et autres *fournisseurs adtech*[234] de manière plus approfondie à l'avenir, IAB Europe devrait également inclure ce traitement dans ses registres d'activités de traitement.

510. Par conséquent, la Chambre Contentieuse considère que le caractère non accessoire du traitement et la violation de l'article 30.1 du RGPD constatée par le Service d'Inspection sont suffisamment prouvés.

g. Analyse d'impact relative à la protection des données (Art. 35 RGPD)

511. La Chambre Contentieuse relève tout d'abord que la défenderesse ne conteste pas que le TCF puisse également être utilisé à des fins de RTB.

512. L'argument de la défenderesse selon lequel le TCF peut être utilisé à d'autres fins, non liées au marketing direct, et que l'OpenRTB peut également fonctionner séparément du TCF

[231] Réponse d'IAB Europe à l'enquête du 10 février 2020 (pièce 57), p. 23.
[232] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 38), p. 6.
[233] IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Pièce 32), p. 14.
[234] Cf. Audience du 11 juin 2021.

n'est donc pas pertinent pour l'examen de la nécessité ou non d'une analyse d'impact sur la protection des données.

513. Au demeurant, la corrélation entre le TCF et le RTB implique que les préférences que les utilisateurs saisissent à l'aide de l'interface de la CMP auront nécessairement un impact sur la manière dont leurs données à caractère personnel seront ensuite traitées par les *fournisseurs* adtech dans le cadre du RTB, conformément au protocole OpenRTB.

514. La Chambre Contentieuse se réfère en outre à la décision n° 01/2019 du Secrétariat Général de l'APD belge[235], dans laquelle le Secrétariat Général a établi une liste des traitements pour lesquels une analyse d'impact sur la protection des données est requise.

515. Il est incontestable pour la Chambre Contentieuse que le TCF a été développé, entre autres, pour le système RTB, dans lequel le comportement en ligne des utilisateurs est observé, collecté, enregistré ou influencé de manière systématique et automatisée, y compris à des fins publicitaires[236]. Il n'est pas non plus contesté que dans le cadre du RTB les données sont largement collectées auprès de tiers (Data Management Platforms, ou DMP) afin d'analyser ou de prédire la situation économique, la santé, les préférences ou intérêts personnels, la fiabilité ou le comportement, la localisation ou les déplacements des personnes physiques[237].

516. Compte tenu du grand nombre de personnes concernées qui entrent en contact avec les sites web et les applications mettant en œuvre le TCF, ainsi que le nombre croissant d'organisations participant au TCF, d'une part, et de l'impact du TCF sur le traitement à grande échelle des données à caractère personnel dans le cadre du RTB, d'autre part, la Chambre Contentieuse constate que, conformément à la décision n° 01/2019, la défenderesse est bien soumise à l'obligation de réaliser une analyse d'impact sur la protection des données, en application de l'article 35 du RGPD. Par conséquent, il y a violation de l'article 35 RGPD.

h. Désignation du délégué à la protection des données (art. 37 RGPD)

517. L'article 37 du RGPD prévoit l'obligation de désigner un délégué à la protection des données (DPD) dans les cas où :

   i. le traitement est effectué par une autorité publique ou un organisme public ; ou

   ii. un responsable du traitement ou un sous-traitant est principalement chargé des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, nécessitent un suivi régulier et systématique à grande échelle des personnes concernées; ou

[235] Décision du Secrétariat Général n° 01/2019 du 16 janvier 2019, disponible sur le site internet de l'APDhttps://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf.
[236] Décision du secrétariat général n° 01/2019 du 16 janvier 2019, para. 6.8).
[237] Décision du secrétariat général n° 01/2019 du 16 janvier 2019, para. 6.3).

iii. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données à caractère personnel visées à l'article 9 du RGPD et de données à caractère personnel relatives aux condamnations pénales et aux infractions visées à l'article 10 du RGPD.

518. La Chambre Contentieuse a déjà conclu que la défenderesse traite des données à caractère personnel en raison du fait qu'IAB Europe, en sa qualité de *Managing Organization*, peut avoir accès aux TC Strings et aux *records of consent*[238].

519. L'ancien Groupe de travail « Article 29 » indique que les activités de traitement qui sont nécessaires pour atteindre les objectifs du responsable du traitement ou du sous-traitant peuvent être considérées comme des activités de base au sens de l'article 37 du RGPD. La Chambre Contentieuse estime que, compte tenu de l'importance du TCF pour la défenderesse, des objectifs déclarés du TCF ainsi que du traitement associé de données à caractère personnel en sa qualité de *Managing Organization*, le traitement dans le cadre du TCF fait partie des activités de base d'IAB Europe.

520. En ce qui concerne la notion de « traitement à grande échelle », le Groupe de travail « Article 29 » précise qu'il faut notamment tenir compte des éléments suivants :

i. le nombre de personnes concernées - soit comme un nombre spécifique, soit comme une proportion de la population concernée ;
ii. la quantité de données et/ou la gamme des différentes données traitées ;
iii. la durée ou la permanence du traitement des données ;
iv. l'étendue géographique de l'activité de traitement.

En l'espèce, la Chambre Contentieuse constate que le TCF est proposé dans différents États membres ; que le TCF exige intrinsèquement que les données à caractère personnel des utilisateurs soient traitées sous la forme d'une TC String aussi longtemps que cela est nécessaire pour pouvoir démontrer que le consentement a été obtenu conformément aux *TCF Policies* ; et que les données à caractère personnel traitées sont en outre partagées avec de nombreux fournisseurs adtech. La Chambre Contentieuse en conclut que le TCF implique un traitement à grande échelle de données à caractère personnel.

521. Pour ce qui est du critère de l'observation régulière et systématique, le WP29 interprète le terme « régulier » d'une ou plusieurs des manières suivantes :

i. quelque chose qui se produit continuellement ou à des moments précis pendant une certaine période de temps ;
ii. quelque chose qui se produit de manière récurrente ou répétitive à des moments fixes ; ou

[238] Voir para. 358 et 468 de la présente décision.

iii. quelque chose qui se produit constamment ou périodiquement.

La Chambre Contentieuse estime que l'obligation contractuelle pour les *fournisseurs adtech* et les CMP de mettre à disposition de la défenderesse des « records of consent », en sa qualité de *Managing Organization*, sur simple demande d'IAB Europe, relève du point (i). Il y a donc une observation régulière des données relatives aux utilisateurs identifiables.

522. Le terme « systématique » doit être compris dans l'une ou plusieurs des acceptions suivantes :

i. quelque chose qui se produit selon un système ;
ii. prédisposé, organisé ou méthodique ;
iii. quelque chose qui se produit dans le cadre d'un programme général de collecte de données ; ou
iv. une action menée dans le cadre d'une stratégie.

523. Une fois de plus, la Chambre Contentieuse estime que le traitement des TC Strings ou des *records of consent* par la défenderesse dans la version actuelle du TCF répond au moins aux trois premiers critères. Par conséquent, la Chambre Contentieuse juge que le TCF doit être considéré comme une observation régulière et systématique d'utilisateurs identifiables.

524. Sur la base des éléments qui précèdent, la Chambre Contentieuse conclut qu'IAB Europe aurait dû désigner un DPD, conformément à l'article 37 du RGPD. Par conséquent, il y a violation de l'article 37 RGPD.

C. Sanction

525. À titre préliminaire, et comme développé ci-dessous, la Chambre Contentieuse note que la présente décision sur le TCF ne traite pas directement des déficiences du cadre plus large de l'OpenRTB. Toutefois, la Chambre Contentieuse attire l'attention sur les risques importants que l'OpenRTB fait peser sur les droits et libertés fondamentaux des personnes concernées, notamment en raison de la grande quantité de données à caractère personnel concernées, des activités de profilage, de la prédiction du comportement et de la surveillance qui en découle (voir A.3.1). Dans la mesure où le TCF est l'outil sur lequel OpenRTB s'appuie pour justifier sa conformité au RGPD, la TC String joue un rôle central dans l'architecture actuelle du protocole OpenRTB

526. Aux termes de l'article 100 LCA, la Chambre Contentieuse a le pouvoir de :

> 1° classer la plainte sans suite ;
> 2° ordonner le non-lieu ;
> 3° prononcer une suspension du prononcé ;
> 4° proposer une transaction ;
> 5° formuler des avertissements ou des réprimandes ;
> 6° ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits ;
> 7° ordonner que l'intéressé soit informé du problème de sécurité ;
> 8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement ;
> 9° ordonner une mise en conformité du traitement ;
> 10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données ;
> 11° ordonner le retrait de l'agréation des organismes de certification ;
> 12° imposer des astreintes ;
> 13° imposer des amendes administratives ;
> 14° ordonner la suspension des flux transfrontaliers de données vers un autre État ou un organisme international ;
> 15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier ;
> 16° décider, au cas par cas, de publier ses décisions sur le site internet de l'Autorité de protection des données.

527. Quant à l'amende administrative qui peut être imposée en vertu de l'article 83 du RGPD et des articles 100, 13° et 101 LCA, l'article 83 du RGPD prévoit :

> « *1.* Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;

b) le fait que la violation a été commise délibérément ou par négligence ;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

g) les catégories de données à caractère personnel concernées par la violation ;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.».

528. Le considérant 150 du RGPD[239] établit une distinction supplémentaire selon que le contrevenant est une entreprise ou non. Dans la première hypothèse, le critère (montant fixe ou pourcentage) pour atteindre l'amende la plus élevée devrait être appliqué. Lorsque, en revanche, l'auteur de l'infraction n'est pas une entreprise, il convient de tenir compte de la situation économique de l'auteur et du niveau général des revenus dans l'État membre concerné. Il s'agit d'éviter l'imposition d'amendes qui pourraient être disproportionnées.

[239] Considérant 150 du RGPD : « [...] Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. ...] ».

529. Il est important de contextualiser les manquements de la défenderesse afin d'identifier les mesures correctives les plus appropriées. Dans ce contexte, la Chambre Contentieuse tiendra compte de toutes les circonstances de l'affaire, y compris — dans les limites qu'elle précise ci-dessous — de la réaction présentée par la défenderesse aux sanctions envisagées et communiquées par le biais du formulaire de sanction[240]. À cet égard, la Chambre Contentieuse précise que le formulaire qu'elle a envoyé mentionne expressément que cela n'implique pas de réouverture des débats. Son seul but est de recueillir la réaction de la défenderesse aux sanctions prévues.

530. Alors que des mesures telles qu'un ordre de mise en conformité ou une interdiction de traitement ultérieur peuvent mettre fin à une infraction identifiée, des amendes administratives, telles que définies au considérant 148 du RGPD, sont imposées en cas d'infractions graves, en plus ou à la place des mesures appropriées qui sont nécessaires pour remédier à l'infraction.

531. La Chambre Contentieuse tient également à rappeler qu'il lui appartient souverainement, en tant qu'autorité administrative indépendante — dans le respect des articles pertinents du RGPD et de la LCA — de déterminer la ou les mesure(s) corrective(s) et sanction(s) appropriée(s). Ceci découle de l'article 83 du RGPD, mais aussi de la Cour des Marchés qui a souligné l'existence d'une large marge de manœuvre dans sa jurisprudence, entre autres dans son arrêt du 7 juillet 2021.[241]

532. La Chambre Contentieuse constate que les plaignants formulent diverses demandes de sanctions à l'encontre de la défenderesse. Toutefois, il n'appartient pas aux plaignants de demander à la Chambre Contentieuse d'ordonner une mesure corrective ou une sanction particulière, et il n'incombe pas à la Chambre Contentieuse de motiver son refus de l'une des demandes formulées par les plaignants[242]. Ces considérations laissent néanmoins intacte l'obligation incombant à la Chambre Contentieuse de motiver le choix des mesures et sanctions qu'elle juge appropriées (parmi la liste des mesures et sanctions mises à sa disposition par l'article 58 du RGPD et l'article 100 de la LCA) pour condamner la défenderesse.

533. En l'espèce, la Chambre Contentieuse note que les plaignants demandent à la Chambre Contentieuse de prendre les mesures et sanctions suivantes. Ces propositions sont intégrées ci-dessous à titre d'information (traduction libre) :

> « *1) En application de l'article 100, §1, 8° de la LCA :*
>
> *a. interdire à IAB Europe le traitement de la TC String dans le TCF ;*

[240] Voir para. 534 ainsi que 272 et seq.

[241] Cour d'appel de Bruxelles, section de la Cour des Marchés, 19e chambre A, section des affaires du marché, 2021/AR/320, p. 37-47.

[242] Cour des Marchés, 1er décembre 2021, FOD Financiën c. GBA, nr. 2021/AR/1044, para. 25

b. *interdire à IAB Europe le traitement dans le TCF de toutes les données à caractère personnel associées au traitement de la TC String, telles que les adresses IP, les sites web visités et les applications utilisées ;*
c. *ordonner à IAB Europe le retrait permanent de son site web et de ses autres canaux de communication publics de tous les documents, fichiers et enregistrements qui, de quelque manière que ce soit, incitent ou obligent un tiers à effectuer un tel traitement ;*

2) En application de l'article 100, §1, 10° de la LCA, ordonner à IAB Europe d'effacer définitivement toutes les TC Strings et autres données à caractère personnel déjà traitées dans le cadre du TCF de tous ses systèmes informatiques, fichiers et supports de données, ainsi que des systèmes informatiques, fichiers et supports de données des sous-traitants contractés par IAB Europe ;

3) En application de l'article 100, §1, 10° de la LCA, ordonner à IAB Europe d'informer tous les destinataires des données à caractère personnel traitées dans le TCF de l'ordonnance imposée par la Chambre Contentieuse, en ce compris :

a. *l'interdiction du traitement de la TC String dans le TCF ;*
b. *l'interdiction du traitement dans le TCF de toutes les données à caractère personnel associées du traitement TC String, telles que les adresses IP, les sites web visités et les applications utilisées ;*
c. *l'ordonnance de suppression définitive de tous les TC Strings et autres données à caractère personnel déjà traitées dans le cadre du TCF de tous les systèmes informatiques, fichiers et supports de données ;*

et ce, de manière clairement visible et lisible dans un encadré en gras en haut de la page d'accueil du site Internet d'IAB Europe www.iabeurope.eu dans la police et la taille habituelles jusqu'à 6 mois après qu'un jugement de la Cour des marchés soit devenu définitif, le cas échéant conformément à l'article 108 LCA, ou par courrier électronique, dans les deux cas avec un hyperlien vers la version anglaise de la décision de la Chambre Contentieuse sur le site Internet de l'APD;

4) En application de l'article 100, §1, 12° LCA au nom de IAB Europe ordonner la confiscation d'une astreinte de 25 000 euros par jour civil entamé de retard dans l'exécution de toute mesure imposée dans la décision interlocutoire de la Chambre Contentieuse à compter de l'expiration de sept jours civils après la décision interlocutoire de la Chambre Contentieuse. »

534. Un formulaire de sanction a été envoyé à la défenderesse le 11 octobre 2021. IAB Europe a soumis sa réponse le 1er novembre 2021[243]. Cette réponse a été prise en compte dans les paragraphes suivants.

[243] Voir titre A.10. – Formulaire de sanction, procédure de coopération européenne, et publication de la décision, *supra*.

C.1. - Violations

535. La Chambre Contentieuse a constaté que la défenderesse avait violé les articles suivants :

- **Articles 5.1.*a*** et **6** du RGPD — Le TCF actuel ne fournit pas de base juridique pour le traitement des préférences des utilisateurs sous la forme d'une TC String. En outre, la Chambre Contentieuse note que le TCF propose deux fondements juridiques pour le traitement des données à caractère personnel par les fournisseurs adtech participants, mais constate qu'aucune d'entre eux ne peut être utilisé. Premièrement, le consentement des personnes concernées n'est actuellement pas donné de manière suffisamment spécifique, informée et granulaire. Deuxièmement, les intérêts des personnes concernées l'emportent sur l'intérêt légitime des organisations participant au TCF, compte tenu du traitement à grande échelle des préférences des utilisateurs (collectés sous le TCF) dans le cadre du protocole OpenRTB et de l'impact que cela peut avoir sur ceux-ci. Étant donné qu'aucun des motifs de licéité énoncés à l'article 6 du RGPD ne s'applique à ce traitement, comme expliqué ci-dessus[244], la défenderesse enfreint les articles 5.1.*a* et 6 RGPD.

  Prenant acte du fait que la défenderesse elle-même n'a plus de contrôle factuel ou technique sur les TC Strings une fois que ceux-ci ont été générés par les CMP et stockés sur les appareils des utilisateurs[245], la Chambre Contentieuse constate qu'elle ne peut pas imposer à la défenderesse la suppression *a posteriori* de tous les TC Strings générés jusqu'à présent. Plus précisément, il incombe aux CMP et aux publishers qui mettent en œuvre le TCF[246] de prendre les mesures appropriées, conformément aux articles 24 et 25 du RGPD, en veillant à ce que les données à caractère personnel qui ont été collectées en violation des articles 5 et 6 du RGPD ne soient plus traitées et supprimées en conséquence. Dans la mesure où IAB Europe stocke encore des TC Strings provenant des cookies de consentement à portée globale, qui ne sont plus pris en charge, la Chambre Contentieuse estime également que les mesures nécessaires doivent être prises par la défenderesse pour garantir l'effacement permanent de ces données à caractère personnel qui ne sont plus nécessaires.

- **Articles 12**, **13**, and **14 RGPD** — Comme développé ci-dessus (voir B.4.2. - Obligation de transparence envers les personnes concernées (articles 12, 13 et 14 du RGPD), la façon dont les informations sont fournies aux personnes concernées ne répond pas à l'exigence d'une « manière transparente, compréhensible et facilement accessible ». Les utilisateurs d'un site web ou d'une application participant au TCF ne reçoivent pas d'informations suffisantes sur les catégories de données à caractère personnel

[244] B.4.1 - Licéité et loyauté du traitement (art. 5.1.a et 6 du RGPD)

[245] Conformément aux Policies obligatoires et aux spécifications techniques établies et imposées aux participants du TCF par IAB Europe.

[246] En outre, la Chambre Contentieuse souligne le fait qu'aucun des CMP et des fournisseurs n'a pris part à la présente procédure.

collectées à leur sujet, et ne sont pas en mesure de déterminer à l'avance la portée et les conséquences du traitement. Les informations données aux utilisateurs sont trop générales pour refléter le traitement spécifique de chaque fournisseur adtech, ce qui empêche également la granularité — et donc la validité — du consentement reçu pour le traitement effectué dans le cadre du protocole OpenRTB. Les personnes concernées ne sont pas en mesure de déterminer à l'avance la portée et les conséquences du traitement, et ne disposent donc pas d'un contrôle suffisant sur le traitement de leurs données pour éviter d'être surprises ultérieurement par un traitement ultérieur de leurs données à caractère personnel.

- **Articles 24**, **25**, **5.1.*f*** et **32 RGPD** — Comme expliqué c*i-dessus*[247], sur la base des articles 5.1.*f* et 32 RGPD, le responsable du traitement est tenu d'assurer la sécurité du traitement et l'intégrité des données à caractère personnel traitées. La Chambre Contentieuse rappelle que la lecture combinée des articles 5.1.*f* et 32, ainsi que 5.2 et 24 RGPD (principe de responsabilité) impose au responsable du traitement de démontrer son respect de l'article 32, en mettant en place des mesures techniques et organisationnelles appropriées, de manière transparente et traçable. Dans le cadre du système TCF actuel, les fournisseurs adtech reçoivent un signal de consentement sans qu'aucune mesure technique ou organisationnelle ne permette de garantir que ce signal de consentement est valide ou qu'un fournisseur adtech l'a effectivement reçu (plutôt que généré). En l'absence de systèmes de contrôle systématiques et automatisés des CMP et des fournisseurs adtech participants par la défenderesse, l'intégrité de la TC String n'est pas suffisamment assurée, puisqu'il est possible pour les CMP de falsifier le signal afin de générer un cookie *euconsent-v2* et de reproduire ainsi un « faux consentement » des utilisateurs à toutes fins et pour tous types de partenaires. Comme indiqué ci-dessus[248], cette hypothèse est d'ailleurs spécifiquement couverte par les conditions d'utilisation du TCF. La Chambre Contentieuse constate donc qu'IAB Europe, en sa qualité de *Managing Organization*, a conçu et fournit un système de gestion du consentement, mais ne prend pas les mesures nécessaires pour assurer la validité, l'intégrité et la conformité des préférences et du consentement des utilisateurs.

  La Chambre Contentieuse constate également que la version actuelle du TCF ne facilite pas l'exercice des droits de la personne concernée, notamment en tenant compte de la relation de responsabilité conjointe du traitement entre l'éditeur, la CMP mise en place et la défenderesse. La Chambre Contentieuse souligne également que le RGPD exige que les droits des personnes concernées puissent être exercés vis-à-vis de chacun des responsables conjoints du TCF de manière à respecter les articles 24 et 25 du RGPD.

[247] Voir titre B.4.3. - Responsabilité (art. 24 RGPD), protection des données dès la conception et par défaut (art. 25 RGPD), intégrité et confidentialité (art. 5.1.f RGPD), et sécurité du traitement (art. 32 RGPD)
[248] Voir para. 485 de la présente décision.

Au vu de ce qui précède, la Chambre Contentieuse constate que la défenderesse a manqué à ses obligations de sécurité du traitement, d'intégrité des données à caractère personnel et de protection des données dès la conception et par défaut (articles 24, 25, 5.1.*f* et 32 RGPD).

- **Article 30 RGPD** — Comme développé ci-dessus[249], la Chambre Contentieuse ne peut suivre l'argument de la défenderesse selon lequel elle estime pouvoir bénéficier des exceptions à l'obligation de tenir un registre de ses activités de traitement, telles que prévues à l'article 30.5 RGPD. Étant donné que le registre des activités de traitement de la défenderesse ne contient aucun traitement relatif au TCF, hormis la gestion des membres et l'administration du TCF, et ce, alors qu'IAB Europe est en mesure accéder aux *records of consent* en tant que *Managing Organization*, la Chambre Contentieuse constate l'infraction à l'article 30 du RGPD dans le chef de la défenderesse.
- **Article 35 GDPR** — Compte tenu du grand nombre de personnes concernées qui entrent en contact avec les sites web et les applications mettant en œuvre le TCF, ainsi que les organisations participant au TCF, d'une part, et de l'impact du TCF sur le traitement à grande échelle des données à caractère personnel à travers le protocole OpenRTB, d'autre part, la Chambre Contentieuse constate que IAB Europe n'a pas réalisé d'analyse d'impact relative à la protection des données (AIPD) complète relative au traitement des données à caractère personnel au sein du TCF, et a donc violé l'article 35 RGPD. La Chambre Contentieuse constate que le TCF a été développé, entre autres, pour le système RTB, dans lequel le comportement en ligne des utilisateurs est observé, collecté, enregistré ou influencé de manière systématique et automatisée, y compris à des fins publicitaires. Il n'est pas non plus contesté qu'au sein du RTB, les données sont largement collectées auprès de tiers (DMP) afin d'analyser ou de prédire la situation économique, la santé, les préférences ou intérêts personnels, la fiabilité ou le comportement, la localisation ou les déplacements des personnes physiques.
- **Article 37 RGPD**— En raison de l'observation à grande échelle, régulière et systématique d'utilisateurs identifiables qu'implique le TCF, et compte tenu du rôle de la défenderesse, plus précisément de sa qualité de *Managing Organization*, la Chambre Contentieuse juge qu'IAB Europe aurait dû désigner un délégué à la protection des données (DPD). En ne le faisant pas, la défenderesse enfreint l'article 37 du RGPD.

C.2. - Sanctions

536. Par conséquent, la Chambre Contentieuse condamne la défenderesse :

I. À rendre le TCF conforme aux obligations de licéité, de loyauté et de transparence (articles 5.1.*a* et 6 RGPD), en établissant une base juridique pour le traitement ainsi

[249] Voir para. 507 *et s*. de la présente décision.

que le partage des préférences des utilisateurs dans le cadre du TCF, sous la forme d'une TC String et d'un cookie *euconsent-v2* placés sur les appareils des utilisateurs à cette fin. Ces obligations impliquent également que toute donnée à caractère personnel collectée jusqu'à présent au moyen d'une TC String dans le cadre des consentements à portée globale, qui ne sont désormais plus pris en charge par IAB Europe, doit être supprimée par la défenderesse sans délai injustifié. En outre, la Chambre Contentieuse ordonne à la défenderesse d'interdire l'utilisation de l'intérêt légitime comme fondement juridique du traitement par les organisations participant au TCF dans son format actuel, par l'entremise des conditions d'utilisation du TCF.

II. À rendre le TCF conforme aux obligations de transparence et d'information (articles 12, 13 et 14 du RGPD), en exigeant que les CMP enregistrées auprès du TCF adoptent une approche harmonisée et conforme au RGPD à l'égard des informations à fournir aux utilisateurs via leur interface. Ces informations, qui portent sur les catégories de données collectées, les finalités de leur collecte et les fondements juridiques applicables au traitement, doivent être précises, concises et compréhensibles afin d'éviter que les utilisateurs soient surpris par le traitement ultérieur de leurs données à caractère personnel par d'autres parties que les publishers ou IAB Europe.

III. À assurer la conformité du TCF avec les obligations d'intégrité et de sécurité, ainsi que la protection des données dès la conception et par défaut (consacrées aux articles 5.1.*f* et 32 RGPD, et 25 RGPD). À cet égard, la Chambre Contentieuse ordonne d'inclure des mesures de contrôle techniques et organisationnelles efficaces pour faciliter l'exercice des droits des personnes concernées et pour garantir l'intégrité de la TC String, compte tenu de la possibilité, dans l'état actuel du système, de falsifier le signal. Un exemple de mesures à mettre en place en vertu de l'article 32 du RGPD est un processus de vérification strict pour les organisations participant au TCF. La Chambre Contentieuse rappelle à la défenderesse, ainsi qu'aux autres responsables conjoints du traitement, leur obligation de prendre les dispositions nécessaires afin de garantir, entre autres, que les personnes concernées puissent effectivement exercer leurs droits. Enfin, dans le cadre de l'article 25 du RGPD, la défenderesse est tenue, via ses conditions d'utilisation, d'interdire aux organisations participant à la version actuelle du TCF d'activer un consentement par défaut, ainsi que de fonder la licéité des activités de traitement envisagées sur l'intérêt légitime.

IV. À assurer la conformité du registre des activités de traitement effectuées dans le cadre du TCF, et en particulier concernant le traitement des préférences et du

consentement des utilisateurs sous la forme d'une TC String et le placement d'un cookie *euconsent-v2* sur leurs appareils.

V. À réaliser une analyse d'impact relative à la protection des données (AIPD), couvrant à la fois les activités de traitement de données à caractère personnel au titre du TCF, et l'impact de ces activités sur le traitement ultérieur sur base du protocole OpenRTB.

VI. À désigner un délégué à la protection des données (DPD), chargé, *entre autres*, de veiller à la conformité des activités de traitement des données personnelles dans le cadre du TCF, conformément aux articles 37 à 39 du RGPD.

537. Ces mesures de mise en conformité devront être réalisées dans un délai maximum de six mois après la validation d'un plan d'action par l'Autorité belge de protection des données, qui sera soumis à la Chambre Contentieuse dans les deux mois qui suivent cette décision. Sur la base de l'article 100 § 1er, 12° de la LCA, une astreinte de 5 000 EUR par jour sera due en cas de non-respect des délais susmentionnés.

538. Outre cette injonction de mise en conformité, la Chambre Contentieuse considère qu'une amende administrative est justifiée en l'espèce pour les raisons suivantes, analysées sur la base de l'article 83.2 RGPD.

539. Les principes de licéité, d'équité, de transparence et de sécurité font partie de l'essence du RGPD, et les violations de ces droits sont passibles des amendes les plus élevées, conformément à l'article 83.5 RGPD. À cet égard, le non-respect des principes fondamentaux de la protection des données doit être sanctionné par des amendes au montant proportionné, selon les circonstances de l'affaire. Dans ce sens, on peut se référer aux lignes directrices sur l'application et la fixation des amendes administratives, selon lesquelles :

> « *Les amendes sont un instrument important que les autorités de contrôle devraient utiliser dans les circonstances appropriées. Les autorités de contrôle sont encouragées à adopter une approche mûrement réfléchie et équilibrée lorsqu'elles appliquent des mesures correctives afin de réagir à la violation d'une manière tant effective et dissuasive que proportionnée. Il ne s'agit pas de considérer les amendes comme un recours ultime ni de craindre de les imposer, mais, en revanche, elles ne doivent pas non plus être utilisées de telle manière que leur efficacité s'en trouverait amoindrie.* »[250]

540. Dans le point (*a*), l'article 83.2 mentionne « la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ».

[250] Groupe de travail Article 29 - Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679 (WP 253), p. 7.

541. S'agissant de la nature et de la gravité des manquements, la Chambre Contentieuse relève que les principes de licéité (articles 5.1.*a* et 6 RGPD), de transparence (articles 12 à 14 RGPD) ainsi que de sécurité (articles 5.1.*f* et 32 RGPD) sont des principes fondamentaux du régime de protection mis en place par le RGPD. Le principe d'imputabilité (accountability) énoncé à l'article 5.2 du RGPD et développé à l'article 24 est également au cœur du RGPD et reflète le changement de paradigme induit par le RGPD, à savoir le passage d'un régime fondé sur des déclarations et autorisations préalables par l'autorité de contrôle à une plus grande imputabilité et responsabilité du responsable du traitement. Le respect de ses obligations par ce dernier et sa capacité à le démontrer n'en sont donc que plus importants.

542. Une base juridique valide et une information transparente sont des éléments essentiels du droit fondamental à la protection des données. Pour ce qui est de la transparence, ce principe constitue un « portail » permettant de renforcer le contrôle des personnes concernées sur leurs données à caractère personnel ainsi que l'exercice des autres droits accordés aux personnes concernées par le RGPD, tels que le droit d'opposition et le droit d'effacement. Les violations de ces principes constituent des infractions graves, qui peuvent faire l'objet des amendes administratives les plus élevées prévues par le RGPD

543. La violation de l'article 25, relatif à l'obligation de protection des données dès la conception et par défaut, ainsi que de l'article 30, relatif à la tenue d'un registre des activités de traitement, constituent également des infractions importantes, notamment au vu de l'ampleur des opérations de traitement et de l'impact sur la vie privée des plaignants ainsi que des autres utilisateurs confrontés à des sites web ou des applications mettant en œuvre le TCF.

544. Pour ce qui est de la nature et la finalité du traitement, et plus particulièrement la nature des données, la Chambre Contentieuse note que la TC String, en tant qu'expression des préférences des utilisateurs concernant les finalités du traitement et les fournisseurs adtech potentiels mis en avant par l'interface de la CMP, constitue la pierre angulaire du TCF. Bien que le champ d'application de cette décision soit le TCF et la TC String, et bien que la sanction imposée à la défenderesse concerne uniquement ce cadre, la conformité du protocole OpenRTB avec le RGPD est évaluée dans le cadre d'une analyse holistique du TCF et de son interaction avec le premier. Dans la mesure où la version actuelle du TCF est l'outil sur lequel l'OpenRTB s'appuie pour justifier sa conformité au RGPD, et dès lors que la défenderesse facilite l'adhésion à et l'utilisation de l'OpenRTB par un nombre important d'organisations participantes, la Chambre Contentieuse constate qu'IAB Europe joue un rôle pivot en ce qui concerne l'OpenRTB, sans être un responsable du traitement des données dans ce contexte.

545. En ce qui concerne la portée du traitement contesté et le nombre de personnes concernées, la Chambre Contentieuse constate que le TCF (dans son format actuel), tel qu'il a été développé par la défenderesse (représentant de grands acteurs du secteur de la

publicité comportementale en ligne[251]), offre un service unique sur le marché. La portée du TCF est donc essentielle, étant donné le nombre croissant de partenaires qui y ont adhéré. En ce qui concerne le niveau de préjudice subi par les personnes concernées, la Chambre Contentieuse souligne une fois de plus que la TC String joue un rôle central dans l'architecture actuelle du protocole OpenRTB. Dès lors, la TC String soutient un système présentant des risques importants que l'OpenRTB fait peser sur les droits et libertés fondamentaux des personnes concernées, notamment en raison de la grande quantité de données à caractère personnel concernées, des activités de profilage, de la prédiction du comportement et de la surveillance qui en découle (voir A.3.1).

546. En ce qui concerne la durée de l'infraction, la Chambre Contentieuse prend note que le TCF est proposé par la défenderesse depuis le 25 avril 2018 comme un mécanisme permettant d'obtenir le consentement des utilisateurs à l'égard de finalités de traitement prédéterminées, et de transférer leurs données à caractère personnel à des participants au TCF, y compris des fournisseurs adtech. Nonobstant les différentes itérations du cadre, qui a été mis à niveau vers la deuxième version du TCF le 21 août 2019, et compte tenu des déficiences systémiques du TCF au regard du RGPD, la Chambre Contentieuse constate que les manquements existent au moins depuis mai 2018, en ce qui concerne la validité du consentement recueilli et le placement d'une String TC sans base juridique valable, et depuis août 2019 pour le recours à l'intérêt légitime comme base juridique en vue de traiter les données à caractère personnel des personnes concernées.

547. L'article 83.2.*b* RGPD requiert de l'APD qu'elle tienne compte du caractère intentionnel ou négligent de l'infraction. Constatant que la défenderesse, en sa qualité de *Managing Organization*, était consciente[252] des risques liés au non-respect du TCF, notamment en ce qui concerne l'intégrité de la TC String et les choix et préférences encapsulés des utilisateurs, et compte tenu de l'impact de la TC String sur les traitements ultérieurs dans le cadre de l'OpenRTB, la Chambre Contentieuse estime qu'IAB Europe a fait preuve de négligence dans l'établissement des mesures régissant la mise en œuvre de la version actuelle du TCF.

548. Dans son point *(c)*, l'article 83.2 RGPD vise les actions potentielles prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées. La Chambre Contentieuse constate l'absence de mesures concrètes prises ou introduites par la défenderesse afin d'atténuer le préjudice subi par les personnes concernées (à savoir le traitement de leurs données à traitement personnel indépendamment de leurs choix, ou en l'absence d'une base juridique valable).

[251] Voir para. 36.
[252] Voir para. 485

549. L'article 83.2*d* du RGPD concerne le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32.

550. Même si la Chambre Contentieuse ne tient pas compte dans la présente décision des développements survenus après la clôture de la procédure en juin 2021, elle prend note que la défenderesse a annoncé lors de l'audience[253] son intention d'introduire un « TCF Vendor Compliance Programme » en septembre 2021, à travers lequel des audits des organisations participant au TCF (figurant sur la *Global Vendors List*) seront mis en place.

551. La Chambre Contentieuse encourage toutes les mesures visant à assurer la conformité avec le RGPD. Néanmoins, comme expliqué aux para. 487-488, compte tenu de l'absence de contrôle systématique par la défenderesse du respect des règles du TCF par les organisations participantes au moment de l'introduction des plaintes, et compte tenu de l'impact significatif de telles violations (par exemple en cas de falsification ou de modification de la TC String), la Chambre Contentieuse considère que l'annonce de cette initiative visant à accroître le respect de l'une de ses obligations en tant que responsable du traitement du TCF et consistant en des audits de fournisseurs adtech figurant sur la *Global Vendors List* démontre que le TCF n'était pas conforme aux obligations de sécurité de la défenderesse, y compris l'obligation de minimiser les dommages subis par les personnes concernées. Aucune autre action n'a été communiquée par la défenderesse à la Chambre Contentieuse à cet égard.

552. Par ailleurs, la Chambre Contentieuse n'est plus en mesure d'examiner la nature de ce programme et, en tout état de cause, ce nouveau programme ne change pas la nature des manquements au RGPD survenus jusqu'à la clôture des débats en juin 2021.

553. À la lumière de l'article 83.2.*e* du RGPD, la Chambre Contentieuse note l'absence, au moment de la présente décision, de toute décision finale d'autres autorités de surveillance compétentes, concernant des infractions pertinentes antérieures par la défenderesse en relation avec le TCF.

554. L'article 83.2.*f* du RGPD concerne le degré de coopération établi avec l'autorité, en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs. À cet égard, la Chambre Contentieuse ne partage pas la conclusion du Service d'Inspection selon laquelle la défenderesse n'a pas suffisamment coopéré avec le premier, hormis la fourniture et la remise du registre des activités de traitement opérées par IAB Europe.

555. Pour ce qui est des catégories de données à caractère personnel concernées par l'infraction (article 83.2.*g* du RGPD), la Chambre Contentieuse reconnaît que les données à caractère personnel contenues dans et traitées au moyen de la TC String sont en

[253] Et confirmé par la défenderesse par une annonce publique sur son site Internet, le 26 août 2021 : https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/.

adéquation avec le principe de minimisation des données, compte tenu de leur nature. Nonobstant ce qui précède, la Chambre Contentieuse réitère sa position selon laquelle le TCF joue un rôle central dans le soutien des opérations de traitement dans le cadre du protocole OpenRTB. Par conséquent, la Chambre Contentieuse conclut qu'il ne peut être exclut que tant les catégories spéciales que les catégories régulières de données à caractère personnel — traitées au moyen d'une *bid request* à laquelle la TC String est jointe — puissent être affectées par les infractions commises en vertu du TCF.

556. Pour ce qui est de l'article 83.2.*h* du RGPD, la Chambre Contentieuse note que ce critère n'est pas pertinent en l'espèce.

557. L'article 83.2.*i* du RGPD n'est pas applicable en l'absence de toute décision finale antérieure à cet égard, prise à l'encontre de la défenderesse.

558. L'article 83.2.*j* du RGPD concerne l'adhésion à des codes de conduite approuvés ou à des mécanismes de certification approuvés. Dans ce contexte, la Chambre Contentieuse note que IAB Europe a déjà été en contact avec l'Autorité belge de protection des données concernant la rédaction et l'adoption d'un code de conduite (au moment où la procédure était déjà en cours). La Chambre Contentieuse souligne également l'absence de suivi de la défenderesse à cet égard depuis juin 2020, sans autre explication de sa part.

559. Enfin, l'article 83.2.*k* du RGPD vise toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation. La Chambre Contentieuse n'a pas retenu d'éléments spécifiques susceptibles de modifier le montant de l'amende.

560. Pour déterminer le montant de l'amende administrative, les articles 83.3 à 83.7 du RGPD utilisent le terme « entreprise » qui, sur la base du considérant 150 du RGPD et comme confirmé par le Groupe de travail « Article 29 » et l'EDPB[254], doit être interprété conformément aux articles 101 et 102 du TFUE. Sur la base de la jurisprudence de la CJUE, la notion d'entreprise aux articles 101 et 102 du TFUE fait référence à une entité économique unique, même si cette entité économique est juridiquement constituée de plusieurs personnes physiques ou morales.[255]

561. Pour évaluer si plusieurs entités forment une entité économique unique, il convient de prendre en compte la capacité de chaque entité à prendre des décisions libres. Il convient également d'examiner si une entité dirigeante (la société mère) exerce ou non une influence décisive sur l'autre entité (le montant de la participation, les liens au niveau du personnel ou

[254] Article-29-Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) et confirmé par l'EDPB dans Endorsement 1/2018 le 25 mai 2018 ; ainsi que la décision contraignante 1/2021, para. 292, de l'EDPB.

[255] Arrêt de la CJUE du 23 avril 1991. *Klaus Höfner et Fritz Elser contre Macrotron GmbH*, C-41/90, ECLI:EU:C:1991:161, paragraphe 21, et arrêt de la CJUE du 14 décembre 2006, *Confederación Española de Empresarios de Estaciones de Servicio*, C-217/05, ECLI:EU:C:2006:784, paragraphe 40. 40

de l'organisation, les instructions et l'existence de contrats d'entreprise sont des exemples de critères).

562. La Chambre Contentieuse n'a pas pu trouver d'indication d'une influence décisive d'IAB Inc. sur la défenderesse IAB Europe, ou d'une limitation de sa liberté de décision à l'égard d'IAB Inc.

563. Ceci a également été développé par la défenderesse dans sa réponse au formulaire de sanction, dans laquelle IAB Europe affirme que IAB Inc. n'a aucune participation dans la défenderesse ni aucun droit de regard sur le déploiement des activités d'IAB Europe. La défenderesse a indiqué qu'IAB Inc. (dont le siège est aux États-Unis) concède des licences de la marque « IAB » à d'autres organisations et demeure une entité entièrement séparée et indépendante d'IAB Europe.

564. La Chambre Contentieuse décide donc de se baser sur les seuls revenus financiers d'IAB Europe comme référence pour le calcul de l'amende administrative, au lieu du chiffre d'affaires annuel d'IAB Inc.

565. À cet égard, la Chambre Contentieuse prend note que les bénéfices bruts annuels de la défenderesse se sont élevées à 2.471.467 EUR en 2020[256]. À titre subsidiaire, la Chambre Contentieuse observe également que les organisations participantes sont tenues de payer une cotisation annuelle de 1.200 EUR à la défenderesse lors de leur inscription au TCF[257]. Compte tenu du nombre total de fournisseurs adtech inscrits au TCF, qui a augmenté de manière significative, passant de 420 le 25 mai 2020 à 744 le 7 juin 2021, la Chambre Contentieuse constate donc qu'une grande partie des revenus d'IAB Europe est générée par l'octroi de licences d'utilisation du TCF. Plus précisément, IAB Europe réaliserait un bénéfice brut d'au moins 981.600 EUR pour 2021 avec la seule cotisation annuelle des participants au TCF — y compris les fournisseurs adtech et les CMP[258].

566. En vertu de l'article 83.4, les infractions aux articles 25, 30, 32, 35 et 37 du RGPD peuvent s'élever jusqu'à 10.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

567. En vertu de l'article 83.5 RGPD, les infractions aux articles 5.1.*a*, 5.1.*f*, 6, et 12 à 14 RGPD peuvent s'élever jusqu'à 20.000.000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent. Le montant maximal de l'amende dans ce cas, tel que prévu à l'article 83.5, est donc de 20.000.000 EUR.

[256] Voir les comptes annuels 21/12/2020, disponibles à l'adresse https://cri.nbb.be/bc9/web/catalog?execution=e1s1.

[257] https://iabeurope.eu/wp-content/uploads/2019/08/TCF-Fact-Sheet_General.pdf

[258] Totalisant 74 CMP le 7 juin 2021 : https://iabeurope.eu/cmp-list/. Le bénéfice réel est susceptible d'être plus élevé, compte tenu du nombre toujours croissant de participants au TCF.

568. S'agissant, entre autres, d'atteintes à un droit fondamental consacré par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, l'appréciation de leur gravité sur le fondement de l'article 83.2.*a* RGPD se fera de manière autonome.

569. Sur la base des éléments développés ci-dessus, de la réaction de la défenderesse au formulaire de sanction proposé, ainsi que des critères énumérés à l'article 83.2 RGPD, la Chambre Contentieuse considère que les infractions susmentionnées justifient d'imposer à la défenderesse une ordonnance de mise en conformité assortie d'une amende administrative de 250.000 EUR (article 100, § 1er, 13° et 101 de la LCA), en tant que sanction effective, proportionnée et dissuasive au regard de l'article 83 RGPD. Pour déterminer ce montant, la Chambre Contentieuse a pris en compte le chiffre d'affaires annuel total de la défenderesse, qui s'élevait à 2.471.467 EUR en 2020[259].

570. Le montant de 250.000 EUR reste, au vu des éléments qui précèdent, proportionné aux infractions qui ont été établies par la Chambre Contentieuse. Ce montant est également nettement inférieur au montant maximal de 20.000.000 EUR prévu par l'article 83.5 du RGPD.

571. La Chambre Contentieuse est d'avis qu'une amende plus faible ne répondrait pas, en l'espèce, aux critères requis par l'article 83.1. du RGPD, selon lequel l'amende administrative doit non seulement être proportionnée, mais aussi effective et dissuasive. Ces éléments découlent du principe de coopération loyale décrit au considérant 13 du RGPD (conformément à l'article 4.3 du Traité sur l'Union européenne).

572. Compte tenu de l'importance de la transparence concernant le processus décisionnel de la Chambre Contentieuse et conformément à l'article 100, §1, 16° de la LCA, cette décision est publiée sur le site internet de l'Autorité de protection des données[260]. Compte tenu de la publicité antérieure entourant cette affaire, ainsi que de l'intérêt général pour le public et le nombre important de personnes concernées et d'organisations impliquées, la Chambre Contentieuse a décidé de ne pas supprimer les données d'identification directe des parties et des personnes mentionnées, qu'il s'agisse de personnes physiques ou morales.

[259] Voir les comptes annuels 21/12/2020, disponibles à l'adresse https://cri.nbb.be/bc9/web/catalog?execution=e1s1.
[260] Voir para. 287.

PAR CES MOTIFS,

la Chambre Contentieuse de l'Autorité de protection des données décide, après délibération :

- d'ordonner à la défenderesse, conformément à l'article 100, paragraphe 1, point 9, de la LCA, en vue de mettre le traitement des données à caractère personnel dans le cadre du TCF en conformité avec les dispositions du RGPD :

  a. de fournir une base juridique valable pour le traitement et la diffusion des préférences des utilisateurs dans le cadre du TCF, sous la forme d'une TC String et d'un cookie *euconsent-v2*, ainsi que d'interdire, par le biais des conditions d'utilisation du TCF, l'utilisation d'intérêts légitimes comme base de licéité pour le traitement des données personnelles par les organisations participant au TCF dans sa forme actuelle, conformément aux articles 5.1.*a* et 6 du RGPD ;

  b. d'assurer des mesures de contrôle techniques et organisationnelles efficaces afin de garantir l'intégrité et la confidentialité de la TC String, conformément aux articles 5.1.*f*, 24, 25 et 32 du RGPD ;

  c. de maintenir un audit strict des organisations adhérant au TCF afin de s'assurer que les organisations participantes répondent aux exigences du RGPD, conformément aux articles 5.1.*f*, 24, 25 et 32 du RGPD ;

  d. de prendre des mesures techniques et organisationnelles visant à empêcher que le consentement soit coché par défaut dans les interfaces des CMP ainsi qu'à empêcher l'autorisation automatique des fournisseurs adtech participants fondant leurs opérations de traitement sur l'intérêt légitime, conformément aux articles 24 et 25 du RGPD ;

  e. de contraindre les CMP à adopter une approche uniforme et conforme au RGPD pour les informations qu'elles soumettent aux utilisateurs, conformément aux articles 12 à 14 et 24 du RGPD ;

  f. de mettre à jour le registre actuel des activités de traitement, en incluant le traitement des données personnelles dans le cadre du TCF par IAB Europe, conformément à l'article 30 du RGPD ;

g. de réaliser une analyse d'impact relative à la protection des données (AIPD) en ce qui concerne les activités de traitement effectuées dans le cadre du TCF et leur impact sur les activités de traitement effectuées dans le cadre du protocole OpenRTB, ainsi qu'adapter cette AIPD aux futures versions ou modifications de la version actuelle du TCF, conformément à l'article 35 du RGPD ;

h. de désigner un délégué à la protection des données (DPD) conformément aux articles 37 à 39 du RGPD.

Ces mesures de mise en conformité devront être mises en œuvre dans un délai maximum de six mois après la validation d'un plan d'action par l'Autorité belge de protection des données, qui sera soumis à la Chambre Contentieuse dans les deux mois qui suivent cette décision. Conformément à l'article 100 § 1er, 12° de la LCA, une astreinte de 5.000 EUR par jour sera due en cas de non-respect des délais susmentionnés.

- d'imposer une amende administrative de 250.000 EUR à la défenderesse en vertu de l'article 101 de la LCA.

Cette décision peut faire l'objet d'un recours devant la Cour des Marchés, conformément à l'article 108, § 1 de la LCA, dans un délai de trente jours à compter de sa notification, avec l'Autorité de protection des données comme défenderesse.

(sé.) Hielke HIJMANS
Président de la Chambre Contentieuse