Délibération SAN-2023-009 du 15 juin 2023

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Jeudi 22 juin 2023

Délibération de la formation restreinte n°SAN-2023-009 du 15 juin 2023 concernant la société CRITEO

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Madame Christine MAUGÜÉ et Messieurs Alain DRU et Bertrand du MARAIS, membres ;

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 ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 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° 2020-005C du 27 décembre 2019 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 des traitements mis en œuvre par la société CRITEO ou pour son compte, en tout lieu susceptible d'être concerné par leur mise en œuvre ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 23 juin 2021 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société CRITEO le 3 août 2022 ;

Vu les observations écrites versées par le conseil de la société CRITEO le 31 octobre 2022 ;

Vu la réponse du rapporteur à ces observations notifiée à la société CRITEO le 7 décembre 2022 ;

Vu les nouvelles observations écrites versées par le conseil de la société CRITEO, reçues le 30 janvier 2023 ;

Vu les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 16 mars 2023 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société CRITEO :

- […]

En visioconférence : […]

La société CRITEO ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. Fondée en 2005 en France, la société CRITEO SA (ci-après la " société ") est spécialisée dans l'affichage de publicités ciblées sur le web. En 2022, le groupe CRITEO employait environ 3 000 employés et avait réalisé un chiffre d'affaires global d'environ 1,9 milliard d'euros pour un résultat net de 10 millions d'euros environ.

2. La société met en œuvre des traitements de données dits de " reciblage publicitaire ", qui consistent à suivre les habitudes de navigation des internautes pour leur afficher des publicités personnalisées, au moyen de cookies déposés dans les terminaux des utilisateurs.

3. Le 8 novembre 2018, la Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a été saisie d'une plainte adressée par l'association " Privacy International ", qui soulignait notamment que la société ne traitait pas les données des internautes conformément aux principes fixés à l'article 5, paragraphe 1, du 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 (ci-après " le RGPD ").

4. Le 4 décembre 2018, la CNIL a été saisie d'une réclamation adressée par l'association " None of Your Business " (ci-après " NOYB ") mandatée par […], qui dénonçait le formalisme imposé par la société auprès de laquelle il avait souhaité retirer son consentement et s'opposer au traitement de ses données (ci-après " le plaignant "). Le plaignant faisait état de ce que, malgré l'envoi d'un courrier électronique en ce sens à la société, cette dernière l'avait redirigé vers diverses procédures en ligne consacrées à l'exercice des droits.

5. Le 14 janvier 2019, conformément à l'article 56 du RGPD, la CNIL a informé l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant les traitements transfrontaliers mis en œuvre par la société, compétence tirée par la CNIL de ce que l'établissement principal de la société se trouve en France.

6. Après échanges entre autorités de protection des données, il s'est avéré que l'ensemble des autorités européennes sont concernées au sens de l'article 4, 22) du RGPD.

7. Dans le cadre de l'instruction de la réclamation déposée par l'association NOYB, la CNIL a interrogé la société sur les suites données aux demandes du plaignant. Cette instruction a donné lieu à un échange de courriers entre la CNIL et la société, en date des 27 mars, 29 avril, 9 septembre, 9 octobre, 27 décembre 2019 et 17 février 2020. Une réunion s'est aussi tenue le 17 janvier 2020.

8. Dans le prolongement de cette instruction et en application de la décision n° 2020-005C du 27 décembre 2019 de la présidente de la Commission, une délégation de la CNIL a effectué plusieurs contrôles auprès de la société afin vérifier le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après " la loi Informatique et Libertés " ou " loi du 6 janvier 1978 ") et du RGPD.

9. Ainsi, le 29 janvier 2020, la délégation a envoyé un questionnaire à la société, auquel cette dernière a répondu le 27 mars 2020, portant sur son organisation, sur les traitements de données à caractère personnel qu'elle met en œuvre, sur sa qualification en tant que responsable de traitement, sur ses relations avec ses clients et partenaires et sur sa gestion des demandes d'exercice des droits.

10. Les 16 et 17 septembre 2020, la délégation a mené un contrôle sur place dans les locaux de la société, au cours duquel elle a notamment procédé à des vérifications sur le site web de deux partenaires de la société. La délégation a également vérifié les suites données à la demande d'exercice des droits du plaignant et obtenu des informations sur les modalités de mise en œuvre du droit de retirer son consentement et du droit à l'effacement. Le contrôle sur place a donné lieu à deux procès-verbaux n° 2020-005/1 et 2020-005/2, notifiés à la société le 30 septembre 2020.

11. Le 13 octobre 2020, partant d'une liste fournie par la société des cent sites web à partir desquels elle collecte le plus de données, la délégation a mené un contrôle en ligne auprès de plusieurs de ces sites pour vérifier notamment les modalités du dépôt du cookie Criteo dans le terminal des utilisateurs et le dispositif mis en œuvre pour recueillir leur consentement. Le contrôle en ligne a donné lieu à un procès-verbal n° 2020-005/3, notifié à la société le 14 octobre 2020.

12. Le 23 juin 2021, sur le fondement de l'article 22 de la loi du 6 janvier 1978, la présidente de la Commission a désigné Monsieur François PELLEGRINI en qualité de rapporteur aux fins d'instruction de ces éléments.

13. Le 9 juin 2022, le rapporteur a adressé une demande complémentaire à la société pour se voir notamment communiquer les dernières versions des conditions générales d'utilisation des services Criteo, ainsi qu'un échantillon récent de contrats conclus par la société avec ses partenaires. La société y a répondu le 17 juin 2022.

14. Le 3 août 2022, à l'issue de son instruction, le rapporteur a fait notifier à la société un rapport détaillant les manquements aux articles 7, 12, 13, 15, 17 et 26 du RGPD qu'il estimait constitués en l'espèce.

15. Ce rapport proposait à la formation restreinte de la Commission de prononcer une amende administrative à l'encontre de la société d'un montant qui ne saurait être inférieur à soixante millions d'euros. Il proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

16. Le 31 octobre 2022, la société a produit des observations en réponse au rapport du rapporteur.

17. Le 7 décembre 2022, le rapporteur a répondu aux observations de la société.

18. Le 30 janvier 2023, la société a présenté de nouvelles observations en réponse à celles du rapporteur.

19. Par courrier du 21 février 2023, le rapporteur a informé le conseil de la société que l'instruction était close, en application de l'article 40, III, du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés.

20. Le rapporteur et la société ont présenté des observations orales lors de la séance de la formation restreinte du 16 mars 2023.

II. Motifs de la décision

A. Sur la procédure de coopération européenne

21. En application de l'article 60 paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 16 mai 2023 aux autorités de contrôle européennes concernées.

22. Au 13 juin 2023, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

B. Sur le traitement en cause, la qualification de données à caractère personnel et la responsabilité de traitement.

1. Sur le traitement en cause ayant pour finalité l'affichage de publicité personnalisée

23. L'article 4, 2) du RGPD définit un traitement comme " 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 ".

24. En l'espèce, la formation restreinte relève que la société met en œuvre un traitement de données dit de " reciblage publicitaire " à des fins d'affichage de publicité personnalisée (ci-après le " traitement en cause ").

25. Concrètement, la société collecte les données de navigation des internautes grâce à des cookies qui sont déposés dans leurs terminaux lorsqu'ils se rendent sur l'un des sites de leurs […] partenaires, comprenant des éditeurs et des annonceurs. Lorsqu'un internaute se rend sur le site web d'un partenaire, la société inscrit un cookie dans le terminal de son navigateur, lequel se voit attribuer un identifiant unique, appelé Criteo ID, qui lui permettra de le reconnaître lors de ses futures visites sur les autres sites des partenaires.

26. Ainsi, lorsqu'un internaute visite le site web d'un annonceur partenaire, la société enregistre dans sa base de données les actions de l'internaute via le cookie (par exemple, la visite de la page d'accueil, la connexion à un compte utilisateur, le clic sur une page " produit ", l'ajout d'un article au panier d'achat).

27. Ensuite, lorsque l'internaute visite le site web d'un éditeur partenaire, l'éditeur adresse une requête à la société afin de lui transmettre des informations telles que la dimension de l'encart publicitaire, la nature du site éditeur ainsi qu'un identifiant permettant à la société de reconnaître l'internaute.

28. La société utilise alors ses technologies de traitement de données pour déterminer quelle publicité serait la plus pertinente à afficher à l'internaute en fonction de ses habitudes de navigation et des produits ou services qui pourraient l'intéresser. En fonction de cette analyse, la société participe ensuite à une enchère en temps réel (" real time bidding " ou " RTB ") pour l'affichage d'une publicité sur l'espace publicitaire de l'éditeur. Si la société remporte l'enchère, la bannière publicitaire d'un annonceur est affichée dans l'encart disponible sur le site web de l'éditeur.

29. Ainsi, en tant qu'intermédiaire entre des annonceurs et des éditeurs de sites web, la société aide, d'une part, les annonceurs à toucher leur public cible avec des publicités plus pertinentes, d'autre part, les éditeurs à valoriser leurs espaces publicitaires.

30. La formation restreinte relève que la société reconnaît mettre en œuvre le traitement décrit aux paragraphes précédents.

2. Sur la qualification de données à caractère personnel des données traitées par la société CRITEO

31. 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 ".

32. Le considérant 30 du RGPD, qui s'inscrit dans une jurisprudence bien établie de la Cour de justice de l'Union européenne (CJUE, 24 nov. 2011, Scarlet Extended SA C 70/10, pt. 51 et 19 oct. 2016, Breyer, C-582/14) prévoit quant à lui 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 ".

33. Dans son arrêt Breyer précité, rendu sous l'empire de la directive 95/46/CE, la CJUE a souligné l'importance d'une approche casuistique du caractère identifiant ou non d'une donnée plutôt qu'une position générale et de principe. Elle a indiqué que, pour déterminer si une personne est identifiable, il convenait de prendre en considération l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne.

34. Le rapporteur considère que la société traite des données à caractère personnel, compte tenu de ce qu'au regard du nombre et de la diversité des données collectées et du fait qu'elles sont toutes reliées à un identifiant, il est possible, avec

des moyens raisonnables, de réidentifier les personnes physiques auxquelles ces données se rapportent.

35. La société estime qu'elle traite des " évènements de navigation ", qui sont des données techniques pseudonymisées qui ne lui permettent pas d'identifier directement les internautes auxquelles elles sont rattachées. Elle soutient qu'elle n'est amenée à reconnaître l'identité d'une personne que dans l'hypothèse d'une demande de droit d'accès où elle pourra faire la correspondance entre l'identifiant de cookie Criteo (Criteo ID) et l'identité de la personne physique. En dehors d'une telle hypothèse, elle estime que le risque de réidentification est très faible et produit sur ce point des simulations effectuées par des prestataires.

36. Elle en tire comme conclusion que dès lors qu'elle ne traite que des données pseudonymisées, les éventuels manquements qu'elle aurait commis ont eu un impact très restreint pour les personnes concernées, ce dont la formation restreinte devrait tenir compte dans son appréciation.

37. La formation restreinte rappelle que seule une véritable anonymisation des données traitées, en faisant perdre aux données leur caractère " personnel ", c'est-à-dire, sans possibilité de réidentifier la personne physique à laquelle elles se rapportent, ferait échapper le traitement à l'ensemble des exigences du RGPD.

38. En l'occurrence, la formation restreinte relève que si la société ne prétend pas traiter des données anonymisées, elle affirme ne traiter que des données pseudonymisées présentant un risque de réidentification très faible.

39. La formation restreinte relève également que l'identifiant de cookie Criteo ID, attribué par la société au moyen des cookies qu'elle dépose, a pour but de distinguer chaque individu dont elle collecte les données et que de très nombreuses informations destinées à enrichir le profil publicitaire de l'internaute sont associées à cet identifiant, parmi lesquelles :

- des données liées à l'identification de la personne : emplacement géographique à partir d'adresse IP, identifiant utilisateur Criteo, identifiant de terminal, identifiants fournis par des partenaires, adresse de courrier électronique sous forme hachée fournie par les partenaires ;

- des données liées à l'activité de la personne, qui correspondent au suivi de l'historique de navigation de l'internaute à travers les sites visités, les produits consultés, ceux ajoutés au panier ainsi que l'acte d'achat. Cela comprend également les éventuelles interactions de l'utilisateur avec les publicités qui lui sont présentées (l'utilisateur a-t-il cliqué sur la bannière ? a-t-il procédé à un achat ?) ;

- des données dérivées ou inférées à partir des informations précédentes afin de pouvoir proposer à l'utilisateur les produits les plus pertinents, compte tenu de ses centres d'intérêt.

40. Ainsi, la formation restreinte note que si la société ne dispose pas directement de l'identité des personnes physiques auxquelles sont liés les terminaux sur lesquels des cookies sont inscrits, la réidentification peut être facilitée par le fait que, dans certaines hypothèses, la société collecte, outre les données liées aux évènements de navigation, d'autres données qui facilitent la réidentification telles que les adresses électroniques des personnes ayant fait leur parcours de navigation depuis un environnement authentifié (ou " logué ") sous forme hachée, des identifiants leur correspondant générés par d'autres acteurs, l'adresse IP sous forme hachée ou encore l'agent utilisateur du terminal utilisé.

41. Par conséquent, dès lors que la société est en mesure de réidentifier des personnes par des moyens raisonnables, les données traitées conservent un caractère personnel, au sens de l'article 4, 1) du RGPD.

42. Il en résulte que le RGPD est applicable et que, eu égard à ce qui a été indiqué ci-dessus, la société est responsable de traitement du traitement en cause.

C. Sur le manquement à l'obligation d'être en mesure de démontrer que la personne concernée a donné son consentement

43. Aux termes de l'article 6, paragraphe 1, du RGPD : " le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions ".

44. En vertu de l'article 4, 11) du RGPD, le consentement est défini comme " 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 ".

45. L'article 7, paragraphe 1, du RGPD relatif aux conditions applicables au consentement prévoit que : " dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant ".

46. Le rapporteur considère que la société n'a mis en place aucune mesure lui permettant de s'assurer que les données à caractère personnel qu'elle traite sont uniquement celles pour lesquelles un consentement valable de la personne a été recueilli. Il note en cela que parmi les sites web contrôlés par la CNIL, plus de la moitié des sites édités par ses partenaires ne recueillaient pas un consentement valide et que la société n'avait pas mis en œuvre de mécanisme d'audit de ses partenaires.

47. La société, invoquant l'arrêt Fashion ID (CJUE, 29 juillet 2019, C 40/17), fait valoir que ses partenaires, qui ont la qualité de responsables conjoints de traitement, restent les mieux placés pour collecter le consentement des personnes concernées en ce que le cookie Criteo est déposé dans le terminal des internautes lors de la navigation sur leur site web.

48. La société ajoute qu'à ce titre, les différents accords conclus avec ses partenaires en application de l'article 26 du RGPD (notamment les Conditions générales d'utilisation de services précitées et son Accord de protection des données) prévoient que cette obligation leur revient. Elle estime que cette répartition contractuelle est suffisante pour assurer le respect de cette obligation, qui s'impose à ses partenaires en vertu du principe de force obligatoire des contrats.

49. Elle soutient que rien ne permet d'établir que les pratiques constatées auprès des douze sites web visités par la délégation de contrôle seraient représentatives de l'état de conformité de ses […] partenaires.

50. Bien qu'elle prétende ne pas avoir d'obligation propre à s'assurer que ses partenaires ont valablement recueilli le consentement des personnes concernées, la société souligne néanmoins ne pas hésiter à résilier les contrats conclus avec ceux qui ne respectent pas leurs obligations en matière de recueil du consentement des internautes.

51. Elle ajoute avoir mis en œuvre d'autres mécanismes de contrôle, tels qu'une stratégie d'audit de ses partenaires qui, au 31 octobre 2022, a permis de vérifier l'état de conformité de près de […] de ses partenaires, ainsi qu'un processus dit de " Know your client " par lequel elle vérifie la conformité de ses futurs partenaires à plusieurs exigences réglementaires (présence d'une bannière cookie et d'une politique de confidentialité) préalablement à la conclusion d'un contrat de services avec eux. Enfin, elle indique avoir résilié son contrat avec l'un de ses partenaires qui avait été contrôlé par la délégation de la CNIL et avoir adressé un avertissement à un autre partenaire ne respectant pas la règlementation applicable en matière de recueil de consentement des internautes.

52. La formation restreinte rappelle qu'en cas de responsabilité conjointe, l'article 26 du RGPD oblige les responsables de traitement conjoints à s'assurer, par le biais d'un accord, qu'ils respectent mutuellement le RGPD et notamment qu'ils organisent entre eux la meilleure façon de répondre aux droits des personnes concernées, en fonction de la nature du traitement et de leur responsabilité respective vis-à-vis de ce traitement.

53. Elle souligne qu'aux points 167 et 168 de ses lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, le comité européen de la protection des données (CEPD) considère qu'en cas de responsabilité conjointe, " les deux responsables du traitement sont toujours tenus de veiller à disposer tous deux d'une base juridique pour le traitement " et qu'ils " peuvent disposer d'un certain degré de flexibilité dans la répartition et l'attribution des obligations entre eux, pour autant qu'ils garantissent le plein respect des exigences du RGPD en ce qui concerne le traitement spécifique ".

54. En premier lieu, s'agissant des rôles et obligations respectives de la société Critéo et des sites partenaires, la formation restreinte relève que dans le cadre de son traitement ayant pour finalité l'affichage de publicité personnalisée, la société traite les données à caractère personnel des internautes visitant les sites de ses partenaires qui sont préalablement collectées par l'intermédiaire du cookie Criteo.

55. Elle relève par ailleurs que la société et les sites de ses partenaires à partir desquels est déposé le cookie Criteo dans le terminal des internautes sont responsables conjoints des opérations de dépôt du cookie Criteo et de la collecte de données des internautes opérée grâce à ce cookie.

56. En ce qui concerne le cadre juridique applicable à ces différentes opérations de traitement, la formation restreinte rappelle que si le dépôt du cookie Criteo dans le terminal de l'internaute se rendant sur le site web d'un partenaire et qui permet à la société d'attribuer un identifiant unique à cet internaute est soumis aux dispositions de l'article 5, paragraphe 3, de la directive 2002/58/EC du Parlement européen et du Conseil du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (ci-après la " directive " ePrivacy " "), transposées en droit français à l'article 82 de la loi Informatique et Libertés, le traitement subséquent à des fins publicitaires, qui est opéré à partir des données à caractère personnel collectées par l'intermédiaire de ce cookie, est soumis aux dispositions du RGPD.

57. En ce qui concerne la base juridique applicable à ces différentes opérations de traitement, la formation restreinte rappelle d'abord qu'au titre de la directive " ePrivacy ", les opérations de lecture ou d'écriture d'information dans le terminal d'un utilisateur ne peuvent être mises en œuvre sans le consentement préalable de ce dernier.

58. Elle relève, ensuite, s'agissant du traitement en cause, que la société a indiqué à la délégation de contrôle dans sa réponse au questionnaire du 29 janvier 2020 que : " tous les traitements que nous réalisons dans le cadre de nos services de publicités en Europe sont basés sur le consentement de l'utilisateur ". Par ailleurs, la politique de confidentialité des traitements de la société mentionne également le consentement comme la base légale applicable pour les finalités d'affichage de publicité personnalisée, qu'elle soit ciblée ou contextuelle.

59. La formation restreinte relève que, selon une position constante de la CNIL, l'articulation des règles de la directive " ePrivacy " et du RGPD permet à l'éditeur du site à partir duquel est déposé le cookie de recueillir le consentement nécessaire au dépôt du cookie en même temps que celui nécessaire au traitement subséquent mis en œuvre à partir des données collectées par ce cookie.

60. Précisément, elle remarque, en l'occurrence, que la société s'est organisée d'une telle façon avec ses partenaires que les conditions générales d'utilisation des services Criteo, auxquelles les partenaires de la société ont adhéré, précisent qu'il revient bien au partenaire de recueillir le consentement de la personne concernée pour le traitement subséquent opéré à partir des données collectées par ce cookie.

61. La formation restreinte estime cependant que le fait que la collecte du consentement des internautes pour la mise en œuvre du traitement en cause revienne aux partenaires n'exonère pas la société de son obligation, en application de l'article 7 du RGPD, d'être en mesure de démontrer que la personne concernée a donné son consentement.

62. Ce double régime de responsabilité permet de garantir qu'à toutes les étapes du traitement des données collectées au titre de la navigation d'un utilisateur sur l'un des sites partenaires de la société, chaque responsable de traitement conjoint respecte les obligations qui lui incombent : pour les partenaires, celles relatives au dépôt et la lecture du cookie Criteo dans le terminal de l'utilisateur et, pour la société, celles relatives aux traitements subséquents opérés à partir des données collectées par le biais de ce cookie.

63. Il convient en effet que les personnes concernées bénéficient effectivement de la protection offerte par les textes en vigueur à laquelle elles ont droit tout au long de leur navigation et, notamment, que leurs données ne sont traitées par la société que si elles y ont préalablement et valablement consenti.

64. En outre, le cœur d'activité de la société consiste à transformer des données brutes de navigation en informations valorisables qu'elle exploite. Dès lors que la société joue un rôle central dans l'écosystème publicitaire, elle doit d'autant plus être en mesure de s'assurer que le traitement en cause respecte la règlementation en vigueur.

65. Enfin, la formation restreinte relève que l'arrêt Fashion ID, invoqué par la société, porte sur la question de savoir qui du gestionnaire du site (la société Fashion Id) ou de l'éditeur du cookie (la société Facebook) devait recueillir le consentement des personnes concernées avant de déposer le cookie édité par Facebook et qu'il a été rendu sous l'empire de la directive 95/46/CE relative à la protection des données.

66. Dans la mesure où le législateur européen a entendu renforcer les droits des personnes et la responsabilisation des acteurs en instaurant, notamment, l'obligation pour le responsable de traitement d'être en mesure de démontrer que la personne dont il traite les données a effectivement donné son consentement, en application de l'article 7, paragraphe 1, du RGPD, la formation restreinte estime que la référence à l'arrêt Fashion ID n'est en l'espèce pas pertinente.

67. En deuxième lieu, la formation restreinte relève que dans le cadre des vérifications en ligne effectuées lors du contrôle sur place du 16 septembre 2020 et lors du contrôle en ligne du 13 octobre 2020, la délégation a constaté sur sept sites web partenaires de la société qu'un cookie Criteo avait été déposé dans le terminal utilisé à cette occasion, dès son arrivée sur la page d'accueil sans qu'elle ait exécuté la moindre action et ce alors qu'à l'époque de ces constatations, la CNIL avait déjà eu l'occasion de rappeler que de telles pratiques entraient en contrariété directe avec les dispositions de la loi Informatique et Libertés applicables aux cookies.

68. La formation restreinte relève par ailleurs que dans trois cas, le site visité ne permettait pas à l'utilisateur de refuser les cookies autrement qu'en paramétrant son navigateur, ce qui ne constitue pas un mécanisme de refus du consentement valide tandis que, dans deux cas, un cookie Criteo était déposé après que la délégation eut exprimé son refus à ce dépôt.

69. Par ailleurs, dans le cadre du contrôle sur place du 16 septembre 2020, la délégation a constaté que les deux sites visités ne comportaient aucun mécanisme permettant un recueil de consentement au dépôt de cookie, tel qu'un bouton ou une case à cocher. Plusieurs évènements liés à la navigation de ces deux sites ont été enregistrés dans la base de données de la société, tels que la visite des pages des produits vendus par les partenaires de la société.

70. Il ressort de l'ensemble de ces vérifications que l'absence de recueil d'un consentement valable a été constatée par la délégation sur près d'un site visité sur deux. Or la formation restreinte relève également que neuf des douze sites visités par les services de la CNIL ont été indiqués par la société elle-même, au titre de ceux générant le plus de données collectées dans sa base de données.

71. S'il est vrai que la procédure de contrôle n'a pas permis de vérifier l'intégralité des sites des […] partenaires de la société, la formation restreinte considère qu'il peut être raisonnablement inféré des constatations précitées qu'à la date des contrôles, la société traitait un volume important de données de navigation pour lesquelles les internautes n'avaient pas donné un consentement valable.

72. En troisième lieu, la formation restreinte remarque qu'à la date de l'engagement de la procédure de contrôle, la société n'avait mis en œuvre aucune mesure satisfaisante permettant de considérer qu'elle était en conformité avec les exigences de l'article 7, paragraphe 1, du RGPD.

73. Ainsi, la formation restreinte relève qu'au début de la procédure de contrôle, à la question de la délégation visant à connaître les mesures mises en place par la société pour s'assurer de la validité du consentement, dans le cas où elle devait déléguer à un tiers le recueil de ce consentement, cette dernière s'était limitée à reproduire une mention de ses conditions générales d'utilisation, dans leur version applicable de mai 2016, aux termes desquelles la société exigeait de ses partenaires, " lorsque la loi le prévoit ", que la politique de confidentialité de leur site inclue " des mentions et des mécanismes de choix conformes aux lois et réglementations applicables ".

74. Or la formation restreinte considère qu'une telle clause ne permettait pas, à elle seule, de garantir l'existence d'un consentement valide et qu'il convenait à tout le moins qu'elle soit complétée pour préciser que l'organisme qui recueille le

consentement doit mettre à disposition de l'autre partie la preuve du consentement, pour que chaque responsable de traitement souhaitant s'en prévaloir puisse en faire effectivement état.

75. En l'occurrence, la formation restreinte relève qu'à la date d'engagement de la procédure de contrôle, cette clause n'était non seulement pas complétée par une clause spécifique portant sur la preuve du consentement, mais encore que la société avait admis également n'avoir jamais résilié de contrat en raison du non-respect par un partenaire de ses obligations contractuelles, ni mis en œuvre aucune autre mesure de contrôle de ses partenaires.

76. En ce sens, la formation restreinte relève que les différentes mesures avancées par la société n'ont été progressivement déployées qu'à partir de 2020, après l'engagement de la procédure de contrôle engagée en janvier 2020.

77. La formation restreinte prend ainsi acte de la campagne d'audits menée par la société auprès de ses partenaires depuis 2020 et du fait que la société a par ailleurs mis fin au contrat la liant à l'un d'entre eux qui ne respectait pas ses obligations en matière de cookies.

78. Elle relève, de même, que dans les versions ultérieures de ses conditions générales d'utilisation, la société a inséré une clause relative à la preuve du consentement selon laquelle le partenaire s'engage à " fournir rapidement à Criteo, sur demande et à tout moment, la preuve qu'un consentement de la personne concernée a été obtenu par le partenaire ".

79. Au regard de ces éléments, la formation restreinte considère que la société s'est mise en conformité avec les exigences de l'article 7, paragraphe 1, du RGPD.

80. Elle souligne néanmoins que cette mise en conformité, intervenue tardivement, est sans incidence sur le fait que la société a traité les données à caractère personnel d'internautes sans être en mesure de démontrer qu'ils ont valablement consenti au traitement ayant pour finalité l'affichage d'une publicité personnalisée, en violation de l'article 7, paragraphe 1, du RGPD.

D. Sur le manquement aux obligations d'information et de transparence

81. L'article 12, paragraphe 1, du RGPD dispose que : " Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique ".

82. Aux termes de l'article 13 du RGPD, le responsable de traitement doit fournir à la personne concernée les informations suivantes :

" a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) le cas échéant, les coordonnées du délégué à la protection des données ;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ".

83. En l'espèce, le rapporteur soutient que l'information fournie par la société aux personnes concernées n'était pas complète en ce qu'elle ne renseignait pas toutes les finalités relatives au traitement en cause dans la version de sa politique de confidentialité applicable à la date des constatations, notamment la finalité relative à l'amélioration de ses technologies.

84. Le rapporteur reproche également un manque de clarté quant à la base juridique du consentement applicable au traitement, dont la société précisait qu'elle diffère en fonction du pays, et quant aux finalités mises en œuvre sur la base de l'intérêt légitime.

85. La société répond avoir mis à jour sa politique de confidentialité.

86. Elle conteste en tout état de cause le premier grief en considérant qu'elle n'avait pas à spécifier la finalité d'amélioration de ses technologies dès lors que, selon elle, cette finalité comporte des éléments techniques concourant globalement à la même finalité que l'affichage de publicités personnalisées.

87. Sur le second grief, elle fait valoir que les éventuelles ambiguïtés dénoncées par le rapporteur n'ont jamais empêché les personnes concernées d'exercer leurs droits.

88. Dans ses secondes observations, la société avance qu'aucun manquement de sa part aux obligations découlant de l'article 13 du RGPD ne peut lui être reproché dans la mesure où elle ne procèderait qu'à une collecte indirecte des données.

89. La formation restreinte rappelle, en premier lieu, que le RGPD distingue le régime de l'obligation d'information qui s'impose au responsable de traitement en fonction de la nature de la collecte des données : le responsable de traitement est soumis aux dispositions de l'article 13 du RGPD lorsque les données sont collectées directement auprès de la personne concernée et aux dispositions de l'article 14 du RGPD dans le cas contraire.

90. Elle ajoute qu'au point 26 de ses lignes directrices du 29 novembre 2017 sur la transparence, dans leur version révisée du 11 avril 2018, le CEPD rappelle que l'article 13 du RGPD s'applique aussi lorsque les données sont collectées par le responsable de traitement " par observation ", c'est-à-dire lorsque le responsable de traitement collecte les données via l'utilisation de capteurs de toute sorte.

91. La formation restreinte relève que le Conseil d'Etat a adopté la même interprétation dans une décision rendue avant l'entrée en application du RGPD, en considérant que le fait que la collecte ne nécessite aucune intervention des personnes concernées était sans incidence sur le caractère direct de cette collecte (Conseil d'Etat, 10ème - 9ème chambres réunies, 8 février 2017, JCDecaux, n° 393714).

92. En l'espèce, la formation restreinte relève que les données sont bien collectées par la société directement auprès de l'internaute, dès lors que lorsque ce dernier navigue sur le site web d'un partenaire de la société, les requêtes du cookie Criteo permettant à cette dernière de savoir qu'un internaute arrive sur la page d'accueil, se connecte à un compte ou encore clique sur une page " produit ", sont directement adressées à ses serveurs, sans transiter par un autre responsable de traitement.

93. La collecte des données étant réalisée auprès des personnes, la formation restreinte en conclut que l'article 13 du RGPD s'applique à la société.

94. En deuxième lieu, la formation restreinte relève que les conditions générales d'utilisation des services Criteo prévoient que les partenaires de la société doivent intégrer dans leur site web une politique de protection des données à caractère personnel comportant un lien vers la politique de confidentialité de Criteo.

95. Elle relève que la section " Base juridique du traitement des données " de la politique de confidentialité de la société, dans sa version applicable à la date des constatations, mentionnait que : " Les opérations de traitement de Criteo respectent les réglementations en vigueur, dans les pays exigeant le consentement des utilisateurs pour l'utilisation de cookies ou de toute autre technologie similaire. Ce consentement est recueilli sur les sites Web et les applications mobiles des Annonceurs et des Éditeurs ".

96. Par ailleurs, il était également mentionné sous la même section que : " Criteo considère avoir un intérêt légitime à traiter vos données aux fins exprimées dans la présente politique de confidentialité, notamment pour :

- respecter les accords commerciaux passés avec nos clients et partenaires ;

- permettre à nos Annonceurs de promouvoir leurs produits et services ;

- permettre à nos Éditeurs de financer leurs activités ".

97. La formation restreinte considère, d'abord, que la première formulation crée une incertitude quant à la base juridique du traitement en ce qu'elle ne permet pas aux internautes situés au sein de l'Union européenne de comprendre que le traitement de leurs données repose sur leur consentement.

98. Elle estime, ensuite, que les finalités annoncées par la société dans la seconde formulation sont exprimées dans des termes vagues et larges qui ne permettent pas à l'utilisateur de comprendre précisément quelles données à caractère personnel sont utilisées et pour quels objectifs. Par ailleurs, la formation restreinte considère contradictoire de mentionner que les finalités relatives à la promotion des produits des annonceurs et au financement des activités des éditeurs reposent sur la base juridique de l'intérêt légitime alors lors que ces finalités sont directement liées au traitement d'affichage de publicité personnalisé, lequel repose, selon la société elle-même, sur la base juridique du consentement des internautes. La formation restreinte ajoute qu'une description aussi approximative et contradictoire des finalités poursuivies sur le fondement de l'intérêt légitime est susceptible d'entraver l'exercice par les personnes concernées de leur droit d'opposition, lequel est intrinsèquement lié à la qualité de l'information délivrée.

99. La formation restreinte relève que la société a répondu à ces lacunes dans la nouvelle version de sa politique de confidentialité, dès lors que cette dernière précise désormais que le consentement s'applique aux personnes résidant dans l'Espace économique européen et qu'elle inclut un tableau synthétisant l'ensemble des finalités de son traitement, dont celles reposant sur la base juridique de l'intérêt légitime, qui comprend une description détaillée de ces finalités et des catégories de données concernées. La formation restreinte observe que la société a également mis fin à la contradiction relevée ci-avant.

100. En troisième lieu, la formation restreinte relève que la rubrique " Finalité du traitement de données personnelles " de la politique de confidentialité de la société, dans sa version applicable à la date des constatations, contenait uniquement la ligne suivante : " Criteo traite vos données personnelles pour des annonces personnalisées ".

101. Or, dans le cadre du contrôle sur place des 16 et 17 septembre 2020, la société précisait à la délégation que le traitement permettait également " d'optimiser les réponses à donner aux enchères, la sélection d'articles à présenter dans une publicité et proposer la meilleure disposition pour cette bannière ".

102. Si la formation restreinte admet que certaines opérations techniques décrites par la société concourent directement à la finalité principale d'affichage de la publicité personnalisée, elle estime que d'autres servent en revanche une finalité distincte.

103. En effet, la société utilise les données collectées par le biais des cookies afin d'améliorer ses propres technologies (finalité dite de " machine learning ", mobilisant les données collectées par la société pour autoconfigurer des traitements algorithmiques de ciblage). Ainsi, l'objectif principal de ce traitement subséquent vise à améliorer l'efficacité du ciblage publicitaire effectué par Criteo de façon générale. Il s'agit donc d'une finalité distincte, qui devait bien être portée à la connaissance des personnes concernées.

104. La formation restreinte relève que dans la nouvelle version de sa politique de confidentialité, mise en ligne le 4 novembre 2022, la société distingue désormais bien, au sein de la rubrique " Utilisation de vos données ", d'une part, la finalité d'" affichage de la publicité personnalisée " et, d'autre part, la finalité d' " entrainement des modèles ", définie comme permettant d' " améliorer les performances des opérations publicitaires de Criteo ".

105. Il résulte de ce qui précède qu'en ne délivrant pas aux personnes concernées l'intégralité des informations prévues, en ayant recours à des termes insuffisamment clairs et précis et en présentant une base juridique des traitements erronée, la société a manqué à ses obligations de transparence et d'information prévues aux articles 12 et 13 du RGPD. Elle prend toutefois acte de ce que la société s'est mise en conformité durant la présente procédure.

E. Sur le manquement à l'obligation de respecter le droit d'accès des personnes concernées aux données à caractère personnel les concernant

106. L'article 12, paragraphe 1, du RGPD dispose que : " Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ".

107. L'article 15, paragraphe 1, du RGPD prévoit que : " La personne concernée a le droit d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel […] ".

108. En l'espèce, dans le cadre des investigations menées par la CNIL, la société a fourni à la délégation trois exemples de réponses adressées à des personnes concernées ayant formulé des demandes d'accès.

109. Il en ressort que lorsqu'une personne exerçait auprès d'elle son droit d'accès, la société lui transmettait les données extraites des trois tables suivantes :

- la table " Advertiser_advent ", qui stocke toutes les données liées aux évènements de l'annonceur ;

- la table " Banner_display ", qui stocke toutes les données nécessaires pour permettre d'afficher une publicité à l'utilisateur (par exemple, le pays de l'utilisateur, les données liées à l'annonceur ou encore la version du système d'exploitation de l'appareil de l'utilisateur) ;

- la table " Click_cas ", qui stocke toutes les données liées aux interactions d'un utilisateur avec les bannières publicitaires.

110. Le rapporteur considère que la société ne répondait que partiellement aux demandes de droit d'accès dont elle était saisie dès lors qu'elle ne communiquait pas les données figurant dans trois autres tables :

- la table " Usermatching ", qui contient les informations permettant de réconcilier des identifiants Criteo (dans le cas où un même utilisateur utilise plusieurs appareils) de manière " déterministe " (la société se base sur des informations fournies par ses partenaires, comme un numéro de carte de fidélité, un identifiant Apple ou Android, et / ou une adresse de messagerie électronique sous forme hachée pour créer un lien entre deux identifiants Criteo) ;

- la table " bc_tcp_timestamp ", qui contient les informations permettant la réconciliation d'identifiants de manière " probabiliste " (la société applique un modèle de prédiction à partir des données liées à deux identifiants qu'elle pense correspondre à un même utilisateur) ;

- la table " Bid_request ", qui contient les informations liées aux évènements relatifs au protocole d'enchères en ligne.

111. Il estime également que l'information fournie n'était pas intelligible pour l'utilisateur dès lors que la société se contentait d'une description sommaire de l'objectif de chaque table sans toutefois fournir d'explications sur l'objectif de chacune des colonnes figurant dans ces tables, ni sur leur contenu.

112. La société fait valoir que ses procédures en cas de demandes formulées au titre du droit d'accès respectent les exigences de l'article 15 du RGPD. Plus particulièrement, elle revient sur chacune des trois tables listées par le rapporteur et explique pourquoi, en cas de demande d'accès, elle ne communiquait pas les données qu'elles contenaient.

113. S'agissant de la table " Usermatching ", la société avance celle-ci ne contient que des données permettant la réconciliation de l'identifiant Criteo avec d'autres identifiants, mais qu'elle s'était néanmoins engagée à fournir ces données dans le cadre de ses réponses à des demandes d'accès dès novembre 2022.

114. S'agissant de la table " bc_tcp_timestamp ", la société explique celle-ci s'appuie sur une méthode probabiliste et peut potentiellement réconcilier deux personnes distinctes, de sorte que la communication des données risque de porter atteinte aux droits et intérêts de tiers dans l'hypothèse où les données se rapportant à une autre personne seraient communiquées à l'auteur de la demande d'accès. Pour cette raison, elle a exclu cette table de ses réponses aux demandes d'accès.

115. S'agissant de la table " bid_request ", la société expose que celle-ci contient environ 400 champs relatifs aux demandes d'enchères, de sorte qu'il s'agit essentiellement de données techniques et que les données restantes sont identiques à celles figurant dans la table " Banner_display " déjà communiquée par la société. Elle précise cependant qu'elle s'était engagée à fournir l'ensemble de ces données dans le cadre de ses réponses à des demandes d'accès avant mars 2023, le temps de mettre en œuvre un plan d'action qui lui permettrait d'extraire ces données par profil.

116. Sur l'intelligibilité de l'information fournie aux personnes concernées, elle indique avoir complété les explications par un tableau listant, pour chaque table, la nature des données traitées, et fournissant une description et des exemples de données, qu'elle transmet dans sa réponse à des demandes d'accès.

117. La formation restreinte prend acte des explications données par la société pour la table " bc_tcp_timestamp " et estime en effet que la société n'avait pas à communiquer les données de cette table dans la mesure où elles peuvent concerner plusieurs personnes sans que la société soit en mesure d'identifier avec certitude quelles données concernent exclusivement la personne à l'origine de la demande.

118. S'agissant des tables " Usermatching " et " bid_request ", elle considère que les éléments avancés et produits par la société permettent désormais à l'utilisateur de mieux comprendre les informations qui lui sont transmises.

119. La formation restreinte relève, cependant, que les explications fournies par la société ne permettent pas de justifier, à la date des constatations, de la non-communication des données contenues dans ces deux tables, alors qu'il n'est pas contesté que ces tables contiennent des données à caractère personnel qui peuvent être combinées avec d'autres données enregistrées par la société et, en particulier, avec l'identifiant attribué à chaque internaute.

120. Elle ajoute qu'il ressort de ces mêmes constatations que, dans le cadre de sa réponse aux demandes de droit d'accès, la société expliquait en une phrase succincte l'objectif de chaque table et invitait les utilisateurs à adresser un courriel pour obtenir davantage d'informations. Ainsi, en l'absence de communication systématique d'informations sur l'objectif et le contenu de chacune des colonnes figurant dans ces tables, la société plaçait l'utilisateur dans l'incertitude quant à la nature des données traitées le concernant.

121. Il résulte de ce qui précède qu'en ne communiquant pas l'intégralité des données à caractère personnel des personnes exerçant leur droit d'accès auprès d'elle et en ne mettant pas d'office à leur disposition une documentation leur permettant de comprendre les données qui leur étaient communiquées, la société a manqué à ses obligations au titre des articles 12 et 15 du RGPD.

F. Sur le manquement à l'obligation de respecter le droit de retrait du consentement et d'effacement des données

122. L'article 7, paragraphe 3, du RGPD dispose que : " La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement ".

123. Aux termes de l'article 17, paragraphe 1, du RGPD, " La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

[…]

b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement

[…]

d) les données à caractère personnel ont fait l'objet d'un traitement illicite

[…]".

124. En l'espèce, des échanges ont eu lieu entre les services de la CNIL et la société à la suite de la réception de la réclamation de […] concernant sa situation individuelle mais aussi de manière plus générale, les procédures mises en place par la société pour répondre aux demandes d'exercice des droits des personnes. La société a indiqué avoir fait évoluer les mesures mises en œuvre, notamment pour rendre effectifs le droit au retrait du consentement et le droit à l'effacement des données.

125. Il ressort des investigations postérieures à ces échanges et au déploiement des mesures annoncées par la société que les personnes concernées qui souhaitaient retirer leur consentement au traitement de leurs données par la société ou qui exerçaient leur droit à l'effacement pouvaient le faire en cliquant sur le bouton " Désactiver les services Criteo " accessible dans la politique de confidentialité de la société se trouvant sur le site " criteo.com ". La société a précisé que lorsqu'une personne clique sur ce bouton, un cookie d'" opt-out " est déposé dans le navigateur de la personne, permettant ainsi d'éviter le dépôt ultérieur de cookies Criteo et l'affichage de publicités personnalisées.

126. La société a précisé que la désactivation des services Criteo, c'est-à-dire le fait de ne plus afficher de publicités personnalisées à la personne, pouvait également se faire par l'utilisation des plateformes mises à disposition par les associations professionnelles représentatives du secteur telles que la plateforme " YourOnlineChoices ".

127. Lors du contrôle sur place du 17 septembre 2020, la délégation a constaté que la société ne gardait plus trace dans ses bases de l'identifiant utilisateur attribué à […]. Au cours de ce même contrôle, la société a déclaré que la procédure de désactivation de ses services ne lui permettait plus " de faire le lien entre l'identifiant utilisateur concerné et le navigateur

de l'utilisateur de telle sorte qu'aucune publicité ne sera proposée à cet identifiant ", sans avoir pour effet de supprimer de ses tables l'identifiant de l'utilisateur à l'origine de la demande d'opposition ou d'effacement. La société a ajouté que : " dans le cas où un identifiant utilisateur a fait l'objet d'une procédure de désactivation, il ne sera plus possible de réconcilier ultérieurement les évènements liés à cet identifiant aux autres identifiants éventuels liés à cet utilisateur ". Enfin, la société a indiqué qu'elle pouvait réutiliser l'identifiant utilisateur Criteo ainsi que les événements liés à la demande de désactivation dans le cadre de l'amélioration de ses technologies.

128. Le rapporteur considère que la société ne répond pas aux exigences de l'article 17 du RGPD dès lors qu'elle ne procède ni à la suppression de l'identifiant de la personne ni à l'effacement des évènements de navigation liés et ce alors que le traitement de la réclamation de […] démontre qu'elle est bien en capacité de procéder à un effacement effectif des données qu'elle traite.

129. La société fait valoir qu'elle n'est pas tenue de procéder à un tel effacement dès lors qu'elle disposerait d'un intérêt légitime à conserver et à traiter les données des personnes ayant formulé une demande d'effacement au titre des six finalités suivantes : correspondance des ventes / attribution, prévention des fraudes / lutte contre la fraude, entrainement des modèles, facturation, " reporting " et résolution des incidents.

130. En ce sens, elle s'estime fondée à ne pas procéder à la suppression effective de ces données tant que la poursuite de ces autres finalités reposant sur l'intérêt légitime justifie leur conservation. Pour chacune de ces six finalités, la société produit une étude démontrant la pertinence de recourir à cette base légale.

131. S'agissant spécifiquement de la finalité d'entrainement des modèles, la société considère que cela permet aux personnes concernées de recevoir des publicités encore plus personnalisées, ce qui rentre également dans leur intérêt. Elle ajoute que la CNIL a déjà reconnu, dans une délibération de sanction n° 2013-420 du 3 janvier 2014 et dans une décision MED-2017-075 du 27 novembre 2017, que " l'amélioration des services " pouvait être considérée comme un intérêt légitime d'un responsable de traitement.

132. La formation restreinte remarque que lorsqu'elle fait suite à une demande d'effacement, la société se limite à interrompre l'affichage de publicités personnalisées dans le terminal de la personne à l'origine de la demande, sans procéder à un effacement effectif des données relatives à cette personne.

133. La formation restreinte relève que la société prétend ne pouvoir procéder à un tel effacement au motif qu'elle a besoin des données collectées dans le cadre de ses traitements de ciblage publicitaire, fondés sur le consentement, pour mener à bien six autres finalités qui reposent, selon cette dernière, sur la base juridique de l'intérêt légitime.

134. Or, sans qu'il soit nécessaire de se prononcer sur l'adéquation de l'intérêt légitime comme base juridique de chacune des six finalités avancées par la société, la formation restreinte considère que, dans les cas où la société n'était en tout état de cause pas en mesure de s'assurer que la personne à l'origine de la demande avait valablement consenti au traitement de ses données par la société, cette dernière ne pouvait continuer à traiter les données de cette personne pour des finalités ultérieures reposant sur le fondement de l'intérêt légitime. Or, comme il a été démontré ci-dessus, la société ne conservait aucune preuve du consentement valable des personnes, en méconnaissance de l'article 7 du RGPD. La société ne pouvait donc se limiter à interrompre l'affichage de publicités personnalisées et devait procéder à l'effacement effectif des données traitées.

135. Cette conclusion s'impose d'autant plus qu'il ressort des investigations que la société traite un volume important de données pour lesquelles il a été établi qu'elles provenaient de cookies déposés avant toute manifestation de volonté de l'internaute et même, dans certains cas, lorsque ce dernier a expressément manifesté son refus.

136. Il résulte de ce qui précède qu'en se limitant à interrompre l'affichage de publicités personnalisées et en ne procédant pas à l'effacement des données à caractère personnel en cas d'exercice de leur droit à l'effacement, pour des personnes pour lesquelles la société ne pouvait s'assurer de la réalité du consentement, la société a manqué à ses obligations au titre des articles 7 et 17 du RGPD.

G. Sur le manquement à l'obligation de prévoir un accord entre responsables conjoints de traitement

137. L'article 26 du RGPD dispose que : " 1. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux. 2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées ".

138. Le rapporteur relève qu'à la date des constatations, la société avait bien conclu avec ses partenaires, responsables conjoints du traitement (les annonceurs, les éditeurs et les plateformes d'enchères en ligne), un contrat qui contenait une description des traitements objets de la responsabilité conjointe et du rôle de chaque responsable vis-à-vis de ces traitements.

139. Il souligne néanmoins que cet accord ne permettait pas de conclure à la conformité de la société avec l'article 26 du RGPD.

140. La société fait valoir que, tel que rédigé, l'accord conclu avec ses partenaires n'a pas lésé les personnes concernées qui ont profité de la pleine protection du RGPD dès lors que les conditions générales d'utilisation de ses services prévoient que les partenaires doivent fournir un lien vers la politique de confidentialité de Criteo et permettre aux personnes concernées d'exprimer leur consentement à la publicité ciblée.

141. Elle justifie néanmoins s'être dotée d'un nouvel accord entré en application le 5 juillet 2022.

142. La formation restreinte considère qu'il ressort de la rédaction de l'article 35 du RGPD que l'acte de répartition des obligations des responsables conjoints du traitement doit couvrir l'ensemble des obligations prévues par le RGPD afin de déterminer, pour chacune de ces obligations, lequel des responsables conjoints du traitement en aura la charge.

143. En l'espèce, la formation restreinte relève qu'à la date des constatations, l'accord conclu par la société avec ses partenaires ne précisait pas certaines des obligations respectives des responsables de traitements vis-à-vis d'exigences contenues dans le RGPD, telles que l'exercice par les personnes concernées de leurs droits, l'obligation de notification d'une violation de données à l'autorité de contrôle et aux personnes concernées ou bien, le cas échéant, la réalisation d'une étude d'impact au titre de l'article 35 du RGPD.

144. Elle remarque que l'obligation de conclure un accord en cas de responsabilité conjointe est une obligation spécifique qui s'impose aux responsables de traitement conjoints au titre de l'article 26 du RGPD.

145. Si, dans sa version du 5 juillet 2022, l'accord conclu par la société avec ses partenaires reprend désormais les mentions attendues au titre de cette disposition, la formation restreinte relève que cette conformité tardive ne remet pas en cause la caractérisation du manquement pour le passé.

146. Il résulte de ce qui précède que la société a manqué à son obligation au titre de l'article 26 du RGPD.

III. Sur le prononcé de mesures correctrices et la publicité

147. L'article 20 de la loi n° 78-17 du 6 janvier 1978 modifiée prévoit que : " lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ".

148. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe III, de la loi Informatique et Libertés, prévoit quant à lui que : " 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 ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

A. Sur le prononcé d'une amende administrative et son montant

149. La société fait d'abord valoir que la CNIL a porté atteinte au principe de non-discrimination en engageant uniquement des poursuites à son égard, après avoir pourtant établi que les sites web de ses partenaires ne respectaient pas la réglementation applicable aux cookies.

150. Elle soutient ensuite qu'elle ne devrait pas être sanctionnée pour ne s'être pas assurée que ses partenaires recueillent un consentement valide autrement que par voie contractuelle dès lors que ces vérifications devraient en fait revenir aux services de la CNIL, qui opérerait de la sorte une " privatisation " de ses missions.

151. La société estime qu'une meilleure prise en compte des critères prévus à l'article 83, paragraphe 2, du RGPD, au regard notamment de l'absence de preuve de dommage, du caractère non délibéré des manquements, des mesures prises pour atténuer les dommages, de la coopération dont elle dit avoir fait preuve avec l'autorité de contrôle et des catégories de données à caractère personnel concernées, qui présentent une faible intrusivité, justifierait que, dans le cas où la formation restreinte décidait de prononcer une amende, elle réduise sensiblement le montant de 60 millions d'euros proposé par le rapporteur.

152. Elle avance que la proposition d'amende du rapporteur représente 50 % de son résultat et près de 3 % de son chiffre d'affaires mondial, ce qui est proche du maximum légal prévu à l'article 83 du RGPD. Par comparaison, elle met en avant les précédentes décisions prononcées par la CNIL à l'encontre de Google (CNIL, FR, 31 décembre 2021, délibération de sanction n° SAN-2021-023) et de Facebook (CNIL, FR, 31 décembre 2021, délibération de sanction n° SAN-2021-024) en matière de cookies, dont le montant atteignait respectivement 0,07 % et 0,06 % de leur chiffre d'affaires global.

153. La formation restreinte rappelle, à titre liminaire, qu'il n'appartient pas à la formation restreinte de porter une appréciation sur la décision de la présidente de la CNIL d'engager des poursuites à l'égard de la seule société.

154. La formation restreinte rappelle que pour évaluer l'opportunité de prononcer une amende et déterminer son montant, elle doit tenir compte des critères précisés à l'article 83 du RGPD tels que la nature, la gravité et la durée de la violation, le nombre de personnes concernées, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle, les catégories de données à caractère personnel concernées par la violation et les avantages financiers obtenus du fait du manquement.

155. En premier lieu, en ce qui concerne le prononcé d'une amende administrative, la formation restreinte estime qu'il convient premièrement de faire application du critère prévu à l'alinéa a) de l'article 83, paragraphe 2, du RGPD relatif à la gravité du manquement compte tenu de la nature, de la portée du traitement et du nombre de personnes concernées par ce dernier.

156. Elle rappelle tout d'abord qu'il a été établi que la société n'était pas en mesure de démontrer que les personnes concernées avaient donné leur consentement au traitement de données à caractère personnel les concernant et que les constatations de la délégation de contrôle ont mis en évidence que la société exploitait des données de navigation provenant pour partie de cookies déposés avant toute manifestation de volonté de l'internaute.

157. Ensuite, en ce qui concerne la portée du traitement, la formation restreinte remarque que le manquement est d'autant plus grave que le traitement en cause, qui vise à afficher des publicités personnalisées, est réalisé à très grande échelle et revêt, par nature, un caractère massif et intrusif.

158. Elle rappelle que pour que les publicités affichées soient pertinentes, la société doit collecter de grandes quantités de données relatives à la navigation des internautes afin d'établir une image précise de leurs habitudes de consommation, de leurs préférences ou préoccupations du moment.

159. Ainsi, chaque visite sur le site d'un annonceur ou d'un éditeur, chaque clic sur un produit ou encore chaque achat effectué par un internaute est enregistré par la société puis analysé à des fins publicitaires. A ce titre, la société revendique sur son site web collecter 35 milliards d'événements par jour par liés à la navigation et aux achats dans le monde. En outre, la société partage et reçoit des données de ses partenaires, pour lui permettre notamment de mieux identifier chaque internaute ou d'établir un lien entre les différents appareils et navigateurs utilisés par un même internaute.

160. La formation restreinte relève que, si prise isolément, chacune des données collectées par la société a une faible valeur identifiante, combinées entre elles, celles-ci sont susceptibles de révéler avec un degré de précision important de nombreux aspects de l'intimité de la vie des personnes, dont leur genre, leur âge et leurs habitudes de consommation, c'est à dire leurs goûts, conférant ainsi au traitement en cause un caractère massif et intrusif.

161. Par conséquent, le résultat de la combinaison entre elles de ces données renforce considérablement le caractère massif et intrusif du traitement en cause et rend d'autant plus nécessaire qu'il soit mis en œuvre dans le strict respect des règles en vigueur, en particulier celles entourant le choix des individus quant à l'utilisation de leurs données.

162. De même, la formation restreinte rappelle que la transformation de données brutes de navigation en informations exploitables constitue le cœur d'activité de la société. Cette dernière doit donc d'autant plus être en mesure de s'assurer que les données à caractère personnel qu'elle traite respectent la règlementation en vigueur.

163. En ce qui concerne le nombre de personnes concernées par le traitement en cause, la formation restreinte relève que la société annonce disposer de données relatives à environ 370 millions d'identifiants utilisateurs à travers l'Union européenne, dont environ 50 millions d'identifiants sur le seul territoire français. Si une seule et même personne est susceptible de correspondre à plusieurs identifiants, ces chiffres révèlent la quantité substantielle de données collectées par la société.

164. S'agissant du manquement relatif à l'information des personnes, la formation restreinte souligne qu'il a engendré une perte de contrôle des internautes sur leurs données dans la mesure où la société n'a pas mis à leur disposition une information complète et compréhensible.

165. S'agissant des manquements relatifs à l'exercice des droits d'accès, de retrait du consentement et d'effacement, la formation restreinte souligne leur caractère structurel et leur gravité en ce que les mesures déployées par la société conduisent non seulement à ce que les demandes des personnes soient incorrectement traitées mais aussi à ce que ces dernières pensent légitimement que leur demande a bien été respectée.

166. Elle rappelle ainsi qu'à la date des constatations, les personnes concernées à l'origine d'une demande d'accès ne se voyaient pas communiquer les données contenues dans deux tables de la base de la société.

167. La formation restreinte rappelle également que la prise en compte par la société d'une demande d'effacement a pour unique effet d'arrêter l'affichage de publicités personnalisées, la société continuant par ailleurs à conserver les données de la personne à l'origine de la demande et même à les utiliser pour d'autres finalités.

168. S'agissant du manquement relatif à l'obligation de prévoir un accord entre les responsables conjoints de traitement, la formation restreinte considère que le fait de ne pas avoir encadré avec plus de précision les traitements réalisés conjointement avec d'autres acteurs a privé les personnes concernées de la pleine protection de leurs données à caractère personnel offerte par le RGPD.

169. Deuxièmement, la formation restreinte estime qu'il convient de faire application du critère prévu à l'alinéa k) de l'article 83, paragraphe 2, du RGPD relatif aux avantages financiers obtenus du fait du manquement.

170. Elle rappelle ainsi que le modèle économique de la société repose exclusivement sur sa capacité à afficher aux internautes les publicités les plus pertinentes pour promouvoir les produits de ses clients annonceurs, et donc sur son aptitude à collecter et à traiter une immense quantité de données à caractère personnel.

171. Or il ressort de la présente procédure que cette collecte et le traitement en cause se font en violation des exigences du RGPD et des droits des personnes concernées dès lors qu'il est reproché à la société de ne pas être en mesure de démontrer que ces dernières ont donné leur consentement au traitement de leurs données et qu'il est établi, dans certains cas, que la société traitait des données pour lesquelles les personnes concernées n'avaient pas consenti ou n'avaient pas donné un consentement valable.

172. Ainsi, les données à caractère personnel collectées et traitées sans consentement valable des personnes ont permis à la société d'augmenter indûment le nombre de personnes concernées par ses traitements et donc ses revenus financiers.

173. La formation restreinte ajoute que la société a également tiré un avantage financier du fait de ne pas procéder à l'effacement des données en continuant à utiliser les données qui ne sont pas effacées à des fins d'amélioration de ses

technologies, ce qui participe à sa compétitivité sur le marché de la publicité ciblée.

174. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 7, 12, 13, 15, 17 et 26 du RGPD.

175. En second lieu, en ce qui concerne la détermination du montant de l'amende, la formation restreinte rappelle qu'en vertu des dispositions de l'article 20, paragraphe III, de la loi Informatique et Libertés et de l'article 83 du RGPD, la société encourt, au regard des manquements constitués évoqués ci-avant, une sanction financière d'un montant maximum de 20 millions d'euros ou 4% de son chiffre d'affaires mondial total de l'exercice précédent, lequel était de 1,9 milliard d'euros en 2022, le montant le plus élevé étant retenu.

176. Dès lors, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83, paragraphe 2, du Règlement évoqués ci-avant, la formation restreinte estime qu'une amende de quarante millions d'euros apparaît justifiée.

177. Elle remarque que si ce montant constitue près de 2 % du chiffre d'affaires mondial de la société, il n'en demeure pas moins inférieur au plafond légal de 4 % prévu à l'article 83, paragraphe 5 du RGPD et à l'article 20, paragraphe III, 7°) de la loi Informatique et Libertés.

178. Par ailleurs, la formation restreinte rappelle que le montant de l'amende peut être supérieur au bénéfice généré par le responsable de traitement, dans la mesure où cela serait nécessaire afin d'assurer le caractère dissuasif de la sanction (voir, en ce sens, CE, 1er mars 2021, Société Futura Internationale, n° 437808, pt. 6).

B. Sur la publicité de la décision

179. La société demande à la formation restreinte de ne pas rendre publique sa décision.

180. La formation restreinte considère au contraire que la publicité de la présente décision se justifie au regard de la gravité des manquements en cause, de la portée du traitement et du nombre de personnes concernées.

181. Elle relève également que cette mesure permettra d'informer les personnes concernées de l'existence du traitement mis en œuvre par la société et du fait que celle-ci a pu traiter leurs données à leur insu, voire en dépit de leur absence de consentement. Cette information leur permettra, le cas échéant, de faire valoir leurs droits Informatique et Libertés auprès de la société.

182. Enfin, elle estime que cette mesure est proportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

• prononcer une amende administrative à l'encontre de la société CRITEO SA d'un montant de quarante millions d'euros (40 000 000 €) au regard des manquements constitués aux articles 7, 12, 13, 15, 17 et 26 du RGPD ;

• rendre publique, sur le site web de la CNIL et sur le site web de Légifrance, sa délibération, qui ne permettra plus d'identifier nommément la société à l'issue d'une durée de deux ans à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.