CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Décision n° MED 2022-015 du 2 mars 2022 mettant en demeure la société [redacted] France

(N° MDM221019)

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données, notamment ses articles 56 et 60 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 20 ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-257C du 12 octobre 2020 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification de tout traitement accessible à partir du domaine « [redacted].fr » ou portant sur des données à caractère personnel collectées à partir de ce dernier ;

Vu la saisine n° 20013890 ;

Vu les autres pièces du dossier ;

I. La procédure

La société [redacted] France (ci-après « la société » ou « [redacted] »), dont le siège social est situé [redacted], a une activité de commerce de détail d'articles de sport en magasin spécialisé.

La Commission nationale de l'informatique et des libertés (ci-après « CNIL ») a été saisie, le 19 août 2020 d'une réclamation (n° 20013890) relative au transfert de données à caractère personnel du plaignant, représenté par l'association NOYB - Centre européen pour les droits numériques, vers les États-Unis d'Amérique, collectées lors de sa visite sur le site web https://www.[redacted].fr. 101 réclamations ont d'ailleurs été déposées par NOYB dans les 27 États membres de l'Union européenne et les trois autres États de l'espace économique européen (EEE) à l'encontre de 101 responsables de traitement qui transfèreraient des données à caractère personnel vers les États-Unis.

En application de la décision n° 2020-257C du 12 octobre 2020 de la Présidente de la CNIL, une délégation de la CNIL a procédé, à une mission de contrôle sur pièces, par l'envoi à la société [redacted] France d'un questionnaire le 16 octobre 2020, et d'une demande de

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

compléments du 4 novembre 2020. La société a répondu par courriers des 6 et 30 novembre 2020. Ces questionnaires portaient sur le transfert des données des visiteurs de la version française du site web https://www.[redacted].fr qui intègre la fonctionnalité Google Analytics.

Le 6 novembre 2020, la société a indiqué à la CNIL qu'elle avait pris la décision d'intégrer la fonctionnalité Google Analytics sur son site web https://www.[redacted].fr et que les statistiques obtenues via Google Analytics concernaient des personnes dans plusieurs États membres de l'Union Européenne. Le traitement issu de l'intégration de la fonctionnalité Google Analytics sur son site web apparait donc transfrontalier au sens de l'article 4.23.b) du RGPD.

Dans le cadre de la coopération entre autorités de protection des données, un questionnaire a également été envoyé le 9 mars 2021 par la CNIL à la société Google LLC, sise 1600 Amphitheatre Parkway à Mountain View (CA 94043) aux États-Unis d'Amérique. Celui-ci portait sur la fonctionnalité Google Analytics. Google LLC a répondu par courrier du 9 avril 2021.

Conformément à l'article 56 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après « RGPD » ou « le Règlement »), la CNIL a informé, le 5 août 2021, l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant ce traitement transfrontalier mis en œuvre par la société, compétence tirée par la CNIL de ce que l'établissement principal de la société se trouve en France.

7 autorités sont considérées comme concernées au sens de l'article 4, point 22 du RGPD : les autorités belge, irlandaise, espagnole, italienne, suédoise, hongroise et de Baden-Württemberg.

Le 28 janvier 2022, dans le cadre de la procédure de coopération, un projet de décision a été soumis aux autorités concernées sur le fondement de l'article 60 du RGPD.

Ce projet n'a pas donné lieu à des objections pertinentes et motivées.

II. Sur le traitement en cause et la responsabilité de traitement

Il ressort des réponses de la société [redacted] France transmises à la délégation de contrôle que la société a intégré la fonctionnalité Google Analytics sur le site web https://www.[redacted].fr. Cette fonctionnalité a été mise en place afin de mesurer l'audience du site (volume du trafic, nombre de visiteurs uniques, origine de connexion, typologie de terminal utilisé, taux de conversion des visiteurs en acheteurs…), d'analyser les parcours de visite pour corriger ou améliorer le site, comprendre et avoir de la visibilité sur l'affichage et l'ordonnancement des produits ainsi que sur leur attractivité et enfin mesurer et anticiper les pics de connexion.

Il ressort de la réponse de Google du 9 avril 2021 les éléments suivants.

Tout d'abord, Google précise que, dans le cadre de sa réponse, le terme « Google » désigne, collectivement, Google LLC et Google Ireland Limited, sauf lorsque la distinction est pertinente.

Google Analytics fonctionne par l'inclusion d'un bloc de code JavaScript sur les pages d'un site web. Quand l'utilisateur d'un site visite une page, ce code JavaScript provoque le

chargement d'un fichier JavaScript et exécute alors l'opération de suivi pour Google Analytics. L'opération de suivi consiste en la récupération de données relatives à la requête à travers différents moyens et l'envoi de ces informations aux serveurs Google Analytics.

Les gestionnaires de sites web qui intègrent la fonctionnalité Google Analytics peuvent transmettre des instructions à Google pour le traitement des données collectées via Google Analytics. Ces instructions sont transmises notamment à travers l'outil de gestion des balises qu'ils ont intégré à leur site et à travers le paramétrage de l'outil. En effet, le gestionnaire du site peut choisir différents paramètres afin de fixer, par exemple, la durée de conservation des données. La fonctionnalité Google Analytics permet en outre aux gestionnaires de site de surveiller et entretenir la stabilité de leur site, par exemple en étant informé de certains évènements tels qu'un pic de fréquentation ou, au contraire, le fait qu'il n'y ait pas de trafic du tout. Google Analytics permet également aux gestionnaires de site d'évaluer et d'optimiser l'efficacité des campagnes publicitaires menées à l'aide d'autres outils Google.

Dans ce cadre, Google Analytics collecte notamment la requête http de l'utilisateur, des informations sur son navigateur et sur son système d'exploitation. Google a précisé qu'une requête http, pour n'importe quelle page, contenait des détails sur le navigateur et le terminal qui fait la requête, tels que le nom de domaine et des informations relatives au navigateur telles que son type, son référent (« referer ») et sa langue. Google Analytics dépose et lit des cookies sur le navigateur de l'utilisateur pour permettre d'évaluer la session de l'utilisateur et les autres informations de la requête de page.

Quand ces informations sont collectées, elles sont transmises aux serveurs de Google Analytics. Google a indiqué que l'ensemble des données collectées via Google Analytics étaient hébergées aux États-Unis.

Ainsi, des données collectées sur le site web [redacted].fr via Google Analytics sont transférées aux États-Unis.

Concernant ces transferts, il ressort des pièces du dossier que le contrat qui lie [redacted] et Google Ireland Limited concernant la fonctionnalité Google Analytics fait référence à une annexe intitulée « Google Ads Data Processing Terms ». Cette annexe contient des clauses contractuelles types destinées à encadrer le transfert vers les États-Unis d'Amérique de données à caractère personnel dans le cadre de la fonctionnalité Google Analytics. La société a indiqué ne pas avoir en sa possession d'éléments permettant d'apprécier avec certitude le respect de ces clauses.

Google a fait valoir avoir mis en œuvre des mesures supplémentaires d'ordre juridique, organisationnel et technique pour encadrer les transferts de données dans le cadre de la fonctionnalité Google Analytics.

Il ressort de l'ensemble de ces éléments que la société, en tant que gestionnaire du site web [redacted].fr, a décidé de mettre en œuvre la fonctionnalité Google Analytics sur ce site en insérant un bloc de code JavaScript dans le code source de ce site. La société a précisé avoir mis en œuvre cette fonctionnalité à des fins d'évaluation et d'optimisation de son site.

Il ressort de l'ensemble de ces éléments que la société gestionnaire du site web https://www.[redacted].fr, en décidant de mettre en œuvre la fonctionnalité Google Analytics sur ce site à des fins d'évaluation et d'optimisation, a déterminé les moyens et les finalités de

la collecte et du traitement des données collectées dans le cadre de l'intégration de Google Analytics sur son site web et doit être considérée comme responsable de traitement au sens de l'article 4.7 du RGPD.

III. Sur la qualification de données à caractère personnel

Il convient d'établir que les données collectées dans le cadre de la fonctionnalité Google Analytics et transférées aux États-Unis d'Amérique constituent des données à caractère personnel.

L'article 4.1 du RGPD définit une donnée à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

Il doit être relevé que des identifiants en ligne, tels que les adresses IP ou les informations stockées dans les cookies peuvent être utilisées comme moyens pour identifier un utilisateur, en particulier lorsqu'elles sont combinées avec d'autres types d'informations similaires. Ceci est illustré par le considérant 30 du RGPD qui prévoit qu'un identifiant en ligne associé à une personne physique, tel qu'une adresse IP ou un témoin de connexion, peut « *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* ».

Dans l'hypothèse où le responsable de traitement ferait valoir ne pas avoir la capacité d'identifier l'utilisateur grâce à l'usage de ce type d'identifiants (seuls ou combinés avec d'autres données), il devrait démontrer les moyens mis en œuvre pour s'assurer du caractère anonyme des identifiants collectés. En l'absence d'une telle démonstration, ces identifiants ne sauraient être qualifiés d'anonymes.

Par conséquent, il convient d'examiner dans quelle mesure la mise en œuvre de Google Analytics sur un site web permet au gestionnaire du site web et à Google de rendre une personne concernée (un visiteur du site web en cause) identifiable.

Il ressort des réponses de [redacted] France transmises les 6 et 30 novembre 2020 que les catégories de données suivantes sont traitées dans le cadre de la fonctionnalité Google Analytics :

- des données relatives aux commandes passées, qui ne sont pas directement identifiantes ;
- un identifiant du cookie visiteur Google Analytics ;
- l'adresse IP du visiteur.

La société précise modifier les identifiants des cookies Google Analytics en déterminant un nouvel identifiant aléatoirement. Elle précise également que les derniers octets des adresses IP sont supprimés.

En ce qui concerne les identifiants du visiteur, il doit être relevé qu'il s'agit d'identifiants uniques, qui ont pour finalité de différencier les individus et ainsi de les identifier en permettant aux acteurs en cause de pouvoir les « reconnaître » ultérieurement. La circonstance que les identifiants soient modifiés par le responsable de traitement pour être remplacés par un nouvel identifiant aléatoire ne leur retire pas leur caractère unique, qui permet de suivre une personne dans sa navigation sur un site qui intègre la fonctionnalité Google Analytics.

En l'espèce, ces identifiants peuvent en outre être combinés avec d'autres informations, telles que l'adresse du site visité, les métadonnées relatives au navigateur et au système d'exploitation, l'heure et les données relatives à la visite du site web. En outre, la transmission d'une adresse IP, même tronquée, peut participer à la réidentification ultérieure de la personne concernée. Cette combinaison permet de renforcer leur caractère discriminant dans la mesure où Google dispose de l'ensemble de ces informations associées à l'identifiant unique.

C'est pourquoi, plusieurs éléments lorsqu'ils sont recoupés, peuvent permettre d'individualiser les visiteurs du site web [redacted].fr, sur lequel Google Analytics est mis en œuvre. Il n'est pas nécessaire de connaître le nom ou l'adresse postale du visiteur puisque, conformément au considérant 26 du RGPD, une telle individualisation des personnes peut être suffisante pour les rendre identifiables.

S'il devait en être décidé autrement, la portée du droit à la protection des données, garanti par l'article 8 de la Charte des droits fondamentaux, serait diminuée. En effet, cela permettrait à des sociétés d'individualiser des individus et de leur associer des informations personnelles (telles que leur visite d'un site web spécifique) sans accorder aux individus de protection contre cette individualisation. Une telle appréciation, qui diminuerait le niveau de protection des individus, serait également contraire à la jurisprudence de la Cour de justice de l'Union européenne qui a itérativement jugé que le champ d'application du RGPD avait une définition très large (voir, par exemple, C-439/19, point 61).

Par ailleurs, il ressort des réponses de Google que, dans le cadre de l'utilisation de Google Analytics, et dans certaines conditions de paramétrage du compte Google, Google est informé qu'un utilisateur connecté à son compte Google a visité un site en particulier. Des données à caractère personnel relatives à ce compte sont dès lors collectées, notamment le nom de son utilisateur, et reliées à l'identifiant unique attribué dans le cadre de la fonctionnalité Google Analytics. L'ensemble des données relatives à cet utilisateur peuvent alors être attribuées à une personne identifiée.

Par conséquent, il doit être considéré que les données en cause doivent être considérées comme des données à caractère personnel au sens de l'article 4 du RGPD.

IV. Sur le manquement à l'obligation d'encadrer les transferts de données à caractère personnel hors de l'Union européenne

L'article 44 du RGPD dispose : « *Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent*

chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis. »

Le chapitre V du Règlement prévoit différents instruments pour assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne, en application de l'article 44 de ce texte :

- les décisions d'adéquation (article 45) ;
- les garanties appropriées (article 46) ;

En l'absence d'un niveau de protection équivalent, il institue des dérogations pour des situations particulières (article 49).

En l'espèce, il doit être examiné si les transferts de données en cause vers les États-Unis d'Amérique sont conformes à l'article 44 du Règlement et, en particulier, si ces transferts sont fondés sur l'un des instruments précités et si des mesures appropriées ont été adoptées.

4.1 Les décisions d'adéquation

Dans l'arrêt du 16 juillet 2020 (C-311/18), la Cour de justice de l'Union européenne a invalidé la décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données Union européenne-États-Unis, sans en maintenir les effets.

En l'absence d'une autre décision d'adéquation pertinente, les transferts en cause ne peuvent pas être fondés sur l'article 45 du RGPD.

4.2 Les garanties appropriées

L'article 46.1 du Règlement dispose « *En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.* »

L'article 46.2 du Règlement prévoit que les « *garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par : [...] c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 ;* ».

4.2.1. Les clauses types de protection des données

En l'espèce, la société et Google ont conclu des clauses contractuelles types pour le transfert de données à caractère personnel vers les États-Unis (« Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors »). Ces clauses sont conformes à celles publiées par la Commission européenne dans sa décision 2010/87/EU.

Dans ce contexte, il doit être souligné que les clauses contractuelles types sont un instrument de transfert au sens du Chapitre V du Règlement et n'ont pas été remises en cause en tant que telles par la Cour de justice dans son arrêt du 16 juillet 2020 (C-311/18). Cependant, la Cour a considéré qu'il découlait de la nature contractuelle de ces clauses qu'elles ne pouvaient lier les

autorités des pays tiers. En particulier, la Cour a considéré que : « *S'il existe, dès lors, des situations dans lesquelles, en fonction de l'état du droit et des pratiques en vigueur dans le pays tiers concerné, le destinataire d'un tel transfert est en mesure de garantir la protection des données nécessaire sur la base des seules clauses types de protection des données, il en existe d'autres dans lesquelles les stipulations contenues dans ces clauses pourraient ne pas constituer un moyen suffisant permettant d'assurer, en pratique, la protection effective des données à caractère personnel transférées dans le pays tiers concerné. Tel est le cas, notamment, lorsque le droit de ce pays tiers permet aux autorités publiques de celui-ci des ingérences dans les droits des personnes concernées relatifs à ces données.* » (C-311/18, point 126, soulignement ajouté).

Il n'est cependant pas nécessaire d'analyser plus en détails le cadre légal applicable aux États-Unis d'Amérique dans la mesure où la Cour a déjà procédé à une telle analyse dans l'arrêt précité. En effet, la Cour a constaté, d'une part, que les programmes de surveillance en cause ne correspondaient pas aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité, si bien qu'il n'était pas permis de considérer que les programmes de surveillance fondés sur ces dispositions sont limités au strict nécessaire (point 184). D'autre part, la Cour a constaté que le cadre juridique en cause ne conférait pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, si bien que ces personnes ne disposaient pas d'un droit au recours effectif (point 192).

L'analyse de la Cour de justice est pertinente en l'espèce dans la mesure où Google LLC (en tant qu'importateur de données aux États-Unis) doit être qualifié de fournisseur de communications électroniques au sens de l'article 50 US. Code § 1881(b)(4) et est, par conséquent, sujet à la surveillance par les services de renseignement américains, en application de l'article 50 US. Code § 1881a ("FISA 702"). Google LLC a par conséquent l'obligation de fournir au gouvernement américain les données à caractère personnel qui seraient requises en vertu de FISA 702.

Il ressort du rapport de transparence de Google que Google LLC est régulièrement destinataire de telles demandes d'accès par les services de renseignement des États-Unis d'Amérique.

Ainsi, d'une part, la Cour de justice a déclaré invalide la décision d'adéquation avec les États-Unis d'Amérique, en raison des possibilités d'accès des services de renseignement américains. D'autre part, les clauses contractuelles types ne peuvent, à elles seules, assurer un niveau de protection suffisant tel qu'exigé par l'article 44 du RGPD dans la mesure où les garanties qu'elles prévoient sont laissées inappliquées en cas d'accès par lesdits services de renseignement. La Cour de justice en a tiré la conclusion suivante : « *Il apparaît ainsi que les clauses types de protection des données adoptées par la Commission au titre de l'article 46, paragraphe 2, sous c), du même règlement visent uniquement à fournir aux responsables du traitement ou à leurs sous-traitants établis dans l'Union des garanties contractuelles s'appliquant de manière uniforme dans tous les pays tiers et, dès lors, indépendamment du niveau de protection garanti dans chacun d'entre eux. Dans la mesure où ces clauses types de protection des données ne peuvent, eu égard à leur nature, fournir des garanties allant au-delà d'une obligation contractuelle de veiller à ce que le niveau de protection requis par le droit de l'Union soit respecté, elles peuvent nécessiter, en fonction de la situation prévalant dans tel ou tel pays tiers, l'adoption de mesures supplémentaires par le responsable du traitement afin d'assurer le respect de ce niveau de protection.* » (point 133).

4.2.2. L'adoption de garanties supplémentaires

Dans ses recommandations 01/2020 du 18 juin 2021, le CEPD a précisé que lorsque l'évaluation du droit ou de la pratique du pays tiers révèle qu'il existe des éléments susceptibles de porter atteinte à l'efficacité des garanties appropriées qu'offre l'instrument de transfert visé à l'article 46 du RGPD auquel l'exportateur a recours dans le cadre d'un transfert particulier – ce qui est le cas en l'espèce, à la suite de l'évaluation menée par la CJUE – l'exportateur doit suspendre le transfert ou mettre en place des mesures supplémentaires. Le CEPD relève à cet égard que « *(t)oute mesure supplémentaire ne peut être réputée efficace au sens de l'arrêt de la CJUE dans l'affaire Schrems II que si et dans la mesure où elle remédie – prise isolément ou en combinaison avec d'autres – aux lacunes relevées dans l'évaluation de la situation juridique et des pratiques applicables du pays tiers que l'exportateur a effectuée.* » (point 75).

Les mesures permettant de compléter les clauses types de protection des données peuvent être classifiées en trois catégories : contractuelles, organisationnelles et techniques (voir, à cet effet, le point 47 des recommandations 01/2020).

En ce qui concerne les mesures contractuelles, le CEPD a relevé que de telles mesures : « *[...] peuvent compléter et renforcer les garanties que peuvent offrir l'instrument de transfert et la législation pertinente du pays tiers [...]. Étant donné la nature contractuelle des mesures, qui ne sont généralement pas susceptibles de lier les autorités du pays tiers lorsqu'elles ne sont pas parties au contrat, ces mesures devraient être combinées avec d'autres mesures techniques et organisationnelles afin d'offrir le niveau requis de protection des données. [...]* » (point 99, soulignement ajouté).

En ce qui concerne les mesures organisationnelles, le CEPD a considéré que la « *[...] sélection et la mise en œuvre d'une ou de plusieurs de ces mesures ne garantissent pas nécessairement et systématiquement que le transfert satisfera la norme d'équivalence essentielle établie par le droit de l'Union. En fonction des circonstances particulières du transfert et de l'évaluation de la législation du pays tiers, des mesures organisationnelles sont nécessaires pour compléter les mesures contractuelles et/ou techniques afin de garantir un niveau de protection des données à caractère personnel essentiellement équivalent à celui garanti au sein de l'EEE* » (point 128, soulignement ajouté).

En ce qui concerne les mesures techniques, le CEPD a souligné que ces « *[...] mesures seront particulièrement nécessaires dans le cas où le droit dudit pays impose à l'importateur de données des obligations qui sont contraires aux garanties offertes par les instruments de transfert visés à l'article 46 du RGPD et qui sont, notamment, susceptibles de porter atteinte à la garantie contractuelle d'un niveau de protection essentiellement équivalent contre l'accès des autorités publiques de ce pays à ces données* » (point 77, soulignement ajouté). Il ajoute que « *Les mesures énumérées [dans les lignes directrices] visent à garantir que l'accès des autorités publiques de pays tiers aux données transférées ne porte pas atteinte à l'efficacité des garanties appropriées que contiennent les instruments de transfert visés à l'article 46 du RGPD. Ces mesures sont nécessaires pour garantir un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE, même si l'accès des autorités publiques est conforme à la législation du pays de l'importateur, lorsque cet accès va au-delà de ce qui est nécessaire et proportionné dans une société démocratique. Ces mesures visent à prévenir tout accès potentiellement illicite, en empêchant les autorités d'identifier les personnes concernées, de déduire des informations les concernant, de les distinguer dans un autre contexte ou d'associer les données transférées à d'autres ensembles de données qui pourraient contenir,*

notamment, des identifiants en ligne fournis par les appareils, applications, outils et protocoles utilisés par les personnes concernées dans d'autres contextes » (point 79, soulignement ajouté).

4.2.3. Les mesures supplémentaires mises en place par Google

Google LLC, en tant que destinataire des données, a adopté des mesures contractuelles, organisationnelles et techniques pour compléter les clauses types de protection des données. Dans sa réponse du 9 avril 2021, Google LLC a décrit les mesures adoptées en détails.

Ainsi que prescrit par la CJUE et le CEPD, il est nécessaire de vérifier si les mesures complémentaires adoptées par Google LLC sont efficaces, c'est-à-dire qu'elles répondent à la problématique particulière de la possibilité d'accès des services de renseignements américains aux données en cause.

En ce qui concerne les « *mesures juridiques et organisationnelles* » adoptées, il doit être relevé que ni la notification des utilisateurs (si celle-ci est possible), ni la publication d'un rapport de transparence ou d'une politique de gestion des demandes d'accès gouvernementales (« *policy on handling government requests* ») ne permet concrètement d'empêcher ou de réduire l'accès des services de renseignement américains. De plus, il ne ressort pas clairement des éléments du dossier dans quelle mesure l'examen attentif du caractère licite de chaque demande auquel Google LLC procède est une mesure supplémentaire efficace. En effet, selon la CJUE, même les demandes licites des services de renseignement américains ne sont pas conformes aux exigences du droit européen de la protection des données.

En ce qui concerne les « *mesures techniques* » adoptées, il doit être relevé qu'il n'a pas été clarifié, ni par Google LLC, ni par la société comment les mesures décrites – telles que la protection des communications entre les services de Google, la protection des données en transit entre des centres de données, la protection des communications entre les utilisateurs et les sites web ou la sécurité sur site – permettent de prévenir ou de réduire les possibilités d'accès des services de renseignement américains sur la base du cadre légal américain.

En ce qui concerne les techniques de chiffrement, telles que celles pour les données entreposées dans des centres de données, mentionnées en particulier par Google LLC comme mesure technique, il doit être relevé que Google LLC, en tant qu'importateur de données a dans tous les cas l'obligation d'accorder l'accès ou de fournir les données importées qui sont en sa possession, y compris les clés de chiffrement nécessaires pour rendre les données intelligibles (voir recommandations 01/2020, point 81). En d'autres termes, tant que Google LLC a la possibilité d'accéder aux données des personnes physiques en texte clair, de telles mesures techniques ne peuvent être considérées comme efficaces en l'espèce.

En ce qui concerne l'argument de Google LLC selon lequel les données de Google Analytics qui sont transférées par les gestionnaires de sites sont pseudonymisées, il doit être relevé que les identifiants uniques universels (UUIDs) ne correspondent pas à la définition de l'article 4.5 du RGPD. En effet, si la pseudonymisation peut être une technique participant à la protection de la vie privée, les identifiants uniques – ainsi qu'il a été souligné précédemment – ont pour finalité spécifique d'individualiser les utilisateurs, et non de servir de garantie. En outre, il a également été souligné supra comment la combinaison d'identifiants uniques avec d'autres éléments (tels que les métadonnées du navigateur ou de l'appareil) et la possibilité de relier de telles informations à un compte Google permettent dans tous les cas de pouvoir identifier un individu.

Par conséquent, les mesures supplémentaires adoptées, telle qu'elles ont été présentées par Google, ne sont pas efficaces dans la mesure où aucune d'entre elles ne résout les problèmes spécifiques au cas d'espèce. En effet, aucune d'entre elles n'empêche les services de renseignement américains d'accéder aux données en cause ou ne rendent cet accès ineffectif.

4.3. Les dérogations prévues par le Chapitre V du Règlement

La société a fait valoir qu'actuellement, le transfert de données en cause en dehors de l'Union européenne n'était basé sur aucun autre instrument prévu par l'article 49 du RGPD.

4.4. Conclusion

Par conséquent, il doit en être conclu que la société ne peut se fonder sur aucun des instruments prévus par le Chapitre V du Règlement pour justifier le transfert des données à caractère personnel des visiteurs de son site web, et en particulier des identifiants uniques, adresses IP, données du navigateur et métadonnées, vers Google LLC aux États-Unis.

Ainsi, du fait de ce transfert de données, la société compromet le niveau de protection des données à caractère personnel des personnes concernées, tel qu'il est garanti à l'article 44 du RGPD.

En conséquence, la société [redacted] France, sise [redacted] est mise en demeure sous un délai d'un (1) mois à compter de la notification de la présente décision, qui peut être renouvelé une fois, et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- **mettre en conformité le traitement relatif à la fonctionnalité Google Analytics avec les articles 44 et suivants du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, si nécessaire, en cessant de traiter des données à caractère personnel dans le cadre de la version actuelle de Google Analytics ;**

- **justifier auprès de la CNIL que la demande précitée a bien été respectée, et ce dans le délai imparti.**

À l'issue de ce délai, si la société [redacted] France s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la société [redacted] France ne s'est pas conformée à la présente mise en demeure, il est rappelé qu'un rapporteur peut être désigné pour requérir que la formation restreinte prononce l'une des sanctions prévues par l'article 20 de la loi du 6 janvier 1978 modifiée.

La Présidente

Marie-Laure DENIS