**SOUMISSION AU COMMISSAIRE À L'INFORMATION**

**-**

**DEMANDE D'AVIS D'ÉVALUATION / PLAINTE CONTRE LES COURTIERS DE DONNÉES ADTECH**

**Criteo, Quantcast et Tapad (les « courtiers de données AdTech »)**

## A. Introduction et objet de cette soumission

1. Par le biais de cette plainte, Privacy International demande aux autorités chargées de la protection des données (APD) du Royaume-Uni (le Bureau du Commissaire à l'information britannique), d'Irlande (la commission irlandaise de protection des données) et de la France (CNIL) de coopérer afin d'enquêter sur trois sociétés « AdTech »**, Criteo**, **Quantcast** et **Tapad**, afin d'évaluer leur conformité avec la législation en matière de protection des données, en particulier avec le règlement général sur la protection des données de l'UE 2016/676 (**le « RGPD »**).

2. Nous notons que, sur la base des informations dont nous disposons, il semble probable que l'autorité principale compétente pour le traitement transfrontalier puisse être différente dans chaque cas. Les trois sociétés sont présentes au Royaume-Uni. Cependant, la principale activité européenne de Quantcast se situe en Irlande et celle de Criteo en France. Étant donné qu'il est probable que les sociétés effectuent un traitement transfrontalier, il est impératif que les autorités compétentes de chacune de ces juridictions prennent en compte les éléments exposés dans le présent document. La manière dont ces autorités peuvent chercher à coopérer pour évaluer la conformité de Criteo, Quantcast et Tapad est toutefois une question sur laquelle elles devront se pencher. En conséquence, Privacy International appelle les autorités chargées de la protection des données à utiliser les pouvoirs qui leur sont conférés par le RGPD, y compris ceux de coopération et d'assistance mutuelle, ainsi que l'autorité dont elles disposent, pour mener une enquête conjointe en vertu de l'article 62 du RGPD. C'est pourquoi Privacy International demande aux autorités de protection des données d'enquêter sur ces sociétés et d'émettre un avis d'évaluation conformément au RGPD et à la législation nationale, notamment en ce qui concerne la loi britannique sur la protection des données de 2018 ; la loi irlandaise sur la protection des données 2018 et la loi française n° 2018-493 du 20 juin 2018 relative à la protection des données à caractère personnel.

3. Privacy International est gravement préoccupé par les activités de traitement de données du secteur du courtage de données et d'AdTech. Nous présentons donc cette plainte contre **Criteo, Quantcast et Tapad**. Simultanément, nous présentons deux autres soumissions/plaintes distinctes

au Commissaire à l'information du Royaume-Uni, contre les courtiers de données/ sociétés de notation de cote de crédit (« credit rating ») **Experian et Equifax** et les sociétés de gestion de base de données consommateurs (« consumer data broker companies») **Acxiom et Oracle.**[1] Ensemble, ces sociétés exploitent les données à caractère personnel de millions de personnes dans l'Union européenne et au-delà.[2]

4. Ces plaintes sont basées sur les informations fournies par ces sociétés - publiquement sur leur site web et dans leurs supports marketing, ainsi qu'en réponse aux demandes d'accès par les membres du personnel de Privacy International. Par conséquent, les violations de la protection des données documentées dans la présente plainte ne font qu'effleurer la surface des pratiques de ces sociétés en matière de données. Nous nous attendons à ce que les APD puissent approfondir nos préoccupations. Même dans ce cas, les infractions identifiées sont très graves et systématiques. En résumé, le traitement des données à caractère personnel par **Criteo, Quantcast** et **Tapad**, en particulier leur profilage :

   - N'a aucune base légale, en violation des articles 5 et 6 du RGPD, dans la mesure où les exigences relatives au consentement ou à l'intérêt légitime ne sont pas respectées. En ce qui concerne les données à caractère personnel de catégorie spéciale, celles-ci n'ont aucune base légale en vertu de l'article 9.
   - Ne respecte pas les principes de protection des données énoncés à l'article 5, à savoir les principes de transparence, de loyauté, de licéité, de limitation de la finalité, de minimisation des données, de précision, d'intégrité et de confiance.
   - Nécessite un complément d'enquête sur le respect des droits et garanties prévu dans le RGPD, notamment des articles 13 et 14 (droit à l'information), de l'article 15 (droit d'accès), de l'article 22 (prise de décision automatisée, y compris le profilage), de l'article 25 (protection des données dès la conception et protection des données par défaut) et de l'article 35 (analyse d'impact relative à la protection des données).

5. Ainsi, Privacy International demande aux autorités chargées de la protection des données, et en particulier à l'autorité principale compétente, de prendre des mesures pour protéger les personnes concernées contre ces violations systématiques et à grande échelle du RGPD.

6. Ces entreprises ne sont pas les seules à pratiquer un traitement de données douteux : Les problèmes qu'illustre notre plainte contre ces societes sont en

[1] Soumis le 8 novembre 2018 au commissaire à l'information du Royaume-Uni

[2] Privacy International a beaucoup écrit sur la manière dont les entreprises exploitent les données à caractère personnel : Comment les sociétés de données obtiennent-elles nos données ? (mai 2018) disponible à l'adresse suivante : https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data ; Un aperçu du profilage des entreprises (avril 2018) https://privacyinternational.org/feature/1721/snapshot-corporate-profiling ; Manipulation invisible : 10 façons dont nos données sont utilisées contre nous https://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-be-being-used-against-us ; Autres questions sur la participation de Cambridge Analytica lors des élections de 2017 au Kenya et les enquêtes de Privacy International (mars 2018) https://privacyinternational.org/feature/1708/fr-faire-questions-cambridge-analyticas-involvement-2017-kenyan-elections-and-privacy

fait des problèmes **récurrents** dans les **domaines** d'AdTech et du **courtage** de données ('data broker'), **dû a la nature même de leurs activités.** Par conséquent, pour cette raison précise et pour toutes les autres, détaillées dans la présente communication ainsi que dans les autres plaintes jointes, il est impératif que les autorités chargées de la protection des données, à savoir le Bureau du Commissaire à l'information britannique (« ICO»), la Commission de Protection des Données (« CPD ») et la Commission Nationale de l'Informatique et des Libertés (« CNIL ») enquêtent non seulement sur ces sociétés spécifiques, mais prennent également des mesures à l'égard des autres acteurs concernés par ces industries et/ou leurs pratiques commerciales générales.

## B. Privacy International

7. Privacy International est une organisation non-gouvernementale (ONG) à but non lucratif (numéro d'organisme de bienfaisance : 1147471) basée à Londres et vouée à la défense du droit à la vie privée dans le monde entier. Fondée en 1990, Privacy International entreprend des recherches et des enquêtes sur la surveillance menée par les gouvernements et les entreprises, en mettant l'accent sur les technologies qui permettent ces pratiques. En tant que tel, Privacy International a des objectifs légaux d'intérêt général et est active dans le domaine de la protection des droits et libertés des personnes concernées. Cette soumission concerne les travaux en cours de Privacy International sur l'exploitation des données, la surveillance par les entreprises et le RGPD.

## C. Pourquoi l'ICO, le CPD et la CNIL devraient-ils examiner cette soumission ?

8. Comme indiqué ci-dessous, le siège social (européen)[3] de chacune de ces sociétés est situé dans un État membre différent, avec des autorités de surveillance principales différentes. Le siège de **Criteo** est sis en **France**, le siège européen de Quantcast est en **Irlande** et celui de Tapad est au Royaume-Uni. Quantcast et Criteo ont également des bureaux au Royaume-Uni. En tant qu'autorités de la protection des données pour chacun des pays où sont implantées ces sociétés, la CNIL, l'ICO et le CPD ont la responsabilité de s'assurer de la conformité de ces sociétés avec le RGPD. Compte tenu de la nature des activités des sociétés, celles-ci sont également susceptibles de pratiquer un traitement transfrontalier qui peut s'avérer intéressant pour les trois APD.

9. Le système de publicité comportementale en ligne et les entreprises qui y participent sont déjà un problème que la CNIL, l'ICO et le CPD ont au moins commencé à envisager. En juillet 2018, la CNIL a engagé des poursuites contre les sociétés AdTech TEEMO et FIDZUP.[4] L'ICO a inclus, dans ses priorités réglementaires pour 2018-2019, le pistage sur internet et un le pistage inter-appareil dans un but marketing.[5] Il a aussi souligné, en juillet 2018, le rôle

[3] Tel que défini à l'article 4(16) du RGPD.
[4] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire
[5] https://ico.org.uk/media/2258810/ico-draft-regulatory-action-policy.pdf

de la publicité micro-ciblée dans le contexte politique dans son rapport récent « Democracy Disrupted »[6] ainsi que l'utilisation de l'analyse de données dans les campagnes politiques dans son rapport d'enquête intermédiaire. Puis, en septembre 2018, le CPD et l'ICO ont reçu des plaintes[7] mettant en évidence un certain nombre de problèmes de protection des données liés au système de « publicité comportementale en ligne ». L'ICO a récemment souligné des préoccupations connexes dans son rapport au Parlement du 6 novembre 2018.[8]

10. Les sociétés qui font l'objet de cette soumission font partie de ce système qui, pour les raisons exposées, nécessite une enquête plus poussée et une action de la part des autorités de protection des données.

## D. Les « courtiers de données » AdTech (en tant que responsables du traitement des données)

11. Cette plainte se concentre sur les entreprises de technologie publicitaire (« AdTech »). Il s'agit d'un terme générique faisant référence aux entreprises de technologie de publicité en ligne qui fournissent les outils d'analyse et les technologies qui constituent le complexe système utilisé en arrière-plan des services numériques pour diriger la publicité envers des audiences et individus ciblés. À un niveau plus général, il s'agit d'entreprises qui effectuent un pistage des internautes et détermine par quelles publicités ils sont ciblés. Cet écosystème implique le traitement des données à caractère personnel de millions d'individus.

12. Les trois sociétés spécifiques á l'encontre desquelles cette plainte est déposée sont **Criteo**, **Quantcast** et **Tapad.** Il s'agit de contrôleurs de données au sens de l'article 4, paragraphe 7, du RGPD. Les dispositions du RGPD s'appliquent au traitement des données à caractère personnel effectué par ces sociétés en vertu de l'article 3, paragraphe 1 du RGPD pour les raisons exposées ci-après.

### Criteo :

13. **Criteo** est présent dans le monde entier, y compris en France, où se trouve son siège social (**Criteo, 32 rue Blanche, 75009 Paris, France**). Dans l'UE, Criteo a également des bureaux en Allemagne (Munich), en Italie, aux Pays-Bas, en Espagne, en Suède et au Royaume-Uni (10 Bloomsbury Way, Londres WC1A 2SH).[9]

---

[6] Le point sur les enquêtes https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf et le Rapport sur la Democracy Disrupted https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[7] Plainte à l'ICO : https://brave.com/ICO-Complaint-.pdf et au CPD : https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf

[8] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

[9] https://www.criteo.com/contact-us/find-us/

14. Criteo est une plateforme publicitaire proposant des outils pour les spécialistes du marketing et les éditeurs, allant de l'acquisition de clients au ciblage de consommateurs, en passant par la publicité mobile, ainsi que des outils d'analyse et de conception. Criteo affirme capturer les données d'identité et d'intérêt de tous les acheteurs connectés à Criteo (72 % de tous les acheteurs en ligne dans le monde)[10] et « collecte et analyse en continu les informations en provenance de plus de 1,4 milliard de consommateurs actifs chaque mois et de plus de 600 milliards de dollars de données transactionnelles chaque année »[11]. Criteo affirme qu'il dispose du « plus grand ensemble de données d'acheteurs ouvert au monde, ce qui signifie que la technologie de machine learning de [Criteo] dispose de toutes les informations détaillées nécessaires pour **prévoir avec précision** ce qui stimule les acheteurs et suscite un engagement plus fort »[12]. (Emphase ajoutée)

15. Privacy International s'inquiète d'un certain nombre de produits et d'outils de Criteo, notamment :

    - **Shopper Graph[13].** Cet outil fournit des données granulaires sur les acheteurs, y compris des informations hors ligne et en ligne, ainsi que des données inter-appareils pour un meilleur ciblage. Il donne également accès à des données précises, récentes et détaillées, basées sur plus de 35 milliards d'historiques de navigation et de transactions quotidiennes provenant de près des trois quarts des acheteurs en ligne dans le monde. Il est soutenu par le **Criteo Engine** qui, lorsque les utilisateurs naviguent en ligne, utilise des données capturées précédemment et en temps réel, soit plus de 120 signaux d'achat, pour prédire en temps réel la propension d'un acheteur à utiliser des produits spécifiques, ainsi que la conception de publicité à laquelle il répondrait le mieux. Criteo indique que la « visibilité granulaire de l'interaction de l'acheteur avec les sites et les applications » leur permet de « prévoir avec précision ce qui stimule les acheteurs ».[14] Criteo appelle cela « le plus grand ensemble de données ouvert sur les acheteurs au monde ». Shopper Graph attribue à chaque utilisateur un identifiant Criteo basé sur 3 types de données : le graphe d'identité « connecte les identifiants d'achat en ligne et hors ligne à travers les appareils, les navigateurs, les applications et les environnements »[15] ; les cartes d'intérêt qui « relient les modèles de navigation et de transactions d'un acheteur aux identificateurs standard de produits, de catégories et de marques »[16] ; et les données de suivi de vente qui « suivent les ventes de campagne financées par la

[10] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[11] https://www.criteo.com/fr/technology/criteo-engine/
[12] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[13] https://www.criteo.com/technology/criteo-shopper-graph/
[14] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[15] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=3
[16] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=10

marque chez les détaillants du Criteo Sponsored Products Exchange »[17]

- **Dynamic Retargeting.** Cet outil est décrit par Criteo comme un moyen de « Ré-engager les consommateurs à chaque étape de leur parcours d'achat grâce à des publicités vidéo et des affichages personnalisés »[18.] Le reciblage dynamique repose sur la possibilité de suivre les utilisateurs sur différents appareils et de diffuser des publicités personnalisées « au bon moment au cours du parcours d'achat ».

16. Une description détaillée de la compréhension par Privacy International des objectifs de traitement de Criteo, des catégories de données à caractère personnel traitées, des sources de données à caractère personnel, des destinataires des données à caractère personnel et de la base légale invoquée est fournie à l'annexe A.

**Quantcast :**

17. Quantcast opère dans le monde entier, y compris en Irlande, où son siège social hors États-Unis est situé (**Quantcast International Limited, Beaux Lane House, Lower Nercer Street, 1er étage, Dublin 2, Irlande**).[19] Dans l'UE, Quantcast est également implanté en Allemagne (Hambourg et Munich), au Royaume-Uni (Londres et Manchester), en France (Paris) et en Suède (Stockholm).[20]

18. Quantcast est une société de technologie publicitaire spécialisée dans la publicité en temps réel supportée par l'Intelligence Artificielle, l'analyse et la mesure d'audience. Selon Quantcast, la société « exploite la plus grande plateforme d'information et de mesure d'audience ouverte du monde sur Internet »[21]. Grâce à « Quantcast Intelligence Cloud (« QIC ») », Quantcast propose une suite d'outils d'analyse, de ciblage et de mesure. Pour reprendre les mots de Quantcast, « QIC mesure les battements de cœur de vos clients tout au long de leur parcours numérique, changeant constamment en fonction de notre perception continue de l'Internet. **Nous connaissons les sites visités. Les mots-clés recherchés. Nous comprenons les habitudes d'achat.** Nous transformons ces données en informations exploitables. »[22] (Emphase ajoutée)

19. Privacy International s'intéresse à un certain nombre de produits de Quantcast, notamment :

---

[17] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=14
[18] https://www.criteo.com/for-marketers/fr/products/criteo-dynamic-retargeting/
[19] https://www.quantcast.com/privacy/
[20] https://www.quantcast.com/about-us/
[21] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-launches-first-widely-available-implementation-of-iab-europes-gdpr-transparency-consent-framework/
[22] https://www.quantcast.com/quantcast-intelligence-cloud/

- **Insights / Quantcast Mesure :** Quantcast utilise le QIC pour comprendre le comportement d'un client potentiel et obtenir des informations à partir de sa navigation sur le Web. Quantcast permet également aux clients de « consulter le trafic et les données d'audience de milliers de sites Web et d'applications pour voir comment vous [le client de Quantcast] comparez ».[23] Quantcast décrit ainsi ces informations : elles permettent aux clients Quantcast de « comprendre ce qui les amène [les consommateurs] au point d'influence - y compris les motivations psychographiques, et même les schémas comportementaux qui précèdent l'intention de recherche ».[24]
- **Quantcast Advertise** (ciblage) : Quantcast peut créer des modèles personnalisés en fonction de critères fournis par leurs clients (leur public idéal ou existant).[25] L'ensemble de données est basé sur « des millions de points de données disponibles » tels que « les comportements avant la recherche, les données démographiques et les achats antérieurs ».[26] Quantcast trouve ensuite les audiences et les clients qui correspondent au profil, permettant ainsi la diffusion à grande échelle d'un message ciblé à un public spécifique.[27]
- **Quantcast Choice** : un outil de gestion du consentement permettant aux éditeurs et aux annonceurs publicitaires (ci-après, 'publicitaires') d'obtenir, de gérer et de propager le consentement du consommateur dans l'ensemble de l'écosystème des contenus numériques et des publicités, sur la base du cadre de consentement et de transparence d'IAB Europe.[28]

20. Une description détaillée de la compréhension par Privacy International des objectifs de traitement de Quantcast, des catégories de données à caractère personnel traitées, des sources de données à caractère personnel, des destinataires des données à caractère personnel et de la base légale invoquée est fournie à l'annexe B.

**Tapad :**

21. La société Tapad Inc est présente dans le monde entier et son siège européen est situé au Royaume-Uni **(Tapad UK Limited, 40 Bernard St, Bloomsbury, Londres WC1N 1LE**).[29] Tapad possède un autre bureau européen à Oslo.[30] Tapad est une société du groupe Telenor.

22. Tapad est spécialisée dans la publicité inter-appareils. Tapad se décrit comme « Réinventant la personnalisation pour le spécialiste du marketing moderne ».[31] L'activité de Tapad est fondée sur son « **graphe d'identité**

[23] https://www.quantcast.com/en-uk/products/measure-audience-insights/
[24] https://www.quantcast.com/products/insights/
[25] https://www.quantcast.com/en-uk/resources/build-trust-with-data-driven-insights/
[26] https://www.quantcast.com/en-uk/products/targeting-overview/
[27] https://www.quantcast.com/products/targeting-overview/
[28] https://www.quantcast.com/gdpr/consent-management-solution/
[29] https://www.tapad.com/privacy
[30] https://www.tapad.com/about-us/find-us
[31] https://www.tapad.com

**numérique** » utilisé pour « analyser des milliards de signaux » et « créer des relations entre les marques et leurs clients **uniques** ».[32] Tapad « utilise les données du consommateur pour produire une communication inter-appareils personnalisée ». Les scientifiques et les ingénieurs de [Tapad] utilisent les données [Tapad] pour extraire des informations et créer une vue complète des consommateurs qui utilisent les appareils. »[33] Privacy International est préoccupé par les produits Tapad, notamment :

- **Le Tapad Graph :** « […] permet aux spécialistes du marketing de capturer une multitude de points de contact avec le consommateur entre appareils et canaux, en les associant à une personne concernée. Cela fournit une vue claire du parcours du consommateur vers la conversion et aide les spécialistes du marketing à identifier les initiatives qui ont un impact… Le Tapad Graph contient des données sur **des milliards d'appareils numériques** utilisés dans le monde entier. Nous connectons les appareils aux consommateurs et aux ménages afin que les données puissent être exploitées pour tous les cas d'utilisation des services marketing. » [34]
- **Device Graph Access (DGA) :** cet outil permet aux clients de Tapad d'accéder à des données inter-appareils. « DGA identifie les relations entre les appareils des consommateurs de vos plateformes et recherche les nouveaux appareils qui appartiennent à vos clients. » [35]
- **Tapad Customer Data Platform** « permet aux opérateurs de réseaux de télécommunication et de téléphonie mobile d'améliorer l'expérience et l'acquisition de clients en regroupant diverses données internes et des données des éditeurs grâce au Tapad Graph ». [36]

23. Une description détaillée de la compréhension par Privacy International des objectifs de traitement de Tapad, des catégories de données à caractère personnel traitées, des sources de données à caractère personnel, des destinataires des données à caractère personnel et de la base légale invoquée est fournie à l'annexe C.

## E. Contexte

### *Préoccupations concernant le courtage de données et l'industrie AdTech*

24. Comme indiqué ci-dessus, la présente soumission est axée sur les sociétés de technologie publicitaire (« AdTech »). Ceci est un terme qui désigne toutes les entreprises qui travaillent dans la « publicité comportementale ». À un niveau généralisé, il s'agit d'entreprises qui effectuent un pistage des internautes et déterminent avec quelles publicités ils sont ciblés. Cet écosystème implique le traitement des données à caractère personnel de millions d'individus.

---

[32] https://www.tapad.com/the-tapad-graph
[33] https://www.tapad.com/the-tapad-graph
[34] https://www.tapad.com/the-tapad-graph
[35] https://www.tapad.com/device-graph-access
[36] https://www.tapad.com/customer-data-platform

25. Les données à caractère personnel sont collectées, générées, partagées et traitées de multiples façons à l'aide de toute une gamme de technologies telles que les cookies, les « web beacons », le « device fingertprinting » (dispositif de prise d'empreinte numérique [i.e. de l'appareil, pas de l'individu]), les « tags » et les kits de développement logiciels (SDK) permettant de segmenter/classer les clients en fonction des pages consultées, des liens visités et des produits achetés. Ces formes de traitement de données à caractère personnel, y compris par les entreprises décrites dans cette soumission, sont liées à l'écosystème du courtage de données qui fait l'objet des soumissions conjointes de Privacy International contre Oracle et Acxiom, Experian et Equifax.

26. Ces dernières années, plusieurs rapports ont détaillé la portée et le rôle des courtiers de données et des sociétés d'analyse de données, la nature problématique du secteur du courtage de données ainsi que ses implications pour les droits des personnes et la société en général.[37] Un rapport particulièrement pertinent est celui de Wolfie Christl (Cracked Labs) intitulé « La surveillance d'entreprise au quotidien : comment les entreprises collectent, combinent, analysent, échangent et utilisent des données à caractère personnel de millions de personnes, » publié en juin 2017.[38] L'enquête décrite dans ce rapport trace et détaille la structure et la portée des écosystèmes de pistage et de profilage numériques d'aujourd'hui, et met en lumière certains des flux de données cachés entre les entreprises.

27. Les courtiers de données et la publicité comportementale/ciblée jouent également un rôle crucial dans les préoccupations relatives aux relations entre l'utilisation des données et la démocratie. Les rapports de l'ICO « Démocratie interrompue » et « Le point sur l'enquête concernant l'utilisation de l'analyse de données dans les campagnes politiques » en juillet 2018[39] soulignent les préoccupations relatives à l'utilisation de données à caractère personnel pour la publicité ciblée, au même titre que le rapport au Parlement du 6 novembre 2018.

28. Ces sociétés s'alimentent toutes entre elles grâce à un partage de données constant. À l'instar des courtiers de données mentionnés dans les soumissions conjointes, les sociétés AdTech (en général, pas seulement celles couvertes dans la présente plainte) ont en commun le fait qu'elles tirent profit du traitement des données de millions de consommateurs, et ce, sans

---

[37] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (Mai 2014), disponible à : https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf ; Open Society & Upturn, "Data Brokers in an Open Society" (Novembre 2016), disponible à : https://www.opensocietyfoundations.org/sites/default/files/data-brokers-in-an-open-society-20161121.pdf ; Institute for Human Rights and Business (IHRB), "Data Brokers and Human Rights: Big Data, Big Business" (Novembre 2016), disponible à : https://www.ihrb.org/focus-areas/information-communication-technology/databrokers-big-data-big-business

[38] http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

[39] Le point sur les enquêtes https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf et le Rapport sur la Democracy Disrupted https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

avoir de lien direct avec ces personnes. Malgré la présence de balises de pistage partout sur le web, ces sociétés ne sont pas connues du grand public. La plupart des gens n'en ont jamais entendu parler, ne savent pas qu'elles traitent et profilent leurs données, si ces données sont même seulement exactes, à quelles fins elles sont utilisées, avec qui elles sont partagées, ou quelles en sont les conséquences.

29. Le Contrôleur européen de la protection des données (« CEPD ») a également fait part de ses préoccupations relatives aux multiples façons dont les méthodes d'analyse de données peuvent être utilisées pour fusionner des données ou obtenir, déduire ou prédire d'autres données sur une personne concernée :

> « […] Par exemple, des informations limitées sur les sympathisants d'un parti politique contenues dans ses bases de données ou des informations de base sur les membres d'une organisation, fournies par ces derniers pourraient être fusionnées avec des données sur le comportement d'achat d'une personne obtenues auprès de courtiers en données. En utilisant des outils fournis par les plateformes de réseaux sociaux, ces données peuvent être combinées en fonction des informations démographiques (par ex. données sur la situation familiale) et des informations sur le comportement et les intérêts individuels. En appliquant les méthodes d'analyse de données susmentionnées, la campagne politique ou l'organisation basée sur l'adhésion intéressée **peut déduire des profils psychologiques ou des préférences politiques détaillées à propos de personnes à partir d'ensembles de données qui, à première vue, ne sont pas liés et ne sont pas sensibles.** »[40] (Emphase ajoutée)

« Les sociétés qui vendent des espaces publicitaires numériques profitent du placement de contenu ciblé en dépit de toute considération éthique: rien ne différencie un bon clic d'un mauvais de la part d'un groupe démographique ciblé. Les conséquences de ces activités de microciblage sont peut-être minimes sur certaines personnes, mais la complexité de la technologie à l'œuvre, les faibles niveaux de confiance et les intentions affichées de plusieurs grands acteurs de la technologie indiquent l'existence d'une culture de la manipulation dans l'environnement en ligne. Cette manipulation peut résulter de stratégies commerciales adoptées par les acteurs du marché eux-mêmes ou d'actions de personnes et d'États qui cherchent à utiliser les plateformes comme intermédiaires pour bouleverser les marchés et la parole publique ou leur nuire. » [41]

30. Le point clé est qu'en utilisant diverses entrées, ces sociétés peuvent faire des déductions intrusives à propos des individus — déductions qui peuvent être utilisées pour orienter la publicité vers des individus et des publics cibles spécifiques. Cela signifie que le résultat de l'analyse est supérieur à la somme de ses parties.

31. Pourtant, malgré les préoccupations exprimées dans ces différents rapports, et malgré que le RGPD ait pris effet dans l'Union Européenne le 25 mai 2018,

---

[40] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf
[41] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf

la majorité de ces sociétés continuent d'être loin de satisfaire aux exigences. Dans la présente plainte, Privacy International s'appuie sur les recherches et les plaintes existantes[42] pour demander la prise rapide de mesures réglementaires, compte tenu en particulier de des droits renforcés et des obligations accrues découlant du RGPD.

***Enquête de Privacy International***

32. L'enquête de Privacy International sur les pratiques en matière de données de ces sociétés a été menée sur trois fronts :

    (i) des demandes d'accès de personnes concernées ont été soumises par des membres de l'équipe de Privacy International. Bien que limitées dans leur substance, les réponses reçues ont permis de mieux comprendre la façon dont ces sociétés traitent les données à caractère personnel (cela inclus des demandes antérieures au RGPD et des lettres de suivi postérieures au 25 mai 2018) ;
    (ii) une analyse des politiques de confidentialité des sociétés avant et après le RGPD (pour les besoins de cette soumission, les politiques de confidentialité mentionnées sont postérieures au RGPD) ; et
    (iii) une recherche sur les supports marketing des entreprises qui sont mises à disposition du public.

33. Les réponses aux demandes et autres documents sont mentionnés tout au long de la soumission. Compte tenu de la portée limitée de notre enquête et des rapports de recherche existants sur les pratiques du secteur, Privacy International considère que les infractions au RGPD décrites dans la présente soumission ne représentent que la partie visible de l'iceberg. Nous espérons et prévoyons que les régulateurs pourront approfondir davantage nos préoccupations concernant les violations systématiques et à grande échelle du RGPD commises par ces sociétés et par l'ensemble de l'industrie.

## F. Cadre juridique et préoccupations - Violation du RGPD

34. Les pratiques en matière de données de ces sociétés donnent lieu à des violations substantielles et continues du RGPD. Les principales préoccupations qui sont exposées dans la présente soumission sont notamment les suivantes : i) le traitement de données à caractère personnel par Criteo, Quantcast et Tapad (ci-après dénommées « ces sociétés » ou « ces entreprises » ) enfreint divers principes de protection des données ; et (ii) n'a pas de base légale valable. Cette soumission n'est pas une liste exhaustive et il est possible que les autorités responsables de la protection des données à caractère personnel en identifient un plus grand nombre lors d'une enquête plus approfondie.

35. La soumission est structurée de manière à expliquer pourquoi le traitement des données à caractère personnel de chaque société n'est pas conforme

[42] Plainte au COI re publicité comportementale, déposée le 12/09/2018, disponible à l'adresse : https://brave.com/ICO-Complaint-.pdf

aux exigences du RGPD. La soumission commence par souligner le rôle du profilage et les concepts de données à caractère personnel et de pseudonymisation, et passe ensuite en revue les défaillances de ces entreprises en ce qui concerne chacun des principes de protection des données pertinents énoncés à l'article 5 du RGPD :

- Principe 1 - « Licéité, loyauté, transparence »
  (a) Transparence (en ce qui concerne les sources, les destinataires, le profilage et les droits des individus)
  (b) Loyauté
  (c) Licéité et base légale en vertu des articles 6 et 9 du RGPD (consentement, intérêt légitime et données à caractère personnel de catégorie spéciale)
- Principe 2 - « Limitation des finalités »
- Principe 3 - « Minimisation des données »
- Principe 4 - « Exactitude »
- Principe 6 - « Intégrité et confidentialité »

36. La soumission souligne également la nécessité d'effectuer une enquête approfondie sur le respect des dispositions relatives à la prise de décision automatisée, notamment le profilage, la protection des données par conception et par défaut, ainsi que les évaluations de l'impact sur la protection des données à caractère personnel.

*Profilage*

37. Un aspect novateur du RGPD est développé dans la définition du profilage, à l'article 4, paragraphe 4 :

    *« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. »*

38. Le considérant 72 confirme que : « Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnelles, par exemple le fondement juridique du traitement ou les principes en matière de protection des données... »

39. Des données distinctes et apparemment inoffensives peuvent être combinées pour créer un profil complet et représentatif d'une personne.[43] Les progrès en matière d'analyse des données, ainsi que le machine learning, ont permis d'inférer, de déduire et de deviner des données sensibles à partir de sources toujours plus nombreuses de données qui ne sont, elles, pas du tout

[43] https://privacyinternational.org/feature/1721/snapshot-corporate-profiling et https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

sensibles. Par exemple, il est possible de prédire des états émotionnels, tels que la confiance, la nervosité, la tristesse et la fatigue, à partir de modèles de saisie sur un clavier d'ordinateur.[44] Les mêmes techniques ont permis de simplifier la désanonymisation des données et d'identifier les personnes uniques à partir des données relatives à leur comportement sur les appareils, les services et même dans les espaces publics.[45] De tels profils peuvent permettre aux utilisateurs des données de déduire des informations extrêmement sensibles qui peuvent être exactes, ou non, et qui peuvent être inexactes de manière à fausser ou à classifier systématiquement certains groupes de personnes. Comme indiqué ci-dessus, de telles analyses signifient que le résultat de l'analyse des données est supérieur à la somme de ses parties : même des données apparemment inoffensives peuvent être utilisées ensemble pour obtenir des informations et des déductions relatives aux détails sensibles de la vie d'une personne concernée.

40. Étant donné que le profilage peut être effectué sans que les personnes concernées ne soient impliquées, il est bien souvent impossible de savoir si ces profils sont exacts, à quelles fins ils sont utilisés, ainsi que les conséquences de ces utilisations. L'exemple de profilage fourni par le Groupe de travail Article 29 (ci-après GT29) est le suivant :

> « Un courtier de données recueille des données auprès de différentes sources publiques et privées, soit pour le compte de ses clients, soit pour ses propres besoins. Il compile les données pour établir des profils sur les personnes concernées et les place dans des segments. Il vend ces informations aux entreprises qui souhaitent améliorer le ciblage de leurs biens et services. Le courtier de données effectue un profilage en plaçant une personne dans une certaine catégorie en fonction de ses intérêts. »[46]

41. Le profilage est au cœur du processus de traitement des données à caractère personnel par Criteo, Quantcast et Tapad. Comme indiqué dans les Annexes A, B et C et comme en témoignent les réponses aux demandes d'accès, les entreprises accumulent de grandes quantités de données provenant de différentes sources via diverses technologies en ligne et auprès de fournisseurs de données (courtiers de données) afin de profiler et déduire plus de données à leur sujet et classer les personnes concernées dans des catégories et des segments, afin de faciliter la publicité ciblée sur plusieurs appareils. Placer des individus dans des catégories/segments implique de porter des jugements sur chaque individu avant de les assimiler aux autres. Même lorsqu'une description de segment s'appuie sur des données agrégées et anonymisées, uniquement parce que l'objectif du profilage est utilisé pour regrouper des individus, cela n'annule pas le fait que des déductions sont

---

[44] Clayton Epp and others, 'Identifying emotional states using keystroke dynamics' (Proceedings of the SIGCHI Conference on Human Factors in Computing Systems May 2011) <http://hci.usask.ca/uploads/203-p715-epp.pdf>715-724.

[45] de Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. & Blondel, V.D. Unique in the Crowd: The privacy bounds of human mobility. Nature srep. 3, 1376; DOI:10.1038/srep01376 (2013).

[46] Article 29 Working Party opinion of profiling & automated decision-making (endorsed by EDPB), disponible à l'adresse : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

tirées à la suite du profilage de chaque individu qui se retrouve dans ce groupe.

42. Le profilage, tel que qu'il est pratiqué par ces sociétés, est explicitement reconnu dans le RGPD (considérant 30) :

    « Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants (par exemple des étiquettes (« tags ») d'identification par radiofréquence). Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes »

43. Comme indiqué dans la présente soumission, Privacy International estime que le profilage effectué par ces sociétés n'est pas conforme aux principes de protection des données, notamment en ce qui concerne la transparence, la licéité, la loyauté, la limitation des finalités, la minimisation des données, l'exactitude et l'exigence d'une base légale (y compris pour les données à caractère personnel de catégorie spéciale). Il existe également des questions en suspens sur le rôle des sociétés AdTech, telles que celles-ci, dans l'établissement de profils qui affectent considérablement les personnes concernées.

*Données à caractère personnel et pseudonymisation*

44. L'article 4(1) du RGPD stipule que « données à caractère personnel » « 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.»

45. L'article 4(5) du RGPD définit la « pseudonymisation » comme un traitement de « données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »

46. Le RGPD indique clairement, y compris dans les considérants, que les données pseudonymisées sont des données à caractère personnel aux fins du RGPD. Le considérant 24 indique « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à

une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. ».

47. Criteo, Quantcast et Tapad soulignent toutes dans leurs politiques de confidentialité qu'elles n'identifient pas « directement » les personnes concernées puisqu'elles utilisent des données « pseudonymes », et ne savent donc pas qui sont ces individus. Par exemple, Quantcast indique « Bien que nous nous basions sur ces informations pour découvrir quels sont vos centres d'intérêt, nous ne savons pas qui vous êtes » ; et Criteo souligne également « Nous ne savons pas qui vous êtes. Nous collectons et utilisons uniquement des données techniques pseudonymes relatives à votre navigation pour afficher des publicités personnalisées. » Les données collectées par Tapad incluent des « identificateur du dispositif de pseudonymes ».

48. La pseudonymisation est encouragée dans le RGPD afin de réduire les risques pour les personnes concernées et de contribuer au respect des obligations en matière de protection des données. Toutefois, la pseudonymisation n'exclut pas que les responsables du traitement de données soient soumis à d'autres obligations en matière de protection des données, et les données pseudonymisées sont toujours des données à caractère personnel.

*Ils disent qu'ils ne savent pas qui sont les personnes concernées mais annoncent en même temps qu'ils le savent.*

49. En fait, le but même et la « valeur » de ces sociétés, de leurs produits et services de données, est de **savoir** qui sont ces personnes afin de pouvoir les cibler encore plus précisément avec de la publicité. Ils annoncent et promeuvent ouvertement leur capacité à fournir des informations sur les personnes concernées et à prédire (et même à influencer) ce qu'ils vont faire ensuite :

    *Criteo*

    « Étant donné que Criteo Engine calcule ces informations en temps réel et au **niveau des acheteurs individuels** plutôt qu'au niveau de segments d'audience larges, l'impression publicitaire résultante est parfaitement optimisée pour l'acheteur, à ce moment précis de son parcours d'achat ».[47] Criteo se vante du « plus grand ensemble de données ouvert sur les acheteurs au monde, ce qui signifie que la technologie de machine learning [de Criteo] dispose de toutes les informations détaillées nécessaires pour **prévoir avec précision** ce qui inspire les clients et susciter un engagement plus fort ».

[47] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=5

*Quantcast*

« Quantcast Intelligence Cloud permet de **comprendre** le public en temps réel. Savoir ce qui les **motive**, comment ils changent et comment vous pouvez les **influencer** »[48]« **Connaissez votre audience grâce à des insights précis, granulaires et multi-dimensionnels** »[49] (Emphase ajoutée)

*Tapad*

« Nos scientifiques de données analysent des milliards de signaux dans The Tapad Graph pour créer des relations entre les marques et leurs clients **uniques**. Les spécialistes du marketing peuvent enfin voir leurs clients comme **des individus** [50]… Les scientifiques et les ingénieurs de [Tapad] utilisent les données [Tapad] pour extraire des informations et créer **un profil complet des consommateurs** qui utilisent les appareils. » [51] (Emphase ajoutée)

*Ils veulent en savoir le plus possible - pistage inter-appareils et données des partenaires.*

50. Ces entreprises cherchent à « connaître » les personnes concernées, ce qui signifie qu'elles cherchent à faire correspondre le comportement des individus sur différents appareils, applications et environnements. L'une des offres majeures de chacune de ces sociétés est le pistage inter-appareils, qui leur permet de savoir, ou du moins déduire (et de traiter en conséquence), que différents appareils sont utilisés par la même personne. Par conséquent, les annonceurs publicitaires et les autres clients de ces sociétés sont en mesure de cibler des individus sur plusieurs appareils, qu'il s'agisse d'un téléphone mobile, d'un ordinateur de bureau, d'un ordinateur portable, d'une tablette et même de la télévision, et de suivre la progression de leurs communications pour en connaitre l'impact, par exemple pour savoir si elles conduisent à un achat (à la fois hors ligne et en ligne). Tout au long de la journée, les gens utilisent différents appareils : leur ordinateur de bureau, leur téléphone portable, leur ordinateur portable personnel ou même leur téléviseur intelligent. Toute entreprise capable de suivre et de lier le comportement des personnes à travers ces différents appareils est en mesure d'obtenir une vision extrêmement détaillée de la plupart des activités d'une personne tout au long de sa journée. En conséquence, il devient presque impossible d'éviter ou d'échapper à un tel pistage.

51. Soucieuses de connaître le comportement détaillé des individus, ces sociétés ne se contentent pas des données collectées via les différentes technologies qu'elles déploient (cookies, pixels, tags et kits de développement logiciels (« SDK ») pour les applications), mais obtiennent encore plus de données à partir d'une vaste gamme de « partenaires » (qui, ensemble, constituent l'écosysteme AdTech et du courtage de donnés), comme indiqué ci-dessous

[48] https://www.quantcast.com/products/insights/
[49] https://www.quantcast.com
[50] https://www.tapad.com
[51] https://www.tapad.com/the-tapad-graph

dans le paragraphe sur la transparence. L'une des utilisations des données provenant de partenaire est de perfectionner leur ciblage inter-appareils :

*Criteo*

« Afin de vous montrer nos annonces personnalisées et d'offrir aux utilisateurs une expérience en ligne sans failles, nous pouvons être amenés à lier vos identifiants aux différents navigateurs et environnements que vous utilisez (« synchronisation des identifiants »). Cette technologie de synchronisation des identifiants permet à Criteo de vous proposer les annonces qui vous correspondent le mieux sur l'appareil ou le navigateur que vous utilisez actuellement, quel qu'il soit, sans collecter ni traiter d'informations personnelles identifiables comme votre nom ou votre adresse pour gérer le linking. À cette fin, Criteo se sert de méthodes de linking précises en s'appuyant sur les données techniques collectées grâce à notre technologie, comme les identifiants de nos partenaires publicitaires ou les clés de hachage d'adresses email qu'ils peuvent nous transmettre. Nous pouvons également recevoir des données relatives à la synchronisation des identifiants de partenaires de confiance utilisant diverses fonctions de linking aux mêmes fins et avec le même niveau de garantie en termes de confidentialité et de protection des données. »[52]

*Quantcast*

« Nous fournissons un service de suivi multiplateforme aux partenaires qui exploitent des sites Web et des applications mobiles. Pour ce faire, nous nous appuyons sur des identifiants hachés (c'est-à-dire cryptés) dérivés des connexions des utilisateurs pour lier votre utilisation sur des plateformes mobiles et de bureau. Cela permet à notre produit de mesure de fournir des rapports pertinents sur toutes les plateformes pour un seul partenaire. Nous utilisons également parfois des données de journal (« Log Data ») ou d'autres données provenant de nos partenaires pour deviner les associations entre des appareils ou des plateformes. »

*Tapad*

« En testant des données probabilistes d'appareil avec des signaux déterministes, nous avons créé le graphe d'identité numérique inter-appareils le plus puissant du marché. Nous utilisons ces technologies sur toutes les plateformes, y compris les sites Web, les applications mobiles, les applications de messagerie et de télévision, afin de pouvoir fournir la meilleure technologie de ciblage multi-plateformes possible. Voici des exemples de déploiement de ces technologies : (1) lors de la diffusion de publicitéset (2) lors de l'intégration avec les sites Web et les applications de nos partenaires afin de fournir une analyse inter-appareils. »

[52] https://www.criteo.com/fr/privacy/

*Ces sociétés ont pour activité le traitement des données à caractère personnel des individus, les normes qui doivent s'appliquer sont donc similaires à celles qui seraient en place si ces sociétés traitaient des millions de noms et d'adresses*

52. Comme indiqué ci-dessus, le considérant 30 du RGPD reconnaît que des identifiants en ligne peuvent être utilisés pour créer des profils d'individus. Les nombreuses données recueillies par ces entreprises (y compris les applications et les sites Web visités par les utilisateurs, leurs projets de voyage, ce qu'ils lisent, ce sur quoi ils travaillent, quand, où et sur quel appareil) leur permettent de « bien connaître » les personnes. Parfois, cela peut même permettre d'identifier directement une personne[53] ou de révéler des données à caractère personnel sensibles, par exemple à travers ce que vous avez lu, ce qui peut à son tour révéler des données à caractère personnel sensibles vous concernant (comme votre état de santé).[54] En effet, c'est cette capacité à suivre, à regrouper ces « informations » pour une publicité comportementale personnalisée, ciblée, qui anime ces entreprises.

53. Criteo, Quantcast et Tapad, ainsi que les sociétés ayant le même but, doivent respecter les mêmes normes de protection des données à caractère personnel que les sociétés qui traitent directement des données d'identification telles que des noms et des adresses. Le RGPD s'applique également aux données à caractère personnel que ces sociétés traitent. Elles doivent donc disposer d'une base légale valable, respecter tous les principes de protection des données, mettre en œuvre des mesures de protection et respecter les droits des personnes. Pour les raisons exposées dans cette soumission, Privacy International estime que les trois sociétés sont défaillantes et que ces sociétés et leurs pratiques justifient une enquête plus approfondie de la part des autorités chargées de la protection des données.

*Les principes de protection des données (article 5 du RGPD)*

**Principe 1 : Licéité, loyauté et transparence**

54. En tant que responsables du traitement de données, les entreprises doivent respecter les principes de protection des données énoncés à l'article 5 du RGPD.

55. L'article 5, paragraphe 1), alinéa a) du RGPD exige que les données soient « traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ».

**a) Transparence**

56. Cette sous-section de la soumission traite de la transparence. Les questions de licéité et de loyauté sont traitées ci-dessous.

[53] Le blog personnel d'un membre du personnel de Privacy International était identifiable à partir des données fournies par Quantcast. L'URL du blog révélait à la fois le nom complet de l'employé et le fait qu'ils étaient connectés à la plateforme de blogging pendant le suivi de l'URL.
[54] Par exemple, une URL parcourue enregistrée par Criteo est retournée dans une demande d'accès, "https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc"

57. Un des problèmes- clés émanant des sociétés AdTech est leur manque de transparence. Étant donné qu'elles n'ont pas d'interface avec les consommateurs, elles n'ont pas de relation directe avec les personnes concernées par les données qu'elles collectent et, par conséquent, elles reçoivent relativement peu d'attention et d'examen de la part du public. La plupart des gens n'ont jamais entendu leurs noms, et sont encore moins conscients que ces sociétés traitent leurs données à caractère personnel et possèdent des profils détaillés sur eux. En outre, les diverses technologies utilisées par ces sociétés, telles que les cookies, les pixels, les tags, les kits de développement logiciels (SDK) sont par nature cachées (malgré les tentatives législatives pour y remédier (règlement «vie privée et communications électroniques»)

58. Faisant suite aux demandes d'accès envoyées par les membres du personnel de Privacy International avant la mise en place du RGPD, Privacy International a écrit à Criteo, Quantcast et Tapad pour demander des informations auxquelles chaque personne qui en faisait la demande avait désormais droit, conformément à l'article 15 du RGPD. Privacy International a également demandé des informations sur les activités de traitement des entreprises telles qu'énoncées dans le droit à l'information figurant dans le RGPD, ainsi que des informations complémentaires conformément aux obligations de transparence et de responsabilité des entreprises au titre de l'article 5, paragraphe 1), alinéa a) et paragraphe 2) du RGPD. Des copies de chaque lettre et de la réponse correspondante sont jointes dans les annexes D, E et F. Privacy International a également examiné les informations fournies par chaque société dans sa politique de confidentialité en ligne, examinées en profondeur aux annexes A, B et C du présent document.

59. Les entreprises ont cherché à principalement répondre aux questions en se référant à leur politique de confidentialité respective, à savoir la politique de confidentialité de Criteo[55], la politique de confidentialité de Quantcast[56] et la politique de confidentialité de Tapad.[57]

60. Si les politiques de confidentialité s'efforcent d'expliquer les différentes manières dont les entreprises collectent les données et les technologies qu'elles utilisent, ces politiques gardent un aspect très général et sont donc insuffisantes lorsqu'une personne concernée souhaite savoir précisément comment ses données spécifiques ont été traitées. Par exemple, les politiques de confidentialité de Tapad et Criteo donnent des exemples non exhaustifs de « partenaires », et aucune entreprise ne répertorie ses clients. Par conséquent, une personne ne pourra pas, à partir de la politique de confidentialité, déterminer avec qui ses données à caractère personnel seront (ou ont été) partagées. En outre, la majorité des données à caractère personnel traitées par les entreprises ne sont pas obtenues par une relation directe avec une personne concernée, mais dépendent plutôt d'autres

[55] https://www.criteo.com/fr/privacy/
[56] https://www.quantcast.com/privacy/
[57] https://www.tapad.com/privacy-policy

personnes, que ce soit le site Web utilisant les technologies de l'entreprise ou d'autres partenaires. Ces sociétés cherchent à laisser aux autres la charge de notifier les personnes de leurs services, plutôt que de les informer elles-memes et conformément à l'article 14 du RGPD qu'elles traitent leurs données à caractère personnel.

61. En ce qui concerne les trois entreprises, ce manque de transparence est le plus évident et inquiétant en ce qui concerne les sources et les destinataires des données à caractère personnel, ainsi que le profilage. Le manque de transparence à cet égard comporte de lourdes conséquences relatives à la capacité des personnes concernées à exercer leurs droits.

Sources

62. En vertu du principe de transparence et en particulier des articles 13, 14 et 15 du RGPD, une personne concernée a le droit de recevoir des informations sur la source des données à caractère personnel traitées par le responsable du traitement. Les orientations du GT29 sur la transparence[58] indiquent clairement que cette obligation s'applique même lorsque la tâche est lourde :

> « […] En revanche, le simple fait qu'une base de données comprenant les données à caractère personnel de plusieurs personnes concernées ait été compilée par un responsable du traitement utilisant plus d'une source ne suffit pas à lever cette obligation s'il est possible (bien que chronophage ou fastidieux) de déterminer la source dont proviennent les données à caractère personnel des personnes concernées. Étant donné les obligations propres à la protection des données dès la conception et par défaut54, les mécanismes de transparence devraient être intégrés à des **systèmes de traitement dès le départ afin que toutes les sources des données à caractère personnel reçues par une entreprise puissent être suivies et retracées jusqu'à leur source, à tout moment pendant le cycle de vie du traitement des données**. » (Emphase ajoutée)

63. Comme indiqué plus en détail dans les annexes A, B et C du présent document, ces entreprises obtiennent des données à partir d'un large éventail de sources :

*Criteo*

64. Criteo se base sur les données suivantes :

- Sites Web et applications mobiles des publicitaires
- Sites Web et applications mobiles des éditeurs
- Les partenaires commerciaux tels que les fournisseurs AdExchange proposent des plateformes et des solutions d'enchères en temps réel

[58] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

(« RTB ») afin que Criteo puisse acheter des emplacements de publicité via les enchères pour le reciblage dynamique Criteo. Une liste de plus de 60 fournisseurs AdExchange figure sur le site Web de Criteo. »

*Quantcast*

65. Quantcast utilise des données provenant de :

- Données de journalisation (log data) de[59] sites au moyen de tags et de cookies, y compris des informations sur les navigateurs, les échanges de publicités et le kit de développement logiciel (SDK) Quantcast dans les applications mobiles
- Informations provenant des partenaires,[60] y compris les courtiers de données tels que Acxiom et Oracle et les échanges RTB.

*Tapad*

66. Tapad utilise des données provenant de :

- Plus de 130 partenaires d'intégration
- 42 milliards d'appareils
- Échanges RTB et fournisseurs côté offre
- Clients d'entreprise
- Données achetées/sous licence d' éditeurs et de courtiers-fournisseurs de kits de développement logiciels (SDK), de fournisseurs d'e-commerce et plus encore
- Données Telco via les 250 millions d'abonnés de Telenor
- Informations provenant de partenaires de données, Blue Kai, eXelate et « autres entreprises »

*Le web des sources de données*

67. Il existe au moins deux problèmes. Premièrement, toutes les sources ne sont pas fournies. Deuxièmement, même lorsque le nombre et la variété des sources sont fournis, le fait que la majorité des sources citées sont d'autres sociétés de données crée un effet de matriochka (les poupées russes). Un courtier de données mène à un autre et ainsi de suite,[61] ce qui signifie que trouver la source originale des données revient à chercher une aiguille dans une botte de foin.

68. Aucune des sociétés ne fournit de liste exhaustive de ses sources. Elles décrivent plutôt certaines des technologies qu'elles utilisent et certains types d'entreprises avec lesquelles elles travaillent en partenariat. L'absence de spécificité ainsi que d'une liste exhaustive amène la personne concernée à se poser des questions quant à ce qui manque, et lui rend également

[59] Voir l'annexe B pour la définition des données de journalisation (log data) par Quantcast
[60] https://www.quantcast.com/privacy/quantcast-partners/
[61] https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

extrêmement difficile et fastidieuse la tâche de démêler et de comprendre ce qui se passe avec ses donnés. En conséquence, il est en réalité impossible pour les personnes concernées de savoir comment les données qu'elles ont fournies à un moment aboutissent entre les mains de ces sociétés. Si les personnes concernées ne connaissent pas la source des données, il est extrêmement difficile d'identifier quelles données ont été fournies et, par conséquent, quelles données ont été déduites sur la base de l'analyse des autres données disponibles et quelles en sont les conséquences pour eux. Cela a des implications pour les droits des personnes concernées, comme indiqué ci-dessous.

Destinataires

69. En vertu du principe de transparence et en particulier des articles 13, 14 et 15 du RGPD, une personne concernée a le droit de connaître les destinataires ou les catégories de destinataires à qui sont envoyées leurs données à caractère personnel, y compris à qui les données à caractère personnel ont été ou seront divulguées. Les orientations du GT29 sur la transparence indiquent clairement qu'il incombe au responsable du traitement de nommer les destinataires des données, car cela sera probablement plus pertinent pour les personnes concernées et, s'ils ne peuvent pas être nommés, d'être aussi précis que possible :

    « **Les destinataires réels (nommés) des données à caractère personnel, ou les catégories de destinataires, doivent être fournis.** Conformément au principe de loyauté, les responsables du traitement doivent fournir aux destinataires les informations les plus significatives pour les personnes concernées. En pratique, il s'agit généralement des destinataires nommés, afin que les personnes concernées sachent exactement qui détient leurs données à caractère personnel. Si les responsables choisissent de fournir les catégories de destinataires, les informations doivent être aussi précises que possible en indiquant le type de destinataire (c.-à-d. faire référence aux activités qu'il exerce), le secteur d'activité, le secteur et le sous-secteur et la localisation des destinataires. » [62] (Emphase ajoutée)

70. Cependant, les informations fournies par les entreprises (Criteo, Quantcast et Tapad) sur les personnes avec lesquelles elles partagent les données (les destinataires) sont limitées.

71. Criteo est extrêmement vague dans sa politique de confidentialité en ce qui concerne les parties avec lesquelles elle partage des données, indiquant qu'elle ne partage des données non agrégées que sur « l'approbation de nos partenaires », mais l'identité de ces partenaires n'est pas spécifiée. En réponse à d'autres questions, Criteo a répondu qu'elle comptait des « milliers » d'« éditeurs partenaires » et de « clients publicitaires,» et qu'elle ne publiait pas de liste de ceux-ci.

[62] P37 Directives du GT29 sur la transparence disponible à l'adresse suivante : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

72. Quantcast indique qu'elle partage des données avec de vagues « tiers ». Pour compléter sa réponse, Quantcast fournit une liste des partenaires nommés, comme indiqué ci-dessus et à l'annexe B. Certains de ceux avec qui Quantcast partage des données incluent notamment Acxiom et Oracle (qui font l'objet d'une plainte distincte de Privacy International), avec lesquels Quantcast partage des identifiants de cookies pour synchroniser les identifiants et intégrer des segments d'audience, comme en témoigne la réponse aux demandes d'accès reçue par les membres du personnel de Privacy International. Toutefois, ces partenaires ne constituent pas une liste (exhaustive ou tout court, étant donné la forme dans ) de clients Quantcast. Il est donc impossible de comprendre dans quelle mesure les données Quantcast des individus sont partagées une première fois, puis partagées à nouveau. De plus, les réponses aux demandes d'accès reçues par les membres du personnel de Privacy International montrent également que les données Oracle Cloud intégrées proviennent d'autres sociétés telles que Affinity Answers (Royaume-Uni), Experian UK et Mastercard UK.

73. Tapad indique qu'elle partage des données avec des « plateformes de clients et de partenaires », à savoir des « spécialistes du marketing et des fournisseurs de technologies informatiques ». Cependant, « en raison d'obligations de confidentialité, nous ne pouvons pas vous fournir le nom de nos clients et partenaires ».

74. Le nombre de destinataires et l'incapacité des entreprises à fournir des détails peuvent être en partie imputables à la nature du secteur et à son mode de fonctionnement. Cependant, en fin de compte, le manque de transparence quant à la partie avec laquelle les données sont partagées ne fait qu'aggraver la nature opaque du traitement, et empêche les personnes concernées de comprendre comment leurs données sont utilisées et partagées, ainsi que les conséquences concrètes que ces pratiques ont pour ces personnes.

75. Les informations fournies par les entreprises quant aux tiersavec lesquels elles partagent des données à caractère personnel ne répondent pas aux normes requises par le principe de transparence énoncé à l'article 5 du RGPD (tel qu'il est précisé dans les orientations du GT29). Toutes les sociétés devraient fournir d'emblée davantage d'informations, d'une manière qui serait plus pertinente pour les personnes concernées. Les catégories de destinataires fournies sont vastes et vagues, sans les détails spécifiques requis par l'avis du GT29.

76. De plus, l'utilisation de catégories ou segments dans ce contexte ne fait qu'exacerber le problème du partage colossal de données, problème qui découle du courtage de données à grande échelle. Pour respecter l'objet et le but du RGPD, des informations plus spécifiques identifiant les destinataires seraient nécessaires pour que les personnes concernées puissent exercer leurs droits.

Profilage

77. Le processus de profilage est souvent invisible pour la personne concernée. Il fonctionne en créant des données dérivées, déduites ou prévues sur des individus - des données à caractère personnel « nouvelles », souvent extrêmement sensibles et intrusives, qui n'ont pas été fournies directement par la personne concernée. Lier des données entre elles constitue également du profilage. Par exemple : lorsque ces sociétés déduisent qu'en raison de certaines caractéristiques, un appareil est lié à un autre (pistage entre ou inter- appareils), il s'agit également de profilage.

78. Le considérant 60 du RGPD déclare que « la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci ».

79. Le GT29 précise : « Compte tenu du principe fondamental de transparence qui sous-tend le RGPD, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé. En particulier, lorsque le traitement implique une prise de décision fondée sur le profilage (indépendamment du fait qu'il relève ou non des dispositions de l'article 22), le fait que le traitement vise à la fois a) le profilage et b) la prise de décision fondée sur le profil généré doit être clairement indiqué à la personne concernée. »[63]

80. Comme indiqué ci-dessus, le modèle commercial de ces trois sociétés est basé sur le profilage. Cependant, il existe un manque flagrant de transparence quant à leur profilage. Il n'est pas expliqué clairement et simplement.

81. Criteo, mis à part le fait qu'elle spécifie explicitement ne pas créer de segments pour (cibler) les enfants, ne fournit aucune information sur la manière dont elle profile/segmente les autres personnes dont les données à caractère personnel sont traitées. Cela tombe bien en-dessous de la norme requise par le RGPD.

82. Quantcast a fait quelques efforts en répondant aux demandes d'accès pour fournir des détails sur le type de segments/inférences qu'elle crée/fait (voir l'annexe B), mais ses réponses nécessitent d'avantage d'explications quant aux conditions selon lesquelles le sexe, l'âge, le niveau d'éducation, le revenu d'une personne concernée et le fait qu'il ait des enfants ou non, ont été déduits, ainsi que sur quelle base légale. De plus, Quantcast traite d'autres données de profil/segmentation provenant, elles, de partenaires tels qu'Acxiom et Oracle, et qui semblent à leur tour traiter des données provenant d'autres sociétés, telles que MasterCard et Experian. Cela peut inclure des données relatives aux centres d'intérêt d'achat, p. ex. « Alcool à domicile_Dépensier_considérable » et « psychographiques et styles de vie ». Cela peut aussi inclure des segments tirés de Mosaic d'Experian et de Personicx d'Acxiom, tels que « Riche, mondain et sage », « Dependent

[63] P16 - Directives du GT29 sur la prise de décision et le profilage automatisés individuels aux fins du règlement 2016/679, disponibles à l'adresse suivante : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Greys », etc.[64] Ceci est profondément problématique, comme indiqué dans la plainte jointe de Privacy International contre ces deux sociétés (Experian et Acxiom).

83. Tapad déduit « l'éligibilité de l'appareil pour les segments basés sur l'intérêt et la démographie », fournit des informations et des « déductions sur les intérêts des utilisateurs pour les clients et les partenaires afin de leur permettre de cibler la publicité, de personnaliser le contenu, d'analyser les comportements et de proposer d'autres services similaires ». Tapad traite également les profils/segments d'autres partenaires, comme indiqué dans les exemples de BlueKai et d'Exelate ci-dessus. Cependant, Tapad ne fournit aucune information sur les profils/segments qu'elle créée et seuls des exemples de segments sont fournis par certains partenaires. Même les exemples fournis soulèvent des questions, exposées plus en détail dans la présente soumission, en termes de loyauté et de base légale, y compris pour les données à caractère personnel sensibles. Par conséquent, les autorités chargées de la protection des données doivent mener une enquête plus approfondie.

84. En vertu du RGPD, ces sociétés sont tenues de fournir aux personnes concernées des informations concises, intelligibles et facilement accessibles sur le traitement de leurs données à caractère personnel aux fins de l'établissement de profils et de toute décision qui pourrait être fondée sur le profil généré :

> « Si le but inclut la création de données à caractère personnel déduites, le but recherché de la création et du traitement ultérieur de telles données à caractère personnel déduites ainsi que les catégories de données déduites traitées doivent toujours être communiqués à la personne concernée au moment de la collecte ou avant le traitement ultérieur pour un nouveau but. »[65]

85. Compte tenu en particulier de l'ampleur de l'activité de profilage de ces entreprises, des informations beaucoup plus détaillées devraient être fournies. Ces sociétés doivent définir clairement le profilage, les données utilisées pour faire de telles déductions, leur source, toutes les déductions relatives à des préférences et caractéristiques sensibles, avec qui les profils sont partagés et la base légale de chacun de ces traitements. Ces sociétés, en particulier Criteo et Tapad, ne sont pas suffisamment claires sur ces points ; elles ne sont pas proactives dans la communication de ces informations aux personnes dont elles traitent les données, et elles ne disposent pas d'une base légale valide, comme indiqué dans la présente soumission.

86. Le GT29 a clairement indiqué que plus le traitement est intrusif (ou moins attendu), plus il est important de fournir des informations aux individus préalablement au traitement (conformément aux articles 13 et 14). Les

[64] Voir la description des données Quantcast d'un membre du personnel : https://privacyinternational.org/feature/2429/quantcast
[65] Directives du GT29 sur la transparence, page 14, note de bas de page 30.

personnes ne devraient pas avoir à parcourir les politiques de confidentialité de ces sociétés ou à faire des demandes d'accès pour recevoir des informations sur le traitement de leurs données.

Implications pour les droits

87. Ce manque de transparence sur la manière dont, le cas échéant (dans le cas de données de catégorie spéciale), Criteo, Quantcast et Tapad collectent des données et les utilisent a également des implications pour l'exercice des droits des personnes concernées (y compris les droits à l'information et d'accès) qui constituent le noyau du RGPD. Le groupe des commissaires à la protection des données à caractère personnel de Berlin (‘ci-après le Groupe de Berlin’) a déclaré dans son document sur le Big Data :

> « La plupart des gens ne connaissent pas beaucoup d'acteurs opérant sur ce marché, en particulier les courtiers de données et les sociétés d'analyse. Ainsi, le droit de la personne concernée de demander l'accès à l'information devient difficile à exercer. »[66]

88. Au moins deux problèmes en découlent.

89. Tout d'abord, lorsque les données sont collectées, les personnes concernées ignorent souvent que cela se produit et que ces informations seront collectées par l'une de ces sociétés AdTech ou par un courtier de données, comme Acxiom, Oracle ou Experian, puis qu’elles seront combinées à d'autres données collectées en fonction de leur activité en ligne par des sociétés AdTech, telles que celles faisant l’objet de la présente plainte, pour fournir des profils détaillés permettant de les cibler. Il est essentiel que lorsque les sites Web et d’autres clients et partenaires fournissent des données à ces sociétés, ils le fassent savoir aux individus. Il incombe également aux sociétés AdTech et aux courtiers avec lesquels elles travaillent d’informer les personnes concernées par les données à caractère personnel traitées et de s’assurer de ne recevoir que les données dont elles sont convaincues qu’il existe une base légale pour leur obtention. Cela est essentiel pour satisfaire le droit à l'information énoncé aux articles 13 et 14 du RGPD, ainsi que pour l'obligation de disposer d'une base légale.

90. Deuxièmement, même lorsqu'une personne concernée soupçonne, ou sait, que ces sociétés ont obtenu ou rassemblé des données le concernant, leur incapacité à fournir des informations complètes dans leurs politiques de confidentialité et en réponse aux demandes concernant à la fois l'origine des données (la source) et les parties avec lesquelles elles ont été partagées (les destinataires), et pourquoi et comment une personne a été classée dans certaines catégories (profilage), rend l'exercice de ses droits relatif au traitement des données à caractère personnel auprès de ces autres parties

---

[66] Groupe de Berlin - Document de travail sur le Big Data et la confidentialité, Les principes de confidentialité sous pression à l'ère de l'analyse du Big Data (Skopje, 5./6. Mai 2014), disponible à l'adresse https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf

extrêmement difficile et lui laisse peu de contrôle sur les données à caractère personnel que ces sociétés traitent.

91. Même lorsqu'une source ou un destinataire potentiel est identifiable, la personne concernée doit se lancer dans une quête des demandes d'accès longue et difficile, allant d'une société à l'autre, sans savoir à quelles données spécifiques se rapporte l'implication de cette société. Quand il s'agit de demandes d'accès en rapport avec le profilage, les informations fournies sont limitées ou inexistantes. Il incombe donc à une personne concernée de deviner ce qui l'a amené à être catégorisé de la sorte et quelles en sont les conséquences. Ce manque de transparence exacerbe le déséquilibre de pouvoir existant entre ces entreprises et les personnes concernées.

92. L'ICO, le CPD et la CNIL devraient examiner dans quelle mesure ces sociétés respectent pleinement les droits des personnes concernées, notamment le droit d'accès, en particulier l'accès aux profils/segments qui concernent une personne.

***b) Loyauté***

93. La loyauté est un principe fondamental du RGPD et doit être examinée plus avant par les APD, dans ce contexte.

94. Le manque de transparence, l'ignorance des personnes quant à l'identité des tiers qui traitent leurs données, comment et à quelles fins, est intrinsèquement lié à la loyauté. Le principe de loyauté inclut l'obligation de prendre en compte les attentes raisonnables des personnes concernées, les effets que le traitement peut avoir sur elles et leur capacité à exercer leurs droits en ce qui concerne ces informations.

95. Le 25 octobre 2018, l'ICO a condamné Facebook à une amende du montant maximal prévu par la loi de 1998 sur la protection des données à caractère personnel pour violation du premier principe de protection des données : la loyauté. Le comportement infractionnel consistait à autoriser Facebook (dans ce cas-ci l'application) à fonctionner de manière à collecter des données à caractère personnel sur les amis Facebook des utilisateurs de l'application, sans que ces amis Facebook soient informés de la collecte de telles données et sans être invités à consentir à une telle collecte de données. L'ICO a constaté que les personnes concernées ne s'attendaient pas à ce que leurs données à caractère personnel soient collectées de cette manière en raison du choix fait par d'autres personnes d'utiliser une application particulière, et Facebook aurait dû informer la personne concernée de la nature des données recherchées, de la manière dont elles seraient utilisées et donner à la personne concernée la possibilité de donner ou de refuser son consentement.

96. Des considérations similaires (c'est á dire, relatives á la loyauté) peuvent et devraient être appliquées à Criteo, Quantcast et Tapad. Les personnes concernées ne sont souvent pas informées que leurs données sont collectées ou comment elles seront utilisées, et quelles en sont les conséquences potentielles. La collecte de centaines de points de données sur les individus,

à l'aide d'obscures technologies , via des sources inconnues, par une entreprise dont ils n'ont jamais entendu parler et avec qui ils n'ont pas de relation directe, dans le but de les profiler pour ensuite partager ces « informations » avec des centaines d'autres entreprises, ne fait pas partie des attentes raisonnables des individus. Il est extrêmement difficile pour les personnes concernées d'échapper à la portée de la prévalence de ces pistages des entreprises sur les sites Web et sur les applications. C'est au contraire aux individus, s'ils se rendent compte à un moment donné que leur activité est suivie de cette manière par ces entreprises, de modifier leurs paramètres d'appareil, d'installer des extensions de navigateur ou d'utiliser les options de retrait basées sur les cookies spécifiques à une entreprise, qui sont intrinsèquement problématiques, comme indiqué plus en détail ci-dessous. **Ce fardeau ne devrait pas être supporté par la personne concernée**, et la question de la loyauté est aggravée par les difficultés que les personnes concernées rencontrent dans l'exercice de leurs droits en matière de données à caractère personnel.

97. Une enquête plus approfondie est nécessaire quant à l'effet que produit sur les personnes concernées les pratiques en matière de données à caractère personnel de ces sociétés, en particulier le profilage.

98. Les orientations du GT29 sur le profilage fournissent l'exemple suivant de ce qui ne satisferait pas aux exigences de l'article 5, paragraphe 1, alinéa a) du RGPD, à la fois en termes de transparence et de loyauté :

> « Un courtier de données vend à des sociétés financières des profils de consommateurs sans le consentement de ceux-ci ou sans connaître les données sous-jacentes. Les profils classent les consommateurs en catégories (avec des qualificatifs tels que « profil rural ayant du mal à joindre les deux bouts », « difficultés en milieu urbain-profil ethnique de deuxième génération », « débuts difficiles : jeunes parents célibataires ») ou « les placent dans une catégorie spécifique », en mettant l'accent sur la vulnérabilité financière des consommateurs. Les sociétés financières proposent à ces consommateurs des prêts sur salaire et d'autres services financiers « non traditionnels » (prêts à taux élevé et autres produits financièrement risqués). »

99. Comme indiqué ci-dessus, ces entreprises s'engagent activement dans le profilage, leur activité consistant à relier des données afin de mieux comprendre les personnes concernées. Ils déduisent quels appareils sont utilisés par une personne (pistage inter-appareils), leur sexe, leur âge, leur revenu, leurs intérêts et bien plus encore. Toutes ces entreprises pratiquent le pistage d'appareils, mais à l'exception de Quantcast, elles ne divulguent aucune information sur les segments démographiques qu'elles utilisent pour cibler des individus.

100. Pour continuer avec l'exemple du ciblage basé sur les circonstances financières fourni par le GT29, nous savons que Quantcast déduit le revenu des personnes concernées sur base de leur historique de navigation. Tapad et Criteo quant à eux ne fournissent aucune information sur la manière dont

les déductions démographiques sont générées, et peuvent donc également profiler les personnes concernées en fonction de leur situation financière.

101. En outre, les courtiers de données partenaires de ces sociétés établissent un profil et segmentent les personnes concernées en fonction de leur situation financière, notamment Acxiom, Oracle et Experian (contenant des segments de données figurant dans les données du partenaire Quantcast reçues par les membres du personnel de Privacy International), Blue Kai (appartenant à Oracle) qui est répertorié en tant que partenaire de Tapad, et l'autre exemple de partenaire de Tapad « Exelate », qui inclut des catégories telles que « prêts » et « dette ». Acxiom, Oracle et Experian font déjà l'objet d'une plainte distincte de Privacy International. Criteo, Quantcast et Tapad, partagent des profils/données avec de nombreux destinataires non identifiés permettant de cibler des personnes à des fins publicitaires, ce qui pourrait inclure de la publicité en fonction de la situation financière. Ceci laisse craindre que les annonceurs publicitaires puissent cibler des personnes en situation financière précaire.[67] Ces sociétés ne fournissent pas suffisamment d'informations pour distinguer leurs activités de l'exemple non-conforme fourni par le GT29 cité ci-dessus.

102. Il n'y a pas que les publicités ciblées basées sur des circonstances financières, qui peuvent paraître déloyales. Comme indiqué par l'EDPS dans son avis sur la manipulation en ligne : « En limitant l'exposition à certaines informations (comme par exemple l'exposition à certaines offres d'emploi) sur la base du sexe de la personne ou en déduisant son 'état de santé, elles [ces sociétés] risquent de perpétuer des attitudes et des pratiques discriminatoires ».[68] Par conséquent, une enquête plus approfondie sur les pratiques et les garanties de ces sociétés est nécessaire.

### c) Licéité et base légale (article 6 du RGPD)

103. Le premier principe de protection des données énoncé à l'article 5, paragraphe 1, alinéa a), exige que les données à caractère personnel soient traitées légalement et l'article 6 du RGPD dresse une liste exhaustive des bases légales sur lesquelles les données à caractère personnel peuvent être traitées. Parmi celles-ci, seules deux des bases spécifiées sont potentiellement applicables à la majorité des traitements effectués par des sociétés AdTech telles que Criteo, Quantcast et Tapad :

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques (« consentement ») (article 6, paragraphe 1, alinéa a)) ;
- 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, ce qui exigent une protection des données à caractère personnel,

[67] https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/
[68] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf

notamment lorsque la personne concernée est un enfant (« intérêts légitimes ») (article 6, paragraphe 1, alinéa f)).

104. À ce jour, et dans la mesure où elles sont impliquées dans ce dossier, Criteo, Quantcast et Tapad ont cherché à présenter la nature de leurs activités de manière à ce qu'elle soit en adéquation avec ces deux bases légales. Toutefois, au vu des éléments de preuve disponibles, il est clair qu'il n'existe aucune base légale pour tout ou partie du traitement effectué par ces sociétés. Il y a donc une violation à première vue, sur laquelle les autorités en charge de la protection des données doivent se pencher davantage.

105. Un problème majeur est le manque de précision quant à la base légale sur laquelle ces sociétés s'appuient pour réaliser leurs différentes opérations de traitement. En dépit des questions spécifiques de Privacy International, elles affirment toutes qu'elles se fient vaguement aux variations du consentement et des intérêts légitimes, sans faire un effort concerté pour le décomposer. Cela soulève des problèmes non seulement en ce qui concerne le RGPD, mais également en ce qui concerne la législation sur la protection de la vie privée, étant donné qu'une grande partie des données que ces entreprises traitent sont obtenues via l'accès à des appareils individuels. Dans la mesure où ces sociétés cherchent à s'appuyer sur un intérêt légitime pour le traitement des données de cookies, elles ne disposent pas d'une base légale valable.

Consentement

106. Le consentement en tant que base légale doit fonctionner de manière à permettre aux personnes concernées de contrôler et de choisir la manière dont leurs données à caractère personnel sont traitées. L'article 4, paragraphe 11 du RGPD définit le « consentement » aux fins du RGPD comme suit : « 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. »

107. Les considérants 42 à 43 développent les préoccupations sous-jacentes à ces exigences :

« (42) Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement. En particulier, dans le cadre d'une déclaration écrite relative à une autre question, des garanties devraient exister afin de garantir que la personne concernée est consciente du consentement donné et de sa portée. Conformément à la directive 93/13/CEE du Conseil (10), une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et elle ne devrait contenir aucune clause abusive. Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement

auquel sont destinées les données à caractère personnel. Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée **ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement** sans subir de préjudice.

(43) Pour garantir que le consentement soit donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un **déséquilibre manifeste** entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. **Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à cette exécution/prestation**. » (Emphase ajoutée)

108. Lorsque le traitement est basé sur le consentement, l'article 7 du RGPD établit des conditions supplémentaires auxquelles un responsable du traitement doit se conformer pour que ce consentement soit valide. En voici quelques-unes :

i. « 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. » Cela signifie que les entreprises ne peuvent pas simplement se fier au fait que les clients ont donné leur consentement. Ils doivent plutôt lire les consentements, indiquer clairement que le consentement obtenu (y compris la langue) est valable et s'étend à leurs activités ;
ii. « Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante. »
iii. « Il est aussi simple de retirer que de donner son consentement. »
iv. Le consentement devrait être donné librement (il ne devrait pas être obtenu à la suite d'un déséquilibre des pouvoirs). En particulier, « il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. »

109. Les orientations du GT29 sur le consentement révisées à la lumière du RGPD (Revised Guidance on Consent)[69] donnent un aperçu utile quant à la signification de ces exigences en pratique. En résumé, le consentement doit être :

- **Donné librement** - cela signifie qu'il ne doit pas y avoir de déséquilibre de pouvoir entre le responsable du traitement et la personne concernée ; que le consentement n'est pas conditionnel ; que le consentement est granulaire (c'est-à-dire qu'il ne confond pas les finalités du traitement) ; et qu'il doit être possible pour la personne concernée de refuser sans préjudice.
- **Spécifique** - le responsable du traitement doit appliquer la spécification de l'objet comme protection contre le détournement de fonction ; les demandes de consentement doivent être granulaires et clairement séparer les informations relatives à l'obtention du consentement des informations relatives à d'autres questions.
- **Informatif** - les directives du GT29 énumèrent un minimum d'informations nécessaires à l'obtention d'un consentement valable. Les directives précisent également que, lorsque « … les données doivent être transférées ou traitées par d'autres responsables du traitement qui souhaitent pouvoir compter sur le consentement initial, ces organisations doivent toutes être nommées ».
- **Sans ambigüité quant à l'indication des souhaits de la personne concernée** - c'est là qu'un individu, par une déclaration ou par une action affirmative claire, signifie qu'il accepte le traitement des données à caractère personnel le concernant. La personne concernée doit avoir pris une mesure délibérée pour consentir au traitement en question.

110. Le GT29 souligne que « Les responsables du traitement qui cherchent à se fonder sur le consentement pour procéder à un profilage devront démontrer que les personnes concernées comprennent exactement ce à quoi elles consentent, et se rappeler que le consentement n'est pas toujours une base appropriée pour le traitement. Dans tous les cas, les personnes concernées devraient disposer de suffisamment d'informations pertinentes sur l'utilisation envisagée et les conséquences du traitement pour garantir que leur consentement représente un choix éclairé. » [70]

*Criteo*

111. Comme indiqué à l'annexe A, dans sa politique de confidentialité, Criteo se fonde sur le consentement pour collecter des données à caractère personnel sur la base du fait que ses clients et partenaires ont informé la personne concernée et collecté son consentement à l'utilisation de cookies (ou d'autres technologies de pistage) dans le but d'offir une publicité ciblée, par exemple via une bannière dédiée. Or, ceci est insuffisant. Aucune preuve n'a été fournie que le consentement était :

[69] Directives du GT29 sur le consentement aux fins du règlement 2016/679, (Novembre 2017) disponibles à: http://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=623051

[70] Page 13 - Directives du GT29 sur la prise de décision et le profilage automatisés individuels aux fins du règlement 2016/679, disponibles à: http://ec.europa.eu/newsroom/article29/item- detail.cfm?item_id=612053

- « Donné librement » : il était probablement subordonné à l'accès à un site Web ;
- « Spécifique » : c'est-à-dire granulaire en ce qu'il était distinct des autres consentements et qu'il était clair pour l'utilisateur cliquant sur « accepter » (si c'était toutefois une option) qu'il consentait au traitement de ses données par Criteo et par tous ceux avec lesquels Criteo les partage en vue de réaliser de la publicité comportementale inter-appareils ;
- « Informatif » : les lacunes dans la transparence du traitement de Criteo ont déjà été exposées ci-dessus et il est donc difficile de savoir si la personne qui a donné son consentement a été pleinement informée. De plus, le GT29 indique clairement que pour que le consentement original soit utilisé pour partager les données avec d'autres parties, ces dernières doivent être nommées ; pourtant, Criteo compte des milliers de clients et de partenaires qu'il ne souhaite pas nommer ;
- « Sans ambiguïté » : Criteo n'a pas démontré quelle action délibérée avait été entreprise par les membres du personnel de Privacy International dont il traitait les données.

112. Criteo fait partie du cadre de transparence et de consentement de l'IAB et Privacy International a également des préoccupations à ce propos et fait déjà l'objet d'une plainte auprès de l'ICO et du CPD.

113. En outre, le mécanisme de « retrait » de Criteo ne répond pas aux normes de l'article 7, paragraphe 3 du RGPD, à savoir qu'il doit être aussi simple de retirer que de donner son consentement. Même si le consentement était obtenu, les options fournies par Criteo pour le retrait du consentement sont insuffisantes. Bien que Criteo offre la possibilité de se désabonner de tous les navigateurs liés pour « l'environnement Web en ligne », Criteo s'appuie sur une option de désactivation basée sur les cookies, ce qui signifie que si la personne concernée supprime ensuite les cookies, ce qui est une pratique typique en matière de sécurité et confidentialité prise par les individus, elle est ensuite tenue de se désabonner (par opposition à abonner) du traitement effectué par Criteo, encore et encore. La politique de confidentialité de Criteo indique : « Vous devez vous désabonner à nouveau si vous supprimez ce cookie d'un navigateur, utilisez un navigateur non lié ou utilisez un nouvel appareil pour accéder à Internet. »

114. Pour ces raisons, Criteo ne dispose pas du consentement valide en vertu du RGPD.

*Quantcast*

115. Comme indiqué ci-dessus, le problème est le manque de précision de la part de ces sociétés quant à la base légale applicable aux traitements. Dans cette optique, la politique de confidentialité de Quantcast ne précise pas laquelle de ses opérations de traitement repose sur le consentement.

116. Les données renvoyées au personnel de Privacy International par Quantcast en réponse aux demandes d'accès incluent, avec leur historique

de navigation, une colonne intitulée « gdprQCConsent ». Cela ne prouve pas en soi qu'un consentement valide a été obtenu.

117. Nous supposons qu'il s'agit de l'outil de gestion du consentement « Quantcast Choice » de Quantcast, qui est l'un des produits qui préoccupe Privacy International. Les préoccupations relatives au consentement énoncées ci-dessous sont illustrées plus en détail dans la description des données Quantcast relatives à un membre du personnel.[71] Elles sont également référencées ci-dessous en rapport aux intérêts légitimes énoncés, compte tenu du manque de clarté de Quantcast quant à la base légale utilisée dans chaque cas.

118. Dans la mesure où le consentement repose sur l'outil de gestion du consentement de Quantcast, nous nous demandons si le consentement obtenu est valide.

119. Tout d'abord, le consentement doit être donné librement. Cependant, la conception même de la solution Quantcast Choice incite par défaut les utilisateurs à accepter, en cliquant sur « J'accepte », le bouton le plus grand et le plus visible. À moins qu'un site Web, qui s'appuie sur le cadre de consentement Quantcast, ait choisi d'inclure l'option « Je n'accepte pas », les utilisateurs ne peuvent que refuser le pistage (ou obtenir plus d'informations sur les objectifs et les personnes avec lesquelles les données sont partagées) en cliquant sur le bouton ambigu et beaucoup moins visible appelé « Afficher les objectifs ». Les personnes concernées ont ensuite la possibilité de consulter la liste complète des fournisseurs, qui peut contenir des centaines de sociétés tierces qui utilisent les données à des fins différentes, telles que la mise en correspondance de données avec des sources hors connexion, la liaison d'appareils ou la collecte de données de localisation géographique précise). Certaines implémentations de Quantcast Choice sont fournies avec des cases de consentement pré-cochées, permettant aux parties premières et tierces d'effectuer un pistage. De plus, si l'on combine ces faits à l'absence de bouton de refus clair dans la zone de consentement initiale, cela entraîne un processus fastidieux, dans lequel les utilisateurs doivent se désabonner, au lieu de s'abonner. Ce consentement n'est pas valide en vertu du RGPD.

120. Une autre préoccupation concerne le concept de consentement global. Selon Quantcast : « Le consentement global signifie que si un utilisateur définit les préférences de consentement sur un autre site à l'aide du consentement global, ces préférences s'appliqueront à votre site et l'utilisateur ne verra la fenêtre de consentement que s'il doit donner son consentement à d'autres fournisseurs. Le consentement défini sur votre site s'appliquera à d'autres sites utilisant le consentement global. »[72] En d'autres termes, chaque fois qu'un utilisateur clique sur « J'ACCEPTE » sur l'un des 10 000 sites utilisant Quantcast Choice, cela est interprété comme une autorisation de pistage par des tiers sur l'entièreté du Web. Le nombre de trackers tiers ('third-party trackers') utilisés par les éditeurs et les propriétaires

[71] https://privacyinternational.org/feature/2429/quantcast
[72] https://help.quantcast.com/hc/en-us/articles/360003814853-Technical-Implementation-Guide

de sites peut varier considérablement, Quantcast.com utilisant lui-même 429 trackers tiers individuels. Le cadre de consentement de Quantcast est conçu pour inciter les consommateurs à donner leur consentement et il est beaucoup plus facile pour eux de donner leur consentement que de le refuser. Par conséquent, il ne faut pas s'étonner que, selon Quantcast, le taux de consentement moyen des consommateurs dépasse 90 %,73 ce qui soulève des questions quant à la possibilité pour les utilisateurs d'exercer efficacement en pratique leur droit de rejeter le consentement .

121. Cela soulève également la question de savoir dans quelle mesure cette forme de « consentement global » peut toujours être librement donnée, informative, spécifique et non ambiguë. Une personne est incitée à donner son consentement à des centaines d'entreprises (qui manquent de transparence, ce qui vaut aussi pour Tapad et Criteo) traitant leurs données à caractère personnel à travers l'entièreté du Web à des fins innombrables.

122. Il s'agit d'un problème inhérent à Quantcast Choice, à la solution et à la forme de consentement global préconisée dans le cadre de transparence et de consentement de l'IAB. Privacy International a également soulevé cette question dans la soumission jointe concernant Oracle. La plainte que l'ICO et le CPD ont déjà reçue concernant le cadre IAB décrit que, du fait de son fonctionnement, une personne concernée perd le contrôle de ses données :

> « Une fois perdu, le contrôle de ces données est perdu à jamais dans l'éther de courtage de données… Ces données sont ensuite transmises à un vaste écosystème de courtiers de données et d'annonceurs publicitaires. Ces tiers peuvent ensuite utiliser les données de la manière qu'ils déterminent, sans que la personne concernée puisse avoir son mot à dire, sans aucune connaissance ni aucun contrôle sur leur utilisation ultérieure. Les utilisations de telles données sont vastes ; elles peuvent être fusionnées avec d'autres données, ou les données peuvent être utilisées pour le profilage de la personne concernée à de nombreuses fins. Les utilisations finales de ces données peuvent donc être des utilisations qui n'ont pas été exprimées par le responsable du traitement dans son interaction avec la personne concernée. De telles utilisations finales peuvent être pénibles pour la personne concernée, si jamais elle devait le savoir. En effet, il n'existe aucun moyen pour le responsable du traitement d'exprimer toutes les utilisations finales puisque ce dernier n'a plus aucun contrôle sur ce qu'il advient des données une fois qu'elles sont transmises. Le problème est inhérent à la manière dont l'industrie est conçue. »

123. Par conséquent, il est impossible pour une personne concernée de donner un consentement libre, spécifique et éclairé au traitement de Quantcast basé sur le choix de Quantcast, et celui-ci ne respecte pas le seuil défini dans le RGPD.

---

[73] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-choice-powers-one-billion-consumer-consent-choices/

124. Privacy International continuera à se pencher sur la question et à en rendre compte. Toutefois, comme cette forme de solution de « consentement global » (telle que celle proposée par Quantcast) prolifère sur le Web, elle nécessite des examens supplémentaires de la part des APD.

*Tapad*

125. Tapad s'appuie sur le consentement pour obtenir des données à caractère personnel d'un appareil. « Pour stocker et accéder aux informations stockées sur l'appareil d'un utilisateur (ce que l'on appelle des cookies), le **consentement** doit être obtenu. Pour ce "consentement aux cookies", Tapad s'appuie sur les fournisseurs de sites Web (éditeurs) et les oblige contractuellement à ne transmettre que les données obtenues légalement. Tapad remplit ainsi son obligation découlant de la directive « vie privée et communications électroniques ».

126. Tapad a raison de dire que pour stocker et accéder aux informations stockées sur un appareil, un utilisateur doit donner son consentement conformément à la directive ePrivacy. Cependant, Tapad ne fournit aucune preuve qu'un consentement valide a bien été obtenu. Tapad ne recueille pas le consentement directement, mais se fie aux éditeurs pour obtenir ce consentement. Tapad fait partie du cadre de transparence et de consentement de l'IAB. Les préoccupations concernant le consentement global dans le cadre de l'IAB ont déjà été exposées ci-dessus.

127. Aucune preuve démontrable du consentement n'a été fournie à Privacy International par Tapad, que ce soit pour le consentement de l'IAB ou autrement. Aucune preuve n'a été fournie que le consentement était :

- « Donné librement » : il était probablement subordonné à l'accès à un site Web ;
- « Spécifique » : c'est-à-dire granulaire en ce qu'il était distinct des autres consentements et qu'il était clair pour l'utilisateur cliquant sur « accepter » (si c'était toutefois une option) qu'il consentait au traitement de ses données par Tapad et par tous ceux avec lesquels Tapad les partage en vue de réaliser de la publicité comportementale inter-appareils ;
- « Informatif » : les lacunes dans la transparence du traitement de Tapad ont déjà été exposées ci-dessus et il est donc difficile de savoir si la personne qui a donné son consentement a été pleinement informée. De plus, le GT29 indique clairement que pour que le consentement original soit utilisé pour partager les données avec d'autres parties, ces dernières doivent être nommées ; pourtant, Criteo compte des milliers de clients et de partenaires qu'elle ne souhaite pas nommer ;
- « Sans ambiguïté » : Tapad n'a pas démontré quelle action délibérée de consentement avait été entreprise par les membres du personnel de Privacy International dont il traitait les données.

128. Cela dit, il semble que Tapad cherche en grande partie à faire appel à un « intérêt légitime » plutôt qu'au consentement. Cependant, le fait que

Tapad s'appuie sur le consentement pour accéder à certaines données (et se conformer à la confidentialité), puis sur un intérêt légitime (comme indiqué ci-dessous) pour le reste du traitement est intrinsèquement problématique et soulève diverses questions quant à la validité de chacune des deux bases légales.

129. Nonobstant la validité de la base légale du consentement, il est préoccupant qu'il soit beaucoup plus facile d'« adhérer » ('opt-in') au traitement des données à caractère personnel par Tapad que de « refuser de participer » ('opt-out'). Cela ne répond pas aux normes de l'article 7, paragraphe 3 du RGPD selon lequel il doit être aussi simple de retirer que de donner son consentement. Tandis que Tapad offre la possibilité de se désabonner via son site Web, une personne doit d'abord identifier le traitement des données par Tapad, localiser le désabonnement dans la politique de confidentialité de Tapad et se désabonner sur chaque appareil et navigateur. Tapad s'appuie sur une option de désabonnement basée sur les cookies, ce qui signifie que si la personne concernée supprime ensuite les cookies (ce qui est une pratique typique en matière de sécurité et de confidentialité prise par les individus), elle est ensuite tenue de désactiver ('opt-out of') (par opposition à activer ('opt-in')) le traitement effectué par Tapad encore et encore, comme expliqué dans Politique de confidentialité de Tapad : « … si vous essayez de vous désabonner en effaçant les cookies ou en supprimant le cache du contenu de votre appareil, Tapad ne sera pas en mesure de savoir que vous vous êtes désabonné sur cet appareil. Si vous visitez ultérieurement l'un des sites Web partenaires de Tapad, vous pourriez alors obtenir un nouveau cookie Tapad. »

130. Pour ces raisons, Tapad ne dispose pas de consentement valide en vertu du RGPD.

Intérêt légitime

131. L'ICO a décrit l'intérêt légitime comme la base légale la plus « flexible ».74 Cependant, cela ne signifie pas qu'il est illimité ou qu'il peut être moulé pour s'adapter à (ou justifier) toute opération de traitement. Le traitement doit satisfaire un test en trois parties. Le responsable du traitement doit identifier un intérêt légitime (finalité) ; montrer que le traitement est nécessaire pour y parvenir (nécessité) ; et l'équilibrer avec les droits et libertés de la personne concernée (équilibrage).

132. Dans son explication des intérêts légitimes en tant que base légale, l'ICO signale que :

- Cela convient probablement davantage lorsque le responsable du traitement utilise les données des personnes de la manière attendue, avec un impact minimal sur la vie privée ou lorsqu'il existe une justification convaincante.

[74] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

- Si un responsable du traitement choisit de s'appuyer sur des intérêts légitimes, il assume une responsabilité supplémentaire en ce qui concerne le respect et la protection des droits des personnes.
- Les responsables du traitement doivent conserver une trace de leurs évaluations des intérêts légitimes
- Les responsables du traitement doivent inclure les détails des intérêts légitimes dans les informations de confidentialité

133. S'il est reconnu que le terme est vague, les directives de l'ICO indiquent clairement que l'« intérêt légitime » doit être clair et spécifique. « Démontrer que vous avez un intérêt légitime signifie […] que vous (ou un tiers) devez avoir un avantage ou un résultat clair et spécifique en tête. Il ne suffit pas de s'appuyer sur des intérêts commerciaux vagues ou génériques. Vous devez penser spécifiquement à ce que vous essayez d'atteindre avec l'opération de traitement en question. »75 Un intérêt légitime doit être « licite », « suffisamment articulé » et « représenter un intérêt réel et actuel ».76

134. Le considérant 47 du GDPR explique que :

« Les intérêts légitimes d'un responsable du traitement, y compris ceux d'un responsable du traitement à qui les données à caractère personnel peuvent être communiquées, ou d'un tiers peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il **existe une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement ou est à son service**. En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée. Les intérêts et droits fondamentaux de la personne concernée pourraient, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur […] Le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime. » (Emphase ajoutée)

135. En outre, l'avis du GT29 reconnaît la pertinence de l'ampleur du traitement des données pour évaluer l'impact du traitement :

---

[75] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

[76] GT29 « Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement selon l'article 7 de la directive 95/46/CE » https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf wp217_fr.pdf

« L'analyse d'impact au sens large peut consister notamment à examiner si les données ont été publiées ou rendues accessibles par quelque autre moyen à un grand nombre de personnes, ou si des volumes considérables de données à caractère personnel sont traités ou combinés avec d'autres données (par exemple, en cas d'établissement de profils, à des fins commerciales, judiciaires, ou autres). Le traitement à grande échelle de **données apparemment anodines et leur combinaison avec d'autres données peuvent parfois permettre des inférences à propos de données plus sensibles**… En plus de conduire potentiellement au traitement de données plus sensibles, une telle analyse peut également conduire à des prédictions étranges, inattendues et parfois aussi inexactes, concernant par exemple le comportement ou la personnalité des personnes concernées. **En fonction de la nature et de l'impact de ces prédictions, cela peut être très intrusif pour la vie privée de la personne concernée**. »[77] (Emphase ajoutée)

136. L'avis d'intérêt légitime du GT29 de 201478 indique que « les responsables du traitement peuvent avoir un intérêt légitime à connaître les préférences de leurs clients afin de leur permettre de mieux personnaliser leurs offres et d'offrir à terme des produits et des services mieux adaptés aux besoins et désirs de leurs clients ». L'avis précise ensuite :

« Cela ne signifie pas pour autant que les responsables du traitement pourraient invoquer l'article 7, point f), **pour surveiller indûment les activités en ligne ou hors ligne de leurs clients, pour compiler d'importants volumes de données à leur propos en provenance de différentes sources, collectées à l'origine dans d'autres contextes et à des fins différentes, et pour créer – mais aussi, par exemple, échanger en passant par des courtiers en informations – des profils complexes concernant la personnalité et les préférences des clients, sans les en informer ni mettre à leur disposition un mécanisme fonctionnel permettant d'exprimer leur opposition, pour ne rien dire de leur consentement éclairé**. Une telle activité de profilage risque de constituer une **violation grave de la vie privée du client** et, dans ce cas, l'intérêt et les **droits de la personne concernée prévaudraient sur l'intérêt poursuivi par le responsable du traitement**. » (Emphase ajoutée)

137. Les directives du GT29 sur la prise de décision et l'établissement de profils individuels automatisés aux fins79 du RGPD indiquent clairement que le présent avis reste pertinent en vertu du RGPD et qu'il serait difficile pour les responsables du traitement de justifier l'utilisation d'intérêts légitimes comme base légale pour le profilage intrusif et les pratiques de pistage à des fins de marketing ou de publicité, par exemple celles qui impliquent le pistage de personnes sur plusieurs sites Web, emplacements, appareils, services ou

[77] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[78] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[79] Directives du GT29 sur la prise de décision et le profilage automatisés individuels aux fins du règlement 2016/679, disponibles à l'adresse suivante : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

courtage de données. Cependant, comme indiqué ci-dessous, Criteo, Quantcast et Tapad s'appuient sur des intérêts légitimes à ces fins-là.

138. En outre, il va de soi que les entreprises ne peuvent pas considérer leurs besoins commerciaux / la poursuite de leurs modèles commerciaux comme synonymes d'« intérêts légitimes ». Le simple fait qu'un organisme puisse avoir besoin de procéder à un profilage intrusif pour gagner de l'argent en contrepartie de ses services n'est pas suffisant. **Comme l'indique clairement le considérant 47 du RGPD, ce qui est légitime devrait être fondé au moins en partie sur le fait de servir ou non un intérêt légitime en raison de la relation entre le responsable du traitement et la personne concernée**.

139. Pourtant, ces sociétés, qui n'ont pas de relations directes avec des particuliers, ont cherché à utiliser la base de l'intérêt légitime pour justifier tout et n'importe quoi, sans tenir dûment compte du fait que la vie privée et le droit à la protection des données à caractère personnel sont des droits fondamentaux.80

*Criteo*

140. La politique de confidentialité de Criteo ne mentionne pas la base d'intérêt légitime. Toutefois, en réponse à une demande d'un membre du personnel de Privacy International, il a été mentionné que « Criteo a un intérêt légitime à traiter les données afin de respecter ses obligations contractuelles envers ses clients et partenaires ». Le fait que cette base ne soit pas mentionnée dans la politique de confidentialité de Criteo suggère que Criteo ne peut plus compter sur cette base. Toutefois, dans la mesure où Criteo cherche à s'appuyer sur des intérêts légitimes pour le traitement de données à caractère personnel pour ses services de publicité ciblés, Privacy International considère que ces intérêts sont invalides. Criteo s'appuie sur des intérêts commerciaux vagues et génériques, sans démontrer aucune considération pour les droits des individus.

*Quantcast*

141. La politique de confidentialité de Quantcast stipule que Quantcast utilise des données à caractère personnel pour fournir ses services, dans la mesure nécessaire à ses intérêts légitimes, notamment : « fournir, améliorer et personnaliser les services offerts à nos partenaires et vous fournir des publicités et du contenu pertinents, sauf si ces intérêts sont remplacés par vos intérêts ou libertés et droits fondamentaux qui exigent la protection des informations personnelles ». En outre, Quantcast « peut partager vos informations (telles que décrites dans la présente politique de confidentialité)

[80] Art. 8 (1) de la Charte des droits fondamentaux de l'Union européenne, art. 16(1) du traité sur le fonctionnement de l'Union européenne (TFUE), art. 1(2) et considérant 1 du RGPD.

si nécessaire pour défendre nos intérêts légitimes et ceux de nos partenaires en diffusant une publicité plus utile et plus pertinente ».

142. Les « intérêts légitimes » de Quantcast ne sont ni clairs ni spécifiques, mais font plutôt référence aux activités et services commerciaux au sens large. Tout ce que Quantcast souhaite faire pour exploiter commercialement les données collectées est jugé comme légitime car il est nécessaire de fournir des services autodéterminés à des fins lucratives.

143. Cependant, Quantcast recueille des informations en temps réel, via Internet, sur les caractéristiques du public et affirme pouvoir le faire sur plus de 100 millions de sites Web. Quantcast traite donc les données à caractère personnel de millions de personnes, de leur historique de navigation aux segments dans lesquels les autres courtiers de données les ont placées. Quantcast a pour tâche de rassembler de vastes zones de données afin de fournir des informations sur la démographie, les intérêts, les attributs et les préférences des personnes concernées (comme indiqué dans la majorité des cas, sans transparence). Il est donc essentiel que les intérêts et les droits des personnes concernées soient dûment pris en compte.

144. Un membre du personnel de Privacy International décrit le tableau que Quantcast a pu obtenir sur sa vie, à partir des données recueillies.[81] Ses données Quantcast combinent une grande partie de son historique de navigation. Quantcast en déduit son sexe, son âge, la présence d'enfants dans son ménage (le nombre d'enfants et leur âge), son niveau d'éducation et le revenu annuel brut de son ménage en dollars US et en livres sterling. Afin de cibler ses publicités avec davantage de précision, Quantcast l'a également classée dans des catégories beaucoup plus détaillées, dont les noms suggèrent que les données ont été obtenues par des courtiers de données comme Acxiom et Oracle, mais également par MasterCard et par des agences de référencement de crédit telles qu'Experian. Certaines catégories sont étrangement spécifiques, d'autres moins. Même avec un accès à ces données - un accès que la plupart des utilisateurs ne pourront pas obtenir, car la demande d'accès impliquait l'obtention d'un identifiant de cookie - il est toujours impossible de comprendre pleinement comment et pourquoi les données se sont retrouvées dans ce profil. Cependant, il n'y a aucun doute qu'elles donnent un aperçu très spécifique de la vie d'une personne concernée à un moment donné (c'est la raison même pour laquelle Quantcast fait ceci). Privacy International a déjà mis en doute la validité du consentement pour ce traitement. Toutefois, aucun intérêt légitime ne constitue une base valide pour cette forme de profilage intrusif.

145. Pour qu'un intérêt légitime soit valide, il faut déterminer si une personne avait des « attentes raisonnables », à l'époque et dans le contexte de la collecte de données à caractère personnel, pour que les données à caractère personnel puissent être utilisées à des fins de publicité et de marketing. La protection des données à caractère personnel et la vie privée sont des droits fondamentaux. Il est invraisemblable (et il est inacceptable de

[81] https://privacyinternational.org/feature/2429/quantcast

le présumer) que les « attentes raisonnables » des personnes concernées étaient que toutes leurs recherches en ligne, tous leurs articles de presse ou blogs lus, toutes les applications utilisées, seraient partagées avec des milliers d'entreprises et associées à d'autres données les concernant (par l'intermédiaire de courtiers en données), afin de créer un profil détaillé sur ces personnes dans le but de les cibler avec de la publicité personnalisée et basée sur leur comportement, encore et encore, par le biais de leurs appareils. En fait, l'Eurobaromètre montre le contraire: la confidentialité de leurs informations personnelles, de leurs communications en ligne et de leur comportement en ligne sont des facteurs très importants pour la majorité des répondants. En outre, près des deux tiers des personnes interrogées ont estimé qu'il était inacceptable d'avoir un accès illimité à un certain site Web seulement en échange du suivi de ses activités en ligne.[82]

146. Pourtant, malgré ce vaste traitement de données à caractère hautement personnel, Quantcast ne fournit que de vagues assurances sur les garanties, et l'affirmation que les intérêts de Quantcast ne passeront pas outre les intérêts des personnes concernées, leurs droits et leurs libertés fondamentales, est sans fondement et ne fournit aucune preuve démontrable que ce soit le cas. Quantcast n'explique pas réellement comment elle prend en compte les droits et les attentes raisonnables des individus. Aucune évaluation de l'intérêt légitime n'est disponible, ou, du moins, n'a été rendue publique ou n'a été transmise en réponse aux demandes d'accès en question, et aucune analyse d'impact sur la protection des données n'a été fournie (comme indiqué ci-dessous). Comme cela a été signalé précédemment, le droit à la vie privée et à la protection des données est un droit fondamental et Quantcast n'a pas réussi à établir que ses intérêts commerciaux ne l'emportaient pas sur ceux-ci.

147. Le GT29 a expressément indiqué que l'intérêt légitime ne constituait pas une base légale acceptable sur laquelle une entreprise telle que Quantcast puisse s'appuyer :

> « À cet égard, il est utile de rappeler l'avis du groupe de travail sur la limitation de la finalité, dans lequel il est spécifiquement indiqué que " lorsqu'un organisme souhaite analyser ou prédire spécifiquement les préférences, le comportement et les attitudes personnels de ses clients, qui informeront par la suite des 'mesures ou décisions' qui sont prises à l'égard de ces clients... un consentement libre, spécifique, informé et sans ambiguïté devrait être presque toujours requis, sans quoi un autre usage ne pourrait être considéré comme compatible. **Il est important de noter qu'un tel consentement devrait être requis**, **par exemple, pour le pistage et le profilage à des fins de marketing direct, de publicité comportementale, de courtage de données, de publicité géolocalisée**

[82] L'EuroBaromètre de la Commission européenne de 2016, une vaste majorité de répondants ont déclaré leur désaccord sur le partage en ligne d'informations personnelles avec des tiers, Commission européenne, Flash Eurobaromètre 443, « e-Privacy Report » (décembre 2016), https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy

**ou d'étude de marché numérique basée** sur le pistage." »[83] (Emphase ajoutée)

148. Le traitement des données à caractère personnel par Quantcast ne respecte pas le seuil de l'article 6, paragraphe 1, alinéa f) du RGPD. En conséquence, dans la mesure où Quantcast s'appuie sur un « intérêt légitime » en tant que personne morale, le traitement et le profilage des données à caractère personnel de millions de personnes concernées sur la base de cette condition enfreint directement le RGPD et les directives du GT29.

*Tapad*

149. Tapad s'appuie sur un « intérêt légitime » pour « poursuivre le traitement et la création du graphe d'appareils en fonction de diverses données (y compris les données de cookie susmentionnées) ». Tapad utilise l'**intérêt légitime** comme base légale pour le traitement. Par ce biais, Tapad remplit son obligation aux fins du RGPD, car le traitement dépasse le placement initial du cookie. L'intérêt légitime du traitement de Tapad est la personnalisation des communications promotionnelles destinées aux internautes, qui fait partie intégrante de l'écosystème en vertu duquel le contenu Internet librement disponible est financé par les recettes publicitaires. » Comme indiqué à l'annexe C, Tapad fait également référence aux intérêts légitimes des « spécialistes du marketing qui souhaitent commercialiser leurs produits » et qu'elle « aide à diffuser et à mesurer une publicité personnalisée » afin de servir les intérêts légitimes des annonceurs publicitaires.

150. De même que pour Criteo et Quantcast, Tapad a cherché à faire coïncider ses activités (qui sont dans son intérêt personnel) et celles de ses partenaires avec la base légale de l'intérêt légitime, sans tenir pleinement compte des droits des individus.

151. Les données fournies en réponse aux demandes d'accès adressées à Tapad par les membres du personnel de Privacy International étaient les moins détaillées des trois companies, comprenant seulement des données limitées quant à certaines URL et applications utilisées. Toutefois, cela ne signifie pas pour autant que l'image que Tapad a d'une personne concernée et les déductions qu'elle en tire sont moins intrusives que les autres sociétés susmentionnées, compte tenu de l'objectif sous-jacent du traitement de Tapad. Tapad a au moins confirmé qu'une « évaluation complète de l'impact sur la protection des données » et un « test d'équilibrage approfondi » avaient été effectués, avec des facteurs tels que « la transparence, une variété d'options de retrait appropriées et faciles d'accès, ainsi que le traitement strict de données uniquement pseudonymes ». Cependant, comme indiqué précédemment, nous avons des inquiétudes concernant la transparence, les options de retrait offertes et les nombreuses informations qui peuvent être obtenues sur une personne concernée à partir de données pseudonymes.

[83] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (p47)

Par conséquent, Privacy International a des préoccupations similaires concernant le fait que Tapad s'appuie légalement sur les intérêts légitimes.

152. Tapad a expliqué : « Selon le considérant 47 du RGPD, le marketing direct peut être considéré par la société de publicité comme étant réalisé pour répondre à un intérêt légitime. Cela doit par conséquent s'appliquer à fortiori au suivi pseudonyme sur Internet, où, contrairement au marketing mené par le spécialiste du marketing, l'identité réelle de la personne concernée est inconnue. »

153. Au contraire, comme indiqué dans l'avis du GT29 précité, l'intérêt légitime n'est pas considéré comme une base valide « **pour le traçage et le profilage à des fins de prospection directe, de publicité comportementale, de courtage en informations, de publicités fondées sur la localisation ou d'étude de marché numérique fondée sur le traçage. »**

Données à caractère personnel sensibles / spéciales (article 9 du RGPD)

154. L'article 9, paragraphe 1 du RGPD stiple que « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits », sauf si l'une des conditions strictement définies à l'article 9, paragraphe 2, est remplie. Dans le contexte d'un courtier de données commercial, la seule condition potentiellement applicable est le consentement explicite de la personne concernée (article 9, paragraphe 2, alinéa a) du RGPD).

155. Comme le note le Groupe de Berlin, plus il y a de données disponibles pour l'analyse, plus il est probable que des données de catégorie spéciale soient révélées :

> « Un aspect difficile associé à l'analyse du Big Data est le fait que la compilation d'informations collectées, qui peuvent ne pas être sensibles en soi, peut générer des données sensibles. Grâce aux outils Big Data, il est possible d'identifier des modèles permettant de prédire les dispositions des personnes, par exemple en matière de santé, de points de vue politiques ou d'orientation sexuelle. Cela constitue une information soumise à une protection spéciale. »[84]

156. Le profilage peut créer des données de catégorie spéciale par déduction, à partir de données qui ne constituent pas une catégorie spéciale

[84] Groupe de Berlin - Document de travail sur le Big Data et la confidentialité, Les principes de confidentialité sous pression à l'ère de l'analyse du Big Data (Skopje, 5./6. Mai 2014), disponible à l'adresse https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2014/06052014_en.pdf

en soi, mais qui le deviennent lorsqu'elles sont combinées avec d'autres données.

157. L'ICO a reconnu que les données supposées/prédites pouvaient bénéficier de la protection de données de catégorie spéciale : « Une opinion sur l'appartenance ethnique d'une personne a de fortes chances d'être qualifiée de "données de catégorie spéciale" en droit, et en tant que tel une base légale au sens de l'article 6 et une condition de traitement au titre de l'article 9 du règlement général sur la protection des données doit être identifiée... »[85]

158. Comme indiqué ailleurs dans la présente soumission, des données apparemment anodines, lorsqu'elles sont traitées à grande échelle et combinées avec d'autres données, peuvent conduire à des déductions sur des données plus sensibles.

159. Criteo, Quantcast et Tapad insistent sur le fait qu'ils ne traitent pas de données à caractère personnel sensibles ou de catégorie spéciale. Pourtant, étant donné la grande quantité de données traitées par ces sociétés et la manière dont les personnes sont profilées et classées, Privacy International considère que par le profilage (à la fois par le biais de catégories qui sont intrinsèquement sensibles et à travers les détails sensibles qui peuvent être révélés par la combinaison des données)[86], ces entreprises traitent effectivement de données qui révèlent des données à caractère personnel de catégorie spéciale, sans base légale au sens de l'article 9 du RGPD. Voici quelques exemples :

160. Les réponses de Criteo aux demandes d'accès des membres du personnel ont démontré que l'entreprise traitait des données à caractère personnel révélant des données à caractère personnel de catégorie spéciale. Un membre du personnel, par exemple, a appris, via une demande d'accès, que Criteo traite des URL qui révèlent des informations détaillées sur son état de santé.[87]

161. En plus des données de navigation, qui peuvent révéler des données sensibles, Quantcast traite également des données de segments provenant de partenaires. Ces catégories comprennent des segments sur la « psychographie et le style de vie » d'une personne concernée qui sont intrinsèquement sensibles, comme indiqué dans les plaintes jointes de Privacy International contre Experian, Oracle et Acxiom. Quantcast a également traité des segments pouvant révéler des données à caractère personnel de catégories spéciales, par exemple sur la relation d'une personne concernée avec l'alcool :

---

[85] Rapport du COI intitulé Democracy Disrupted disponible à l'adresse suivante : https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[86] Comme indiqué dans chaque annexe A, B et C

[87] L'URL partagée par la société avec un membre du personnel PI était la suivante : https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc

- DATA_SEGMENT:Acxiom UK:Shopping Interests:Fast Moving Consumer Goods:Buyers:Alcohol at Home Heavy Spenders
- DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Going to the Pub

162. Tapad utilise également les données provenant de partenaires. La liste des partenaires Tapad n'est pas exhaustive et les deux exemples cités, Blue Kai et eXelate, incluent diverses catégories liées à la santé, notamment « Réhabilitation » dans la liste Blue Kai. Dans la liste eXelate figurent les intérêts concernant les services financiers relatifs aux dettes et aux emprunts, ainsi que les organisations religieuses ; les catégories diverses incluent des références à l'origine raciale ou ethnique, par exemple la communauté asiatique.

163. Comme indiqué ci-dessus, le traitement par ces sociétés manque de transparence et de consentement valable. Par conséquent, ils ne disposent d'aucune base légale au titre de l'article 9 du RGPD pour le traitement de catégories spéciales de données à caractère personnel. Par conséquent, à tout le moins, cette question nécessite un processus complet d'enquête et d'évaluation par les APD afin de s'assurer que ces affirmations des sociétés sont bien étayées, compte tenu des préoccupations exprimées ci-après.

### *(2) Principe 2 : Limitation de la finalité*

164. L'article 5, paragraphe 1, alinéa b) du RGPD exige que les données à caractère personnel soient « collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités… (« limitation de la finalité ») ».

165. L'avis 03/2013 du GT29 sur la limitation[88] de la finalité indique clairement que toute finalité doit être : **spécifiée** avant et en tout état de cause au plus tard au moment où la collecte de données à caractère personnel a lieu et les finalités doivent être identifiées de manière précise et complète ; **explicite**, suffisamment claire et sans ambiguïté et clairement exprimée (c'est-à-dire sans but caché) ; et **légitime**, conformément à la loi et aux attentes raisonnables de la personne concernée.

166. L'évaluation de la compatibilité de la finalité du traitement nécessite de prendre en compte le contexte dans lequel les données ont été collectées et les attentes raisonnables de la personne concernée en matière d'utilisation ultérieure, ainsi que la nature des données et leur impact sur la personne concernée. De manière générale, il convient également, le cas échéant, de prendre en compte la nature de la relation entre le responsable du traitement et la personne concernée. Toutefois, Criteo, Quantcast et Tapad n'ont pas de relations directes avec les personnes dont elles traitent les données à caractère personnel. Cela signifie que les courtiers de données doivent s'assurer que les données qu'ils traitent ne sont traitées que de manière

[88] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

compatible avec les objectifs spécifiés par le responsable du traitement d'origine.

167. Dans son avis sur la manipulation en ligne, le CEPD[89] a réaffirmé l'importance de la limitation de la finalité dans le contexte du profilage, en notant que :

> « L'inquiétude que suscite l'utilisation, au moyen d'algorithmes, de données issues de profils pour d'autres finalités est de voir ces données perdre leur contexte original. Le fait de donner une nouvelle finalité aux données affectera probablement l'autonomie informationnelle de chacun, continuera de diminuer le contrôle exercé par les personnes concernées sur leurs données, mettant ainsi à mal la confiance envers les environnements et les services numériques. D'où l'importance cruciale de la limitation de la finalité comme principe de la législation relative à la protection des données. » [90]

168. « Les analyses de données comprennent des méthodes et des schémas d'utilisation que ni l'entité qui collecte les données ni la personne concernée ont envisagé ou auraient pu imaginer au moment de la collecte. Le traitement algorithmique des données à caractère personnel permet de générer de nouvelles données. Lorsque la personne concernée partage quelques données discrètes, il est souvent possible que ces données soient fusionnées, ce qui génère une deuxième, voire une troisième, génération de données sur cette personne. »[91]

169. Les objectifs de Criteo, Quantcast et Tapad sont de définir de nouvelles finalités et de réutiliser les données pour profiler et fournir des « informations » afin que leurs clients puissent cibler les utilisateurs avec une publicité personnalisée en fonction de leur comportement. Ceci est en contradiction directe avec le principe de limitation de la finalité. Ces sociétés ne sont pas en contact direct avec des personnes et les finalités pour lesquelles elles traitent des données à caractère personnel (comme indiqué aux annexes A, B et C) sont extrêmement vagues et différentes de la finalité pour laquelle la personne a initialement fourni ses données, à savoir l'accès à du contenu en ligne, mais aussi d'autres activités recueillies par des courtiers de données.

170. Les finalités énoncées aux annexes A, B et C ne sont pas suffisamment spécifiques et explicites, pas plus qu'elles ne démontrent qu'elles ont été communiquées à la personne concernée. Aucune justification n'a été fournie pour expliquer pourquoi ces sociétés considèrent que les finalités pour lesquelles elles traitent des données à caractère personnel répondent aux attentes raisonnables des personnes concernées et sont compatibles avec la finalité initiale du traitement (par exemple, le moment où la personne concernée a fourni les données à la personne concernée au responsable du traitement d'origine).

---

[89] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf
[90] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf
[91] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf

171. Les politiques de confidentialité des sociétés mentionnent qu'elles ont mis en place certaines garanties relatives au traitement ultérieur, telles que demander par contrat à des tiers de fournir des données obtenues légalement[92]ou afficher des politiques de confidentialité adéquates et protéger de toute autre manière les droits de confidentialité de leurs visiteurs.[93]

172. Cependant, aucun détail n'est fourni concernant ces mesures contractuelles, techniques et organisationnelles. Elles ne précisent pas non plus quels processus ont été mis en place pour vérifier que les données qu'elles obtiennent elles-mêmes d'autres responsables du traitement peuvent être utilisées pour les propres besoins des courtiers de données ou pour vérifier que les parties avec qui sont partagées les données respectent les prétendues mesures de protection. Cela est particulièrement pertinent dans ce secteur et auprès de ces entreprises, compte tenu de la multiplicité des sources et des destinataires.

173. L'existence (ou non) de tels processus, leur fonctionnement, les garanties fournies par les entreprises et leur audit sont des domaines sur lesquels l'ICO devrait enquêter davantage. En particulier, sachant que, en vertu de l'article 82 du RGPD, chaque contrôleur ou responsable du traitement est tenu responsable des dommages dans leur totalité.

(3) ***Principe 3 : Minimisation des données***

174. L'article 5, paragraphe 1, alinéa c) du RGPD exige que les données à caractère personnel soient « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».

175. Alors que les entreprises peuvent chercher à minimiser les données qu'elles stockent, en limitant les périodes de conservation des données, les modèles commerciaux de Criteo, Quantcast et Tapad sont basés sur la maximisation des données, l'antithèse du principe de minimisation des données. Les produits proposés par ces sociétés sont conçus pour maximiser la quantité d'informations sur les personnes concernées afin d'analyser, de profiler, d'évaluer, de catégoriser et d'informer les décisions qui sont prises à leur sujet. Par exemple, Criteo affirme sa capacité à capturer les données d'identité et d'intérêt de 1,4 milliard de clients actifs par mois ; Quantcast affirme collecter des informations en temps réel sur les audiences de plus de 100 millions de sites Web et Tapad prétend analyser des milliards de signaux provenant de milliards d'appareils.

***(4) Principe 4 : Exactitude***

[92] https://www.tapad.com/privacy-policy
[93] https://www.quantcast.com/privacy/

176. L'article 5, paragraphe 1, alinéa d) du RGPD exige que les données à caractère personnel soient « exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ».

177. Les dangers d'un profilage inexact ont été signalés par l'ICO en ce qui concerne l'ethnicité. Dans Democracy Disrupted, l'ICO a déclaré : « À notre avis, il existe un risque important que des hypothèses ou des prévisions concernant l'appartenance ethnique d'une personne soient inexactes et, une fois directement attribuées à une personne, elles pourraient constituer des informations personnelles inexactes, ce qui pourrait constituer une violation potentielle de l'article 5, paragraphe 1, alinéa d) du règlement général sur la protection des données. »[94]

178. Les directives du GT29 indiquent clairement que les responsables du traitement doivent considérer l'exactitude à chaque étape du traitement et doivent introduire des mesures robustes pour vérifier et garantir que les données réutilisées ou obtenues indirectement sont exactes et à jour.[95]

179. Les responsables du traitement ont l'obligation de s'assurer de l'exactitude des données. Le profilage à l'aide de le machine learning', toutefois, est intrinsèquement probabiliste. Le profilage établit simplement une corrélation et, en conséquence, ne peut que déterminer qu'une personne concernée est hautement susceptible d'être une femme, susceptible d'être insolvable ou solvable, ou non susceptible d'être marié, hétérosexuel ou introverti. Même un niveau élevé d'exactitude ne prévient pas complètement les faux positifs et les faux négatifs. Si les responsables du traitement ne peuvent pas garantir que le profilage utilisant le machine learning produit des données précises, cela soulève des questions quant à leur pertinence. Pourtant[96], Criteo, Quantcast[97] et Tapad font[98] tous de la promotion du machine learning un élément central de leurs activités.

180. L'un des risques inhérents au profilage du consommateur et à l'adaptation probabiliste d'identité inter-appareil, auquel participent les trois sociétés, est que les identités et les segments qui en résultent sont inexacts. Dans ce contexte, il est important de souligner que les personnes peuvent être affectées tout autant et de la même manière que ce soit par les données inexactes ou par les données exactes que les entreprises détiennent à leur insu.

181. Les segments des partenaires, par exemple dans les données Quantcast fournies aux membres du personnel, contenaient des évaluations

---

[94] https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

[95] Directives du GT29 sur la prise de décision et le profilage automatisés individuels aux fins du règlement 2016/679, page 12, disponibles à l'adresse suivante : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[96] http://labs.criteo.com/2015/08/large-scale-machine-learning-at-criteo/

[97] https://www.quantcast.com/ai/

[98] https://www.tapad.com/the-tapad-graph

erronées concernant leur situation financière ; leur mode de vie ; et le fait d'avoir ou non des enfants. Étant donné que ces données sont partagées et utilisées par un nombre et des catégories de destinataires non divulgués, ces inexactitudes peuvent avoir des conséquences variables. Il peut être tout simplement possible que des annonces publicitaires ne les intéressent pas. Cependant, il existe également de nombreux exemples documentés de l'impact significatif de la publicité ciblée sur les personnes concernées. Par exemple une mère dont le bébé est mort-né peut recevoir des publicités liées aux bébés/parents.[99] Les directives du GT29 sur la prise de décision et le profilage automatisés des individus permettent de reconnaître que la publicité ciblée peut avoir des effets importants.[100]

182. Comme indiqué ci-dessus, le recours à des méthodes probabilistes (en particulier à des techniques telles que le machine learning) présente un risque inhérent de pouvoir déduire l'identité (sur plusieurs appareils), les centres d'intérêt, les informations démographiques et le comportement des personnes. Par définition, de telles déductions seront parfois fausses pour certaines personnes.

183. Nous considérons par conséquent que Criteo, Quantcast et Tapad traitent des données inexactes concernant des personnes, y compris par le biais de l'établissement de profils, en violation de leurs obligations en vertu de l'article 5, paragraphe 1, alinéa (d) du RGPD.

**(5) Principe 6 - Intégrité et confidentialité**

184. L'ICO et le CPD ont déjà reçu une plainte concernant le secteur de la publicité comportementale, qui représente l'une des principales préoccupations concernant les cadres et les politiques en vigueur dans ce secteur. Cela inclut le cadre de transparence et de consentement d'IAB Europe utilisé par Criteo, Quantcast et Tapad, qui affirme qu'ils n'offrent pas de protection adéquate contre la divulgation et le traitement non autorisés et potentiellement illimités de données à caractère personnel.[101]

185. Cela nécessite une enquête plus approfondie de la part des APD dans le contexte du traitement effectué par ces sociétés.

*Prise de décision individuelle automatisée avec profilage (article 22 du RGPD)*

186. L'article 22 du RGPD dispose que « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. »

187. Le GT29 affirme que la décision de présenter une publicité ciblée sur la base du profilage peut entrer dans le champ d'application de l'article 22 car

---

[99] https://www.bbc.co.uk/news/av/uk-45901514/facebook-baby-ads-taunted-me-after-stillbirth
[100] P22, directives du GT29 - Prise de décision et profilage automatisés
[101] https://brave.com/ICO-Complaint-.pdf et https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf

elle peut affecter de manière significative des individus.[102] Cela dépendra des caractéristiques particulières du cas, notamment :

- l'intrusion du processus de profilage, y compris le pistage d'individus sur différents sites Web, appareils et services ;
- les attentes et les souhaits des personnes concernées ;
- la façon dont la publicité est délivrée ; ou
- l'utilisation de la connaissance des vulnérabilités des personnes concernées.

188. L'avis fournit une illustration supplémentaire de ceci :

« Un traitement qui pourrait avoir peu d'incidences sur les personnes en général peut en fait avoir un effet significatif à l'égard de certains groupes de la société, tels que les groupes minoritaires ou les adultes vulnérables. Par exemple, une personne dont il est connu qu'elle éprouve des difficultés financières ou qui est susceptible d'éprouver de telles difficultés, et qui est régulièrement ciblée par des publicités pour des prêts à taux d'intérêt élevé, peut s'inscrire à ces offres et s'endetter davantage.

La prise de décision automatisée qui se traduit par des prix différentiels fondés sur des données à caractère personnel ou des caractéristiques personnelles pourrait également avoir un effet significatif si, par exemple, des prix prohibitifs empêchent effectivement une personne d'accéder à certains biens ou services.

La personne concernée pourrait également subir des effets l'affectant de manière significative de façon similaire, qui seraient déclenchés par les actions d'individus autres que celui auquel se rapporte la décision automatisée. Une illustration en est donnée ci-dessous. »[103]

189. Fournissant l'exemple suivant :

> Hypothétiquement, une société émettrice de cartes de crédit pourrait réduire la limite de crédit d'un client, non pas en fonction de ses propres antécédents de remboursement, mais en fonction de critères de crédit non traditionnels, comme une analyse d'autres clients vivant dans la même région qui font leurs courses dans les mêmes magasins.
>
> Cela pourrait signifier qu'une personne est privée d'opportunités en raison des actions de tiers.
>
> Dans un contexte différent, l'utilisation de ces types de caractéristiques pourrait avoir l'avantage d'accorder du crédit à ceux qui n'ont pas

[102] Directives du GT29 sur la prise de décision et le profilage automatisés individuels aux fins du règlement 2016/679, page 22, disponibles à l'adresse suivante : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[103] Directives du GT29 sur la prise de décision et le profilage individuels automatisés aux fins du règlement 2016/679, adoptées le 3 octobre 2017. Dernière révision et adoption le 6 février 2018

d'antécédents de crédit conventionnels et qui, autrement, se seraient vu refuser cette possibilité.

190. Criteo, Quantcast et Tapad traitent une grande quantité de données à caractère personnel concernant des individus. Leurs points de vue et profils sur les données démographiques des individus sont ensuite utilisés par leurs clients pour des publicités ciblées. Comme indiqué ci-dessus, nous savons que Quantcast déduit des données sur les revenus d'une personne concernée à partir de son historique de navigation et utilise également des segments de données de courtiers de données tels que Acxiom et Experian relatifs à la situation financière. Tapad utilise des segments de partenaires d'Exelate qui comprennent l'intérêt porté aux services financiers concernant les prêts et les dettes, et Criteo n'explique pas du tout ses profils. Ceci leur permet de faciliter le ciblage d'individus en fonction de leurs finances et bien plus encore, y compris des données à caractère personnel de catégorie spéciale, telles que la santé et l'origine ethnique, comme indiqué ci-dessus.

191. En partie à cause du manque de transparence, il est difficile de nommer toutes les décisions potentielles pouvant avoir des effets importants résultant des pratiques de ces entreprises. Toutefois, un examen plus approfondi de ces rôles, ainsi que des autres rôles et responsabilités d'AdTech au titre de l'article 22 du RGPD est nécessaire.

*Protection des données par conception et par défaut (article 25 du RGPD)*

192. Criteo et Tapad ont fourni de brefs détails en réponse aux questions de Privacy International concernant leur implémentation, ou non, de la protection des données par conception et par défaut. Les APD doivent toutefois examiner de manière plus approfondie la façon dont ces sociétés mettent en œuvre ces obligations, compte tenu des préoccupations exprimées dans la présente communication, notamment en ce qui concerne les principes de limitation de la finalité et de minimisation des données.

*Évaluations d'impact sur la protection des données (article 35 du RGPD)*

193. Les lignes directrices du GT29 sur l'évaluation de l'impact sur la protection des données[104] définissent les critères à prendre en compte en matière de traitement, susceptibles de présenter un risque élevé pour les droits et libertés de la personne physique, notamment les données traitées à grande échelle, la correspondance et la combinaison de jeux de données, l'évaluation ou la notation (par exemple une entreprise établissant des profils de comportement ou de marketing basés sur l'utilisation ou la navigation sur son site web), les données sensibles ou de nature très personnelle, le pistage systématique, la prise de décision automatisée avec des effets significatifs juridiques ou similaires, et l'utilisation innovante ou l'application de nouvelles solutions technologiques. Ces sociétés répondent à de multiples critères, comme cela a déjà été exposé dans la soumission, et toutes ces sociétés traitent les données de millions de personnes. Quantcast met en avant ses

[104] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

informations « axées sur l'IA », Criteo et Tapad encouragent leur utilisation des algorithmes de « machine learning ». Par conséquent, une analyse d'impact sur la protection des données est requise conformément à l'article 35 du RGPD. En réponse aux questions de Privacy International sur le fait de savoir si ces sociétés avaient effectué des évaluations d'impact sur la protection des données (avec une demande de copie), seul Tapad a confirmé avoir effectué une analyse d'impact sur la protection des données. Aucune copie n'a été fournie. Les APD doivent enquêter sur cette question et, dans la mesure du possible, la rendre publique.

## F. Recours - Avis d'évaluation

*Avis d'évaluation*

194. Pour toutes les raisons exposées ci-dessus, Privacy International demande à l'ICO, au CPD et à la CNIL d'enquêter sur les activités de traitement de données à caractère personnel de ces sociétés et d'exercer leurs pouvoirs respectifs en matière d'émission d'avis d'évaluation et d'enquêter sur ces compagnies sur base des plaintes de Privacy international à leur encontre.

195. Plusieurs aspects doivent être examinés dans le cadre d'une évaluation globale de la légalité des activités de traitement des données à caractère personnel poursuivies par Criteo, Quantcast et Tapad, en particulier en ce qui concerne le **profilage**. À savoir, si chaque entreprise se conforme aux points suivants :

- Le principe de **transparence**, notamment en ce qui concerne les sources, les destinataires et le profilage ;
- Le principe **de loyauté**, en particulier en tenant compte des attentes raisonnables de la personne, de l'absence de relation directe et de la nature opaque du traitement ;
- Le principe de **licéité**, qui repose notamment sur l'article 6 du RGPD, et qui indique si le fait que la société se base sur le **consentement** et/ou les **intérêts légitimes** est justifié ;
- L'évaluation du traitement par les deux sociétés des **données à caractère personnel de catégorie spéciale** (y compris par le biais de données présumées et indirectes et de la base légale au titre de l'article 9) ;
- Le principe de **limitation des finalités** ;
- Le principe de **minimisation des données** ;
- Le principe d'**exactitude** ;
- Le principe d'**intégrité et de confidentialité** ;
- **Les droits des personnes concernées**, notamment le droit à l'information, le droit d'accès, le droit d'effacement et les droits en matière de prise de décision automatisée, y compris le profilage en termes d'effets sur les personnes concernées.
- La mise en place de garanties, y compris **la protection des données à caractère personnel par défaut et par conception** ainsi que **les évaluations d'impact sur la protection des données**.

196. Nous prévoyons également que les APD pourraient exiger des mesures d'exécution supplémentaires afin de veiller à ce que les sociétés se conforment au RGPD à l'avenir.

197. Comme indiqué dans la présente soumission, l'un des problèmes majeurs posés par les activités de traitement de données de ces sociétés AdTech est l'échelle. Elles profilent, à tout moment, des millions de personnes à travers l'UE. Par conséquent, conformément aux dispositions relatives à la coopération et à l'assistance mutuelle du chapitre VIII du RGPD, et comme indiqué ci-dessus, nous invitons l'ICO, le CPD et la CNIL, dans le cadre de la présente enquête, à se concerter pour identifier une autorité principale et/ou intervenir dans le cadre des enquêtes sur les trois sociétés visées par cette plainte.

198. En outre, nous invitons également l'ICO, les APD et la CNIL à se concerter avec les autres autorités de contrôle de l'UE et à mener une enquête commune au titre de l'article 62 du RGPD. Avec d'autres organisations de la société civile, nous porterons ces préoccupations à l'attention d'autres APD, ainsi qu'à celle du Contrôleur européen de la protection des données à caractère personnel et du Comité européen de la protection des données à caractère personnel.

## Annexe A - Criteo

### A. L'activité de Criteo

1. Criteo est une plateforme publicitaire « spécialisée dans la publicité personnalisée » et proposant des outils pour les spécialistes du marketing et les éditeurs, allant de l'acquisition de clients à la correspondance avec l'audience, en passant par la publicité pour applications et des outils d'analyse et de conception. Criteo prétend capturer les données d'identité et d'intérêt de tous les acheteurs connectés à Criteo (72 % de tous les acheteurs en ligne dans le monde)[105] et avoir « une connaissance approfondie de plus de 1,4 milliard d'acheteurs actifs par mois »[106]. Criteo déclare disposer du « plus grand ensemble de données d'acheteurs ouvert au monde, ce qui signifie que la technologie du machine learning [de Criteo] dispose de toutes les informations détaillées nécessaires pour **prévoir avec précision** ce qui stimule les acheteurs et suscite un engagement plus fort ». (Emphase ajoutée). En particulier, nous nous intéressons aux produits suivants :

    - **Shopper Graph**[107] Cet outil fournit des données granulaires sur les acheteurs, y compris des informations hors ligne et en ligne, ainsi que des données inter-appareils pour un meilleur ciblage. Il donne également accès à des données d'achat récentes et détaillées, basées sur plus de 35 milliards d'historiques de navigation et de transactions quotidiennes provenant de près des trois quarts des acheteurs en ligne dans le monde. Il est soutenu par le **moteur Criteo** qui, lorsque les utilisateurs naviguent en ligne, utilise des données capturées précédemment et en temps réel (plus de 120 signaux d'achat) pour déterminer, à ce moment-là, la propension de l'acheteur à utiliser des produits, ainsi que la conception de publicité à laquelle il répondrait le mieux. Criteo indique que la « visibilité granulaire de l'interaction de l'acheteur avec les sites et les applications » leur permet de « prévoir avec précision ce qui stimule les acheteurs ».[108] Criteo appelle cela « le plus grand ensemble de données ouvert sur les acheteurs au monde ». Le Shopper Graph, qui attribue un identifiant Criteo à chaque individus, est basé sur 3 types de données : identité, intérêt et mesure.[109]
        i. Identité : représentée par un identifiant Criteo lié aux données de chaque utilisateur. Il est possible de récupérer ce contenu via des cookies propriétaires ou tiers, de liens sponsorisés ou d'une API.
        ii. Une carte des centres d'intérêts est établie à partir du pistage des utilisateurs du site Web / de l'application, ou à partir des habitudes d'achat fournies par les commerçants externes.
        iii. Les données de mesure suivent les ventes d'une campagne marketing spécifique et les relient à des jeux de données existants.

[105] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[106] https://www.criteo.com/technology/criteo-engine/
[107] https://www.criteo.com/technology/criteo-shopper-graph/
[108] https://www.criteo.com/insights/explained-data-in-the-criteo-engine/?slide=2
[109] https://www.criteo.com/insights/explained-criteo-shopper-graph/?slide=2

- **Dynamic Retargeting** Cet outil est décrit par Criteo comme un moyen de « ré-engage[r] les consommateurs à chaque étape de leur parcours d'achat grâce à des publicités vidéo et affichages personnalisés »[110]. Le reciblage dynamique repose sur la possibilité de suivre les utilisateurs sur différents appareils et de leur diffuser des publicités personnalisées « au bon moment dans le parcours de l'acheteur ».

2. La politique de confidentialité de Criteo[111] mentionne également l'existence de « technologies autres que les cookies » qu'elle utilise dans « dans des cas limités où les paramètres par défaut de votre navigateur ont pour but d'empêcher l'utilisation de cookies pour la personnalisation intersite**, mais seulement si vous avez expressément consenti à nos services de manière non-ambiguë (et avoir eu la possibilité de refuser ultérieurement).** ».

## B. Objectifs du traitement de données

3. La politique de confidentialité de Criteo[112] stipule qu'elle utilise des données à caractère personnel pour « afficher des publicités présentant des produits susceptibles de vous intéresser en nous appuyant sur votre comportement de navigation ou sur les recherches que vous avez effectuées récemment». Les données collectées par Criteo lui permet également d'analyser les tendances et d'identifier les intérêts des utilisateurs grâce à leur utilisation d'applications mobiles ou à leur historique de navigation.

4. La politique de confidentialité de Criteo fournit des exemples illustratifs (similaires à ceux fournis à Privacy International en réponse à ses demandes d'accès) :

   Exemple de publicité pour le produit « Criteo Dynamic Retargeting » : si vous visitez et parcourez le site Web / l'application mobile A, lors d'une visite en ligne ultérieure sur le site Web / l'application mobile B, vous verrez des publicités personnalisées en fonction de votre historique de navigation sur le site Web / l'application mobile A.

   Exemple de publicité pour le produit « Criteo Sponsored Products» : si vous effectuez une recherche sur le site Web de nos partenaires (« Produits sponsorisés Criteo »), vous verrez des publicités personnalisées en fonction de votre recherche sur ce site Web.

5. Criteo collecte non seulement des données à des fins publicitaires, mais également pour recueillir des informations et tirer des conclusions quant aux tendance des acheteurs :

   « Les données que nous collectons sont également utilisées à des fins de reportage, pour donner à nos clients et partenaires plus d'informations sur les performances de leurs campagnes publicitaires et pour améliorer les performances dans le temps. »

---

[110] https://www.criteo.com/fr/products/criteo-dynamic-retargeting/
[111] https://www.criteo.com/fr/privacy/
[112] https://www.criteo.com/fr/privacy/

6. Pour ce faire, Criteo utilise des cookies de pistage et des « technologies similaires » placés sur le navigateur de l'utilisateur ou via des identifiants publicitaires (via des applications mobiles).[113] Criteo « étiquette » ensuite les visiteurs sur les sites Web et les applications de ses partenaires. Criteo le fait sur tous les appareils utilisant la « synchronisation d'ID ».

## C. Types de données à caractère personnel

7. Les types de données à caractère personnel que traite Criteo sont répertoriés dans sa politique de confidentialité comme provenant à la fois de son 'réseau Criteo' et de 'partenaires approuvés' :

« Nous collectons des données relatives à votre activité de navigation via des cookies ou des identifiants publicitaires qui enregistrent :

- des événements liés à votre **activité sur le site Web de notre partenaire publicitaire** (tels que le nombre de pages consultées, les produits que vous avez consultés sur ce site Web, vos recherches effectuées sur le site Web du partenaire) ;
- des informations relatives à votre appareil (**type d'appareil, système d'exploitation, version**) ;
- des informations imprécises liées à **votre situation géographique** et dérivées de l'**adresse IP tronquée** de votre connexion (afin de vous diffuser des publicités uniquement pour des produits et services disponibles dans votre pays, région ou ville) ;
- et des événements liés à la diffusion de publicités Criteo, comme le nombre de publicités que vous recevez.

Nous recueillons également certaines informations automatiquement, notamment le **type de navigateur, les pages de renvoi/de sortie, les fichiers consultés sur notre site (pages HTML, graphiques, etc.), le système d'exploitation, la date et l'heure et/ou les données de parcours de navigation à des fins d'analyse des tendances et d'optimisation de nos services.**

Nous n'utilisons ni ne conservons aucune adresse IP complète à des fins de ciblage. Criteo n'utilisera vos adresses IP complètes qu'aux fins suivantes :

- détection des fraudes pour être plus facilement alerté de situations ne pouvant découler d'un comportement humain, comme un nombre très important de clics sur une période réduite;
- Attribution des ventes ;
- Rapports de marketing contenant des données agrégées.

Nous collectons également les identifiants utilisateurs techniques provenant de nos partenaires publicitaires afin de lier les différents navigateurs et applications mobiles que vous utilisez et vous montrer des publicités pertinentes s'appuyant sur votre comportement dans tous les environnements (« synchronisation des identifiants »). À cette fin, nous pouvons traiter et conserver :

- Criteo Dynamic Retargeting :
  - **les identifiants techniques de nos partenaires publicitaires, de votre identifiant du flux CRM ou de votre adresse e-mail : nous utilisons une technologie de double hachage de pointe pour garantir la non-réversibilité de vos informations, le hachage de votre adresse email correspondant à une série de caractères ne permettant pas de vous identifier (le hachage de nom@email.comdonnerait par exemple 98307a5ba02fa1072b8792f743bd8b5151360556b8e5a6120fa9a04ae02c88c0) ;**
  - **les identifiants publicitaires mobiles (comme l'identifiant IDFA d'Apple ou l'identifiant AAID de Google), qui sont des données techniques spécifiques**

[113] https://www.criteo.com/fr/privacy/

**créées par les fabricants de téléphones portables pour permettre de procéder aux personnalisations et à l'analyse des clients d'une manière sécurisée ne permettant pas d'identifier les utilisateurs ;**

- Criteo Sponsored Products
    - Identifiants techniques de nos partenaires publicitaires et/ou votre identifiant du flux CRM

Données collectées auprès de partenaires approuvés :

Nous pouvons collecter des **identifiants techniques auprès de tiers** afin d'améliorer notre synchronisation et de vous offrir une expérience en ligne sans failles. Ces partenaires approuvés s'engagent à ne partager que les informations relatives à la synchronisation des identifiants nous permettant de lier les cookies et/ou les identifiants mobiles et de proposer un mécanisme de choix efficace aux utilisateurs finaux (désabonnement).

Par exemple, les informations de linking provenant de nos partenaires peuvent être ID de cookie ABC = identifiant publicitaire IDFA d'Apple, 123 = valeur hachée MD5. Nos partenaires peuvent utiliser des méthodes probabilistes ou déterministes, mais dans tous les cas, veuillez noter que hormis les informations relatives à la synchronisation des identifiants, aucune autre donnée (qu'il s'agisse d'informations personnelles identifiables ou non identifiables) éventuellement collectée par nos partenaires dans le cadre de l'exécution de leurs services ne nous sera communiquée. En outre, nous exigeons de nos partenaires qu'ils proposent aux utilisateurs un moyen facile de désactiver la collecte et l'utilisation de leurs données. »[114]

8. Nous avons appris sur le site Web[115] de Criteo qu'elle collecte au moins les données suivantes sur le site Web et l'application mobile de son client publicitaire Cela a été confirmé par les données que nous avons reçues suite à notre demande d'accès :

    - Noms des sites Web consultés par les utilisateurs - liste des pages et des produits consultés, cliqués, mis en panier ou achetés sur les sites Web des clients publicitaires
    - URL des pages consultées par les utilisateurs ' referrer '),
    - Informations techniques agrégées relatives au navigateur et à l'appareil de l'utilisateur ('user agent')
    - Horodatage ou *Timestamp* (date, heure)
    - Criteo Cookie (ou ID publicitaire mobile dans l'environnement de l'application mobile, où les cookies ne sont pas pris en charge)
    - Adresse IP tronquée
    - ID CRM haché (facultatif au choix des clients publicitaires Criteo à des fins de reciblage inter-appareils)
    - Adresse e-mail hachée (facultatif au choix des clients publicitaires Criteo à des fins de reciblage inter-appareils)

9. Pour répondre à la demande d'accès soumise par Privacy International, Criteo a fourni des données relatives à 3 types d'événements, « imps », « événements pour publicitaires» et « clics ». Un exemple tiré d'une des demandes d'accès formulées par un membre du personnel de Privacy International est visible ci-dessous:

[114] https://www.criteo.com/fr/privacy/
[115] https://www.criteo.com/insights/gdpr-need-know-criteo/

| **Événements pour** publicitaires | |
|---|---|
| Description | |
| Identifiant du cookie | 24df9e49-8b61-4078-b9b7-d418c3cb4da8 |
| Informations sur le navigateur et l'appareil | Mozilla/5.0 (Macintosh ; Intel Mac OS X 10_13) AppleWebKit/604.1.38 (KHTML, tel que Gecko) Version/11.0 Safari/604.1.38 |
| Plateforme d'hébergement | UE |
| URL précédente | NULL |
| Horodatage | 1516052446 |
| ID des sites marchands | 1327 |
| URL parcourue | https://www.booking.com/ |
| Horodatage de l'utilisateur | NULL |
| Centres de données Criteo | NL_AM5 |
| Identifiant CRM du partenaire (NULL si non envoyé) | NULL |
| type de site Web (d = ordinateur de bureau ; m = mobile ; t = tablette) | d |
| ID du partenaire (NULL si non envoyé) | 24df9e49-8b61-4078-b9b7-d418c3cb4da8 |
| Horodatage de l'événement | 1516052446 |
| Produits consultés | [{internalid:18635,category:3,alternateid:20719,price:43.0,quantity:1,externalid:20719,priceineuro:48.32384},{internalid:18000,category:8,alternateid:20069,price:50.0,quantity:1,externalid:20069,priceineuro:56.19051},{internalid:548994,category:8,alternateid:906893,price:61.0,quantity:1,externalid:906893,priceineuro:68.55242}] |
| Type d'événement | Ressource |
| IP Criteo | 10.12.166.109 |
| | NULL |
| Nouveau client ou non (NULL = non) | NULL |
| Version de Criteo Tag utilisée par le site | 4.5.4 |
| Environnement (Web ou application) | web |
| Adresse e-mail hachée (NULL si non envoyé) | {email_id_is_valid:null,crm_id_is_valid:null} |
| Navigateur utilisé | safari |
| Version du navigateur | 11 |
| Appareil | Autre |
| Système d'exploitation | Mac OS X |
| Pays de l'utilisateur | GB |
| Environnement dans l'application FAUX = NON / VRAI = OUI | FAUX |
| Vue Web de l'application FAUX = NON / VRAI = OUI | FAUX |
| | Desktop |
| Type d'identifiant utilisé | idfs |
| Lien d'information | NULL |
| Date | 15/01/2018 |
| Heure | 21 |

| | |
|---|---|
| Type d'événement | Autre |
| Nom du partenaire Criteo | BOOKINGUK |

| Clics | |
|---|---|
| Horodatage | 1522829480 |
| Domaine parcouru | motherboard.vice.com |
| Identifiant du cookie | 24df9e49-8b61-4078-b9b7-d418c3cb4da8 |
| Jours depuis la dernière visite | -1 |
| IP Criteo | 10.12.160.86 |
| Centre de données Criteo<br>(FR_EQX = Paris ; NL_AM5 = Amsterdam) | NL_AM5 |
| Campagne Facebook<br>(O = non, 1 = oui) | 0 |
| Version principale du SE | 10 |
| Version du système d'exploitation | Mac OS X |
| Type d'appareil | Autre |
| Version du navigateur | 11 |
| Sous-version | 0 |
| Navigateur | safari |
| Environnement (Web ou application) | web |
| Identifiant de cookie de l'opportunité d'affichage | 24df9e49-8b61-4078-b9b7-d418c3cb4da8 |
| Destination du clic (application/web) | web |
| ID du marchand (= ID du partenaire) | 28388 |
| jour | 04/04/2018 |
| Heure | 8 |
| Nom du partenaire Criteo | MATCHESFASHIONUKIEGB |

| Imps | |
|---|---|
| Description | |
| Horodatage | 1521398294 |
| Nombre d'affichage | 1 |
| IP Criteo | 10.12.163.55 |
| Centre de données Criteo<br>(FR_EQX = Paris ; NL_AM5 = Amsterdam) | NL_AM5 |
| Identifiant du cookie | 24df9e49-8b61-4078-b9b7-d418c3cb4da8 |
| Domaine parcouru | www.dailymail.co.uk |
| ID de la campagne | 129697 |
| Identifiant de la bannière | 9220775 |
| ID du marchand | 1054 |
| ID du client Criteo | 457 |
| Identifiant du réseau utilisé pour afficher une annonce | 1867 |
| ID du partenaire | 121278 |
| Informations envoyées par la plateforme RTB | 1156173 |

| | |
|---|---|
| ID de la plateforme RTB | 73 |
| Url envoyée par les plateformes RTB | http://www.dailymail.co.uk/home/index.html |
| Informations envoyées par les plateformes RTB | FAUX |
| Informations envoyées par les plateformes RTB | 0 |
| Version du système d'exploitation | Mac OS X |
| Type d'appareil | Autre |
| Version du navigateur | 11 |
| Sous-version | 0 |
| Navigateur | safari |
| Environnement (Web ou application) | web |
| Pays de l'utilisateur | GB |
| Horodatage RTB | 10078 |
| Temps d'arbitrage | 3000 |
| Type d'appareil | Ordinateur de bureau |
| Adresse IP tronquée | 1406685440 |
| Type d'identifiant utilisé | idfs |
| Jour | 18/03/2018 |
| Heure | 18 |
| Plateforme d'hébergement | UE |
| Valeur aléatoire pour les tests A / B | 0 |
| Campagne Facebook<br>(O = non, 1 = oui) | 0 |
| Nom du marchand | HOF |

10. Criteo génère un identifiant Criteo afin de distinguer les navigateurs.

## D. Sources de données à caractère personnel

11. La politique de confidentialité de Criteo ne comporte pas de section spécifique relative aux sources. Toutefois, les types de données énumérés ci-dessus indiquent clairement que Criteo collecte des données auprès de ses partenaires publicitaires. L'identité de ces partenaires publicitaires n'est pas précisée.

12. Criteo peut également importer des données (identifiants techniques pour la synchronisation d'identifiants) auprès de « partenaires approuvés». Aucune information n'est fournie quant à l'identité de ces partenaires approuvés.

13. Grâce aux demandes d'accès du personnel de Privacy International, nous avons pu vérifier que Criteo possède des données de niveau individuel provenant d'un certain nombre d'autres sources, qu'elle connecte aux données client. Ces données proviennent d'une gamme de :

    - Sites Web et applications mobiles des publicitaires
    - Sites Web et applications mobiles des éditeurs

- Partenaires commerciaux tels que les plateformes RTB (Real Time Bidding) afin que Criteo achète des emplacements de publicité via les enchères de Criteo Dynamic Retargeting.

14. La liste des partenaires fournis par Criteo est la suivante :

- AdForm
- AdGeneration
- AdStir
- AdYouLike
- Ameba
- ANTS
- AOL
- Appnexus
- BidSwitch
- CheetahMobile
- D2C
- Facebook
- Fluct
- FreeWheel
- Fyber
- Geniee
- Google
- Improve Digital
- IMobile
- Index
- Inmobi
- Ividence
- kakao
- Ligatus
- Mail.ru
- LiveIntent
- MediaNet
- MicroAd
- Mobfox
- MoPub
- NasMedia
- Nativo
- Nend
- OATH
- OpenX
- Outbrain
- Plista
- ProfitX
- Pubmatic
- Quantum Advertising
- Rambler
- Rubicon Project
- Sharethrough
- Smaato
- Smart
- SmartClip
- Sovrn
- Stroer
- Taboola
- Teads
- Telaria
- TimesInternet
- Toast Exchange
- Triplelift
- Twiago
- UCFunnel
- Yahoo
- Yandex
- Yieldlab
- Yieldmo
- YieldOne

## E. Destinataires des données à caractère personnel

15. La politique de confidentialité de Criteo indique également que Criteo peut partager des données agrégées sur les performances de sa campagne :

« Nous pouvons être amenés à partager des données regroupées concernant la performance des campagnes de nos clients avec nos filiales ou nos sociétés affiliées et partager des données regroupées avec nos partenaires. Les données regroupées ne permettent pas d'identifier un partenaire ni de vous identifier directement. Nous ne partageons des données non regroupées qu'avec l'autorisation de nos partenaires et conformément à nos accords commerciaux. Les données non regroupées peuvent être conservées par des tiers comme les centres de données et les fournisseurs d'hébergement fournissant leurs services pour notre compte. Ces entreprises sont autorisées à utiliser les informations que nous fournissons uniquement lorsque cela est nécessaire pour nous fournir des services.

Nous travaillons en partenariat avec des plateformes d'Ad exchange pour acheter des emplacements publicitaires mis aux enchères pour Criteo Dynamic Retargeting. Avant une enchère, nous lions notre identifiant à la plateforme d'ad exchange et participons à l'enchère en envoyant le montant correspondant et le code bannière à afficher. »[116]

16. Lorsque Privacy International a demandé des informations supplémentaires sur les « partenaires éditeurs » et « partenaires publicitaires» mentionnés dans les données fournies en réponse aux demandes d'accès, Criteo a répondu :

« Criteo compte des milliers d'éditeurs partenaires et ne publie pas de liste de ces partenaires. / Criteo compte des milliers de clients publicitaires et ne publie pas de liste de ces clients. » et « Criteo compte des milliers de clients publicitaires et ne publie pas de liste de ces clients. »

## F. Preuve du profilage

17. Criteo ne mentionne pas spécifiquement le profilage dans sa politique de confidentialité. Cependant, la politique de confidentialité mentionne l'existence de 'segments' lorsqu'elle aborde des données que Criteo ne collecte pas :

« Nous ne créons pas de segments ciblant spécifiquement les mineurs de moins de 16 ans. »

18. Ceci suggère que Criteo segmente (c'est-à-dire crée des segments pour) d'autres groupes.

19. Lorsqu'elle a été interrogée sur le profilage par Privacy International, Criteo a répondu :

« Les produits Criteo sont basés sur des algorithmes conçus pour décider si une publicité de l'un des clients publicitaires de Criteo doit être affichée pour un ensemble particulier de données utilisateur / historique de navigation et, le cas échéant, comment cette publicité doit être personnalisée pour séduire cet utilisateur. Selon les directives du GT29, Criteo n'exerce pas d'activités de profilage au sens de l'article 22 du RGPD. "

## G. Base légale

[116] https://www.criteo.com/fr/privacy/

20. En réponse au questionnement par Privacy International quant à la base légale du traitement de l'historique de navigation des membres de son personnel, du reciblage et de l'affichage de publicités personnalisées, Criteo a répondu :

« Sur base des recommandations de la CNIL (l'autorité française de protection des données supervisant Criteo), Criteo s'appuie sur le **consentement** qu'elle a obligé ses partenaires publicitaires à obtenir [du membre du personnel PI], qui a également été informé de son droit de faire objection au traitement de ses données. Nous pensons également que Criteo a un **intérêt légitime** à traiter les données afin de respecter ses obligations contractuelles envers ses clients et ses partenaires. Nous obligeons les sites Web des publicitaires à fournir à leurs utilisateurs des informations complètes sur l'utilisation de la technologie Criteo et à recueillir leur consentement avant que tout cookie ne soit déposé, dans les pays où cela est obligatoire. » (Emphase ajoutée)

21. La politique de confidentialité de Criteo stipule que la base juridique de Criteo repose sur le consentement :

« La collecte de vos données à caractère personnel repose sur votre consentement : Criteo agit en qualité de responsable conjoint du traitement avec ses clients et partenaires qui, dès lors que la législation l'impose, vous ont informé et ont obtenu votre consentement pour le placement de cookies (ou d'autres technologies de suivi) à des fins de publicité ciblée, par exemple par le biais d'une bannière dédiée sur leur site Internet. Vous pouvez retirer tout consentement au traitement de vos données à caractère personnel à tout moment. »

## H. Données à caractère personnel sensibles / de catégorie spéciale

22. En ce qui concerne les données à caractère personnel sensibles ou de catégorie spéciale (conformément à l'article 9 du RGPD), la réponse de Criteo à Privacy International indiquait :

« Criteo peut confirmer qu'elle ne traite *pas* de données à caractère personnel sensibles. Dans la mesure où Criteo traite des données à caractère personnel non sensibles, il s'agit des identifiants en ligne pseudonymes mentionnés ci-dessus. Notez que Criteo a également des consignes en matière de publicité interdisant aux partenaires d'afficher le contenu, les produits ou les services énumérés ici. »

23. La politique de confidentialité de Criteo stipule :

> « Nous ne collectons pas d'informations sensibles (comme la religion, les opinions politiques, l'état de santé, l'orientation sexuelle etc.). »

24. Cependant, les URL fournies en réponse aux demandes d'accès de Privacy International ont révélé des détails très spécifiques sur la santé d'un membre du personnel.[117]

[117] Par exemple, https://www.babycenter.com/0_fatigue-during-pregnancy_2911.bc

## Annexe B - Quantcast

### A. L'activité de Quantcast

- Quantcast est une société de technologie publicitaire spécialisée dans la publicité en temps réel soutenue par l'Intelligence Artificielle, l'analyse d'audience et les mesures. Selon Quantcast, la société « exploite la plus grande plateforme d'information et de mesure d'audience ouverte du monde sur Internet »[118]. Par le biais de « Quantcast Intelligence Cloud (« QIC ») », elle offre une suite d'outils d'analyse, de ciblage et de mesure. Selon Quantcast, « QIC mesure les battements de cœur de vos clients tout au long de leur parcours numérique, changeant constamment en fonction de notre perception continue de l'Internet. **Nous connaissons les sites visités. Les mots-clés recherchés. Nous comprenons les habitudes d'achat.** Nous transformons ces données en informations exploitables. »[119] (Emphase ajoutée)

- Privacy International s'intéresse à un certain nombre de produits de Quantcast, notamment :

    - **Insights / Quantcast Measure:** Quantcast utilise le QIC pour comprendre le comportement d'un client potentiel et obtenir des informations à partir de sa navigation sur le Web. Quantcast permet également aux clients « d'obtenir le trafic et les données d'audience de milliers de sites Web et d'applications pour voir comment vous [le client de Quantcast] comparez ».[120] Quantcast décrit les informations comme permettant aux clients Quantcast « d'apprendre ce qui les motive [les consommateurs] au point d'influence - y compris les motivations psychographiques, et même les schémas comportementaux qui précèdent l'intention de recherche ».[121]
    - **Quantas Advertise (ciblage) :** Quantcast peut créer des modèles personnalisés en fonction de critères fournis par leurs clients (leur public idéal ou existant).[122] L'ensemble de données est basé sur « des millions de points de données disponibles » tels que « les comportements avant la recherche, les données démographiques et les achats antérieurs ».[123] Quantcast trouve ensuite les audiences et les clients qui correspondent au profil, permettant ainsi la diffusion d'un message ciblé à un public spécifique à grande échelle.[124]
    - **Quantcast Choice** : un outil de gestion du consentement permettant aux éditeurs et aux publicitaires d'obtenir, de gérer et de propager le consentement du consommateur dans l'ensemble de l'écosystème des contenus numériques et des publicités, sur la base du cadre de transparence et de consentement d'IAB Europe.[125]

---

[118] https://www.quantcast.com/en-uk/about-us/press/press-release/quantcast-launches-first-widely-available-implementation-of-iab-europes-gdpr-transparency-consent-framework/
[119] https://www.quantcast.com/quantcast-intelligence-cloud/
[120] https://www.quantcast.com/en-uk/products/measure-audience-insights/
[121] https://www.quantcast.com/products/insights/
[122] https://www.quantcast.com/en-uk/resources/build-trust-with-data-driven-insights/
[123] https://www.quantcast.com/en-uk/products/targeting-overview/
[124] https://www.quantcast.com/products/targeting-overview/
[125] https://www.quantcast.com/gdpr/consent-management-solution/

**B. Objectifs du traitement de données**

- En réponse aux demandes d'accès émanant du personnel de Privacy International, Quantcast a déclaré que les objectifs de son traitement des données à caractère personnel étaient les suivants :
    - « Permettre aux propriétaires de sites Web et aux applications de mieux comprendre leurs publics ; et
    - Prendre des décisions avisées en ce qui concerne le contenu à afficher et l'emplacement des publicités en ligne afin que nous puissions diffuser des publicités en ligne pertinentes pour les consommateurs individuels. »

- Des informations sur ces objectifs se retrouvent dans différentes sections de la politique de confidentialité de Quantcast, :

« *Ce que nous faisons* »

- « Nos outils de mesure aident les propriétaires de sites Web à comprendre les caractéristiques et la démographie des personnes qui visitent leurs sites »
- « Nos produits de publicité permettent aux entreprises de diffuser des publicités en ligne pertinentes aux consommateurs individuels. Pour les entreprises qui souhaitent faire de la publicité en ligne, nos produits de publicité aident à diffuser leurs publicités aux personnes les plus susceptibles de les trouver intéressantes. »

*« Associations multiplateformes »*

> « Nous fournissons un service de reporting multiplateforme aux partenaires qui exploitent des sites Web et des applications mobiles. Pour ce faire, nous nous appuyons sur les identifiants hachés (c'est-à-dire cryptés) dérivés des connexions de l'utilisateur pour joindre son utilisation des différentes plateformes (mobiles et de bureau). Cela permet à notre produit de mesure de fournir à un partenaire des rapports pertinents pour l'ensemble de ses plateformes. Nous utilisons également parfois des données de journalisation ('log data') ou d'autres données de nos partenaires pour supposer des liens entre [l'utilisation d'] appareils ou de plateformes. »

*Re Quantcast Choice*

> « Lorsque vous visitez un site ou une application utilisant Quantcast Choice, y compris le site Quantcast, nous utilisons des tags, des cookies, des kits de développement logiciels (SDK) et des plug-ins pour stocker des informations sur les avis de confidentialité que vous avez reçus et les choix de confidentialité que vous avez faits. Nous le faisons conformément aux directives et spécifications techniques du cadre de la transparence et du consentement d'IAB Europe. Nous n'utilisons aucune information recueillie

auprès de Quantcast Choice à d'autres fins. En d'autres termes, nous *n'utilisons pas* ces informations pour informer nos produits de mesure et de publicité, en dehors de la compréhension des avis de confidentialité que vous avez reçus et des choix que vous avez faits en matière de confidentialité. »

## C. Types de données à caractère personnel

5. La politique de confidentialité de Quantcast décrit les « informations collectées via nos services », qui donnent une idée du type de données que Quantcast traite :

« Lorsque vous visitez un site ou une application exploitée par un partenaire Quantcast, nous pouvons collecter des **données de journal (‘log data’) à partir de** ses sites et de ses applications via l'utilisation d'étiquettes et de cookies. Nous recevons également des **informations directement de nos partenaires**. Nous associons ces informations à un identifiant aléatoire unique associé à votre appareil (comme un identifiant de cookie), mais ne l'associons jamais à votre nom, votre adresse électronique, votre adresse ou votre numéro de téléphone, car nous ne recueillons pas ce type d'informations d'identification directe sur les consommateurs. L’utilisation de ces informations provenant de partenaires, qui incluent des **informations sur certains des sites que vous visitez et sur certaines des applications que vous utilisez**, est nécessaire pour protéger nos intérêts légitimes qui sont d'améliorer la précision de nos produits et de déterminer le type de publicité et de contenu qui pourrait vous intéresser. Par exemple, si vous recherchiez des billets d’avion pour San Francisco, nous pourrions prévoir que vous êtes intéressé par l’achat d’un joli chandail chaud et vous montrer ensuite une publicité de l’un de nos clients publicitaires vendant des chandails. (Pour être plus précis, nous prédirions que votre *appareil* pourrait appartenir à une personne intéressée par les chandails, car nous ne savons pas qui *vous êtes*.) » (Emphase ajoutée en gras)

2. La politique de confidentialité de Quantcast comprend une explication des données de journalisation (log data) :

« Les données de journal incluent (1) des informations qui nous sont envoyées par les navigateurs rencontrant nos étiquettes (**tags)**, qui comprennent, par exemple, le **type de navigateur, l'heure du navigateur, l'heure d'accès, la résolution de l'écran, l'adresse IP, l'URL du site de référence, l'URL du site actuel et les chaînes de recherche** ; (2) des informations qui nous sont envoyées par des plateformes d’**échanges publicitaires** sous forme de demandes d’enchères, qui peuvent inclure les informations ci-dessus ainsi que des informations telles que des **identifiants d’enchères**, dans le but de solliciter des offres pour placer des publicités en ligne ; et (3) des informations reçues du **Quantcast SDK** intégré dans les applications mobiles, qui peuvent inclure les éléments cités précédemment, ainsi que des informations telles que l'**identification de l'appareil, des informations de localisation, des données d'application et des informations d'utilisation, ainsi que des identificateurs uniques d'application et d'installation**. » (Emphase ajoutée)

3. Les réponses aux demandes d'accès du personnel de Privacy International ont fourni une grande quantité de données dans divers tableurs. Ceci est illustré dans le compte-rendu de l'un des membres de l'équipe.[126] Les données comprenaient :

    - **'Historique'** contient des enregistrements horodatés liés à l'activité en ligne d'un navigateur. Les données incluent : Ip ; ref ; cookieit ; time ; custom url ; encoded ip address ; encoded referring url (ref) ; cookie ; ua ; Key Value Character Large Object Store (kvClob) ; anonID ; gdprQCConsent ; gdprAnonVersion ; requestContent ; cookieIn ; type ; encodedID ; Ces données révèlent l'historique de navigation de la personne concernée sur des sites Web comportant l'etiquette ('tag') de Quantcast. Cela en soi peut permettre l'identification des personnes concernées, par exemple à travers l'URL de leur blog tumblr une fois qu'elles se sont connectées.
    - **Dérivé :** cette catégorie peut inclure des données dérivées fournies par des partenaires Quantcast et des segments de ciblage associés (tels que les segments dans lesquels vos cookies apparaissent).
    - **Déduction** : Quantcast analyse les données de l'historique pour en déduire à quel point votre comportement en ligne est similaire à celui d'un groupe de navigateurs exploités par des personnes ayant une caractéristique démographique particulière. Les données fournies incluent « plage de données », « i_unit », « a_unit » (titre d'une catégorie démographique, qui peut également contenir des informations relatives au modèle de pays utilisé pour déduire les valeurs démographiques) ainsi qu'une « une valeur » (probabilités normalisées dont la somme totalise 1).
    - **Les données de Partenaire** incluent un grand nombre de segments de données (y compris Oracle Data Cloud, Acxiom UK et Experian), un ID de segment, un nom de segment, un ID de cookie et une date de début/fin.

## D. Sources de données à caractère personnel

4. Interrogée sur ses sources de données par Privacy International, Quantcast a répondu qu'elle « identifiait clairement les sources de données à caractère personnel que nous recueillons dans notre politique de confidentialité auxquelles vous pouvez accéder à l'adresse https://www.quantcast.com/privacy. En particulier, veuillez vous reporter à la section intitulée " Informations collectées via nos services " ».

5. La section sur les « informations collectées via nos services » est citée ci-dessus dans la rubrique « Types de données à caractère personnel ». Elle comprend les données de journalisation (log data) obtenues via des étiquettes (tags) et des cookies, ainsi que des informations provenant directement des partenaires Quantcast. Certains des partenaires sont

[126] https://privacyinternational.org/feature/2429/quantcast

énumérés ci-dessous, notamment les plateformes de gestion de données et les fournisseurs de données tels que Acxiom et Oracle.

**E. Destinataires des données à caractère personnel**

6. La politique de confidentialité de Quantcast stipule :

   « Nous partageons avec des tiers certaines informations, y compris les données de journalisation (log data), dans le cadre de la provision et de l'amélioration de nos produits. Par exemple, nous divulguons certaines de ces données aux entreprises impliquées dans la diffusion de publicité ou dans leur visibilité. De même, nous divulguons certaines de ces données afin de fournir ou de faciliter la mesure d'audience du site, l'analyse du trafic ou l'analyse démographique, et pour permettre aux sites Web de fournir à leurs publicitaires des segments d'audience appropriés pour leurs produits ou services. Comme décrit dans la présente politique de confidentialité, puisque nous ne collectons pas intentionnellement d'informations directement identifiables sur les consommateurs (comme votre nom ou votre adresse électronique), nous ne partageons pas (et ne pourrions pas) partager ce type d'informations avec nos partenaires. Pour en savoir plus sur les informations que nous partageons avec nos partenaires, visitez notre [127] page Partenaires. »

7. Lorsqu'on lui a demandé plus d'informations sur les destinataires des données, Quantcast a répondu :

   « Nous avons déjà fourni le nom des destinataires des données à caractère personnel sur la page Partenaires à l'adresse https://www.quantcast.com/privacy/quantcast-partners, comme le suggère l'article 15, paragraphe 1, alinéa c) du RGPD. »

8. La page Partenaires Quantcast répertorie les responsables et les sous-traitants avec lesquels Quantcast collabore dans divers secteurs :

| | |
|---|---|
| **Vérification des publicités** | • DoubleVerify, responsable du traitement<br>• Integral Ad Science, responsable du traitement<br>• Moat, Inc., responsable du traitement |
| **Plateformes de gestion de données et fournisseurs de données** | • Acxiom Limited, responsable du traitement<br>• Adobe Systems Incorporated, responsable du traitement<br>• Krux Digital LLC, responsable du traitement<br>• LiveRamp, Inc., responsable du traitement |

[127] https://www.quantcast.com/privacy/quantcast-partners/

| | |
|---|---|
| | • Oracle America, Inc., responsable du traitement<br>• Research Now Group, Inc., responsable du traitement |
| **Infrastructure** | • Amazon Web Services, responsable du traitement |
| **Marketing et recherche client** | • AutopilotHQ, Inc., responsable du traitement<br>• FullStory, Inc., responsable du traitement<br>• Google Inc. (Google Analytics), responsable du traitement<br>• Marketo, Inc., responsable du traitement<br>• MixPanel, Inc., responsable du traitement<br>• OneClipboard Inc. (dba Splashthat), responsable du traitement<br>• Optimizely, Inc., responsable du traitement<br>• Qualtrics, LLC, responsable du traitement<br>• Segment.io, Inc., responsable du traitement |
| **Plateformes d'échange pour les enchères en temps réel (RTB)** | • AppNexus, Inc., responsable du traitement<br>• Bidswitch GmbH, responsable du traitement<br>• DoubleClick Ad Exchange, une division de Google Inc., responsable du traitement<br>• Index Exchange Inc., responsable du traitement<br>• Lijit Networks, Inc. (Sovrn), responsable du traitement<br>• Oath Americas, Inc., responsable du traitement<br>• OpenX Technologies, Inc., responsable du traitement<br>• PubMatic, Inc., responsable du traitement<br>• PulsePoint, Inc., responsable du traitement<br>• Smart Ad Server, responsable du traitement<br>• SpotX, Inc., responsable du traitement<br>• Switch Concepts Ltd, responsable du traitement |

| | |
|---|---|
| | • Le Rubicon Project, Inc., responsable du traitement |

9. Les réponses aux demandes d'accès émanant des membres du personnel de Privacy International comprenaient également des données de partenaires, qui comprenaient des segments de données d'Oracle Data Cloud et Acxiom UK et TwentyCi, ainsi que d'autres sociétés de données telles qu'Experian, Mastercard et Affinity Answers. Figuraient dans ces réponses une gamme de catégorisation à propos des intérêts de la personne en matière de consommation, de médias, de profession, ainsi que des catégorisations de modes de vie, notamment tirées de PersonicX d'Acxiom et de Mosaic d'Experian.

**F. Preuve du profilage**

10. La politique de confidentialité de Quantcast définit les services que Quantcast fournit de manière générale. Le profilage, c'est-à-dire la déduction et la dérivation de données sur des personnes, apparait comme essentiel :

    « [Services Quantcast] Ce terme désigne globalement l'ensemble des services que nous fournissons au travers de nos produits, y compris la collecte d'informations sur le consommateur, l'analyse de ces informations, la fourniture de ces informations et des **informations dérivées** de ces informations à nos partenaires Quantcast, ainsi que la sélection et le placement de publicités et de contenus optimaux sur la base de ces informations. » (Emphase ajoutée)

11. En réponse aux demandes d'accès des membres du personnel de Privacy International, Quantcast a répondu :

    « Pour certains navigateurs, nos systèmes analysent certaines des données figurant dans l'historique **pour en déduire à quel point votre comportement en ligne est similaire à celui d'un groupe de navigateurs exploité par des personnes ayant une caractéristique démographique particulière**. Cette similarité est représentée avec une valeur de probabilité normalisée. Dans l'UE, les navigateurs des personnes concernées peuvent être évalués selon plusieurs catégories démographiques (voir ci-dessous). Pour chaque catégorie démographique, la somme des valeurs de probabilité normalisées correspondant aux caractéristiques démographiques de cette catégorie totalisera « 1 ». Cependant, tous les navigateurs ne sont pas évalués, de sorte que tous les navigateurs n'auront pas de valeurs de probabilité normalisées. Nous mettons à jour fréquemment les analyses démographiques. »

12. Quantcast a répertorié les catégories démographiques suivantes en réponse aux demandes :

| a_unit | Définition | Caractéristique démographique |
|---|---|---|

| | | |
|---|---|---|
| GenderVisits | Sexe | "Homme", "Femme" |
| InetHHAgeAndGenderVisits | ÂGE + SEXE | "Homme 18-24", "Homme 25-34", "Homme 35-44", "Homme 45-54", "Homme 55-64", "Homme de 65 ans et plus", "Femme 18-24", "Femme 25-34 "," Femme 35-44 "," Femme 45-54 "," Femme 55-64 "," Femme 65+ ", |
| InetHHAgeVisits | ÂGE | "18-24", "25-34", "35-44", "45-54", "55-64", "65+", |
| InetHHChildrenV2Visits | Présence d'enfants dans le ménage (nombre d'enfants et leur âge) “ | "Pas d'enfants", "Enfants de moins de 3 ans", "Enfants de 3 à 12 ans", "Enfants de 13 à 17 ans", "Enfants de moins de 3 ans et de 3 à 12 ans", "Enfants de 3 à 12 ans et de 13 à 17 ans", |
| InetHHEducationVisits | ÉDUCATION | "Pas universitaire", "Universitaire", "Grad. Sch." |
| InetHHIncomeVisits | Revenu annuel brut du ménage en dollars américains | "$0-50k", "$50-100k", "$100-150k", "$150k+" |
| InetHHIncomeVisitsGBP | Revenu annuel brut des ménages dans la monnaie de la Grande-Bretagne | "£0-30k", "£30-50k", "£50-70k", "£70k+" |

### F. Base légale

13. La politique de confidentialité de Quantcast définit ce qui suit :

« Afin de fournir nos services, nous utilisons les informations décrites dans cette politique de confidentialité comme étant nécessaires à nos **intérêts légitimes**. Ces intérêts légitimes incluent nos intérêts à fournir, améliorer et personnaliser les services offerts à nos partenaires et à vous fournir des publicités et des contenus pertinents, à moins que ces intérêts ne nuisent à vos intérêts ou droits et libertés fondamentaux nécessitant la protection de vos informations personnelles. Nous pouvons partager vos informations (telles que décrites dans la présente politique de confidentialité) si nécessaire pour défendre nos intérêts légitimes et ceux de nos partenaires en diffusant une publicité plus utile et plus pertinente. Vous avez le droit de vous opposer à ce traitement lorsque nous nous appuyons sur des intérêts légitimes, comme décrit dans la section Opposition et désinscription ci-dessous… En outre, si vous nous avez donné votre **consentement** pour utiliser vos informations de certaines manières, nous nous baserons sur votre consentement pour traiter les informations. Vous pouvez révoquer ce consentement à tout moment. Veuillez consulter la section Opposition et désinscription ci-dessous pour savoir comment retirer votre consentement. » (Emphase ajoutée)

### H. Données à caractère personnel sensibles / de catégorie spéciale

14. En réponse aux demandes d'accès émanant des membres de l'équipe PI, Quantcast a répondu comme suit :

    **«** Dans l'UE, les catégories de données à caractère personnel que nous collectons auprès des internautes ne comprennent pas les données à caractère personnel de catégorie spéciale telles que les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, etc., et le traitement de données génétiques, données biométriques visant à identifier de manière unique une personne physique, les données relatives à la santé ou les données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique. Nous ne traitons pas non plus de données à caractère personnel liées à des condamnations pénales ou à des infractions. Nous ne recueillons pas votre nom, adresse ou date de naissance. Les données que nous collectons sont pseudonymisées. Nous ne savons pas qui vous êtes et nos partenaires, tels que les éditeurs de sites Web et les agences de publicité, sont obligés de s'abstenir de nous envoyer des données à caractère personnel appartenant aux catégories décrites dans ce paragraphe."

15. La politique de confidentialité de Quantcast stipule **:**

    **« Quantcast ne collecte ni n'utilise en connaissance de cause aucune information sensible sur la santé, telle que, par exemple, des informations relatives à des affections ou des prescriptions passées ou présentes. Dans l'Espace Economique Européen, Quantcast ne collecte ni n'utilise en connaissance de cause aucune information personnelle révélant une origine raciale ou ethnique, des opinions politiques, des convictions religieuses ou philosophiques, ni l'appartenance à un syndicat, des données génétiques ou biométriques visant à identifier de manière unique une personne concernée, ou des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne concernée. »**

16. Les données fournies par Quantcast, y compris l'historique de navigation et les segments de données de partenaires, incluent des données à partir desquelles des données à caractère personnel sensibles ou des données de catégories spéciales pourraient être révélées, par exemple :

- DATA_SEGMENT:Acxiom UK:Shopping Interests:Fast Moving Consumer Goods:Buyers:Alcohol at Home Heavy Spenders
- DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Going to the Pub

## Annexe C - Tapad

### A. L'activité de Tapad

1. Tapad est spécialisée dans la publicité inter-appareils. Tapad se décrit comme « Réinventant la personnalisation pour le spécialiste du marketing moderne ».[128] Tapad est fondé sur son « **graphe d'identité numérique** » utilisé pour « analyser des milliards de signaux » et « créer des relations entre les marques et leurs clients **uniques** ».[129] Tapad « utilise les données du consommateur pour produire une communication inter-appareils personnalisée . Les scientifiques et les ingénieurs de [Tapad] utilisent les données [de Tapad] pour extraire des informations et créer **un portrait complet des consommateurs** derrière leurs appareils. »[130] (Emphase ajoutée)

2. Privacy International est préoccupé par les produits Tapad, notamment :

   - **Le Tapad Graph :** « […] permet aux spécialistes du marketing de capturer une multitude de points de contact avec le consommateur à travers les appareils et canaux, en les associant à un individu unique. Cela fournit une vue claire du chemin que parcourt le consommateur vers la conversion et aide les spécialistes du marketing à identifier les initiatives qui ont un impact… Le graphe Tapad contient des données sur **des milliards d'appareils numériques** utilisés dans le monde entier. Nous connectons les appareils aux consommateurs et aux ménages afin que les données puissent être exploitées pour tous les cas d'utilisation des services marketing. » [131] (Emphase ajoutée)
   - **Device Graph Access (DGA) :** cet outil permet aux clients de Tapad d'accéder à ces données inter-appareils. « DGA identifie les relations entre les appareils des consommateurs de vos plateformes et recherche les nouveaux appareils qui appartiennent à vos clients. » [132]
   - **Tapad Customer Data Platform** « permet aux opérateurs de réseaux de télécommunication et de téléphonie mobile d'améliorer l'expérience et l'acquisition de clients en regroupant diverses données internes et de l'éditeur avec le Tapad Graph ». [133]

### B. Objectifs du traitement de données

3. La politique de confidentialité de Tapad définit les objectifs pour lesquels Tapad traite les données à caractère personnel collectées :

   - « Évaluer la probabilité et la nature des connexions entre les appareils (un attribut clé de notre Graph).
   - Déduire l'éligibilité de l'appareil pour les **segments d'intérêts et** démographiques.

[128] https://www.tapad.com
[129] https://www.tapad.com/the-tapad-graph
[130] https://www.tapad.com/the-tapad-graph
[131] https://www.tapad.com/the-tapad-graph
[132] https://www.tapad.com/device-graph-access
[133] https://www.tapad.com/customer-data-platform

- Fournir aux utilisateurs une publicité ciblée en fonction des informations collectées par Tapad, sauf si l'utilisateur a choisi de ne pas y participer.
- Fournir des informations, faciliter la diffusion des publicités et fournir des rapports aux clients (tels que les publicitaires et les éditeurs) et aux partenaires, y compris les rapports statistiques relatifs à l'activité sur un site Web, l'optimisation de l'emplacement des publicités, les performances des publicités, les mesures de portée et de fréquence, la facturation, et l'enregistrement des publicités diffusées un jour donné sur un site Web particulier.
- Fournir aux clients et aux partenaires des informations venant du Device Graph et des **déductions concernant les intérêts des utilisateurs**, leur permettant de cibler leurs publicités, de personnaliser leur contenu, d'analyser les comportements et de se livrer à d'autres services similaires.
- Partager des informations agrégées avec des tiers.
- Fournir des services de reporting et d'analyse sur de l'impact inter-écran des campagnes multimédias numériques.
- Données sources pour la modélisation d'audiences similaires »[134] (Emphase ajoutée).

4. La politique de confidentialité de Tapad continue avec :

   « Création de profils à travers la construction d'audiences de manière automatique mais sans effet juridique sur l'utilisateur.

   En outre, Tapad peut utiliser ces informations pour effectuer des analyses internes afin de réaliser et d'optimiser les services et les technologies associées, ainsi que pour faire fonctionner et améliorer le site Tapad (www.tapad.com).

   Tapad reçoit également des « identifiants de correspondance » ("Matching IDs") de ses partenaires et clients dans le but d'aider nos partenaires et clients à comprendre lesquels de leurs clients existants ou des identifiants qui leur sont connus correspondent à des identifiants spécifiques dans le Device Graph de Tapad. Les identifiants de correspondance peuvent représenter des identifiants de cookie, des identifiants de client, des identifiants statistiques, des adresses électroniques, des numéros de téléphone (au Pakistan, en Thaïlande, au Bangladesh et en Malaisie uniquement), ou d'autres types de données envoyées au partenaire ou au client. Cependant, Tapad ne reçoit jamais ces informations sous une forme identifiable. Tapad exige que les partenaires et les clients masquent et protègent tous les identifiants de correspondance avant de les envoyer à Tapad, de sorte que les données sous-jacentes n'ont aucune signification pour Tapad, comme par exemple dans le cas d'un identifiant de cookie tiers : si Tapad ne possède pas de tableau, Tapad n'a pas la capacité d'accéder aux données sous-jacentes. Les identifiants de correspondance peuvent être utilisés à des fins

[134] https://www.tapad.com/privacy-policy

d'analyse, de ciblage publicitaire, de gestion de Device Graph ou pour enrichir les données ou les services de Tapad. »[135]

### C. Types de données à caractère personnel

17. Aux questions de de Privacy International, Tapad a répondu :

    « Tapad collecte des données à caractère personnel sous la forme d'identifiants d'appareils pseudonymisés et d'autres identifiants indirects. Celles-ci se limitent aux cookies et aux identifiants de publicités pour mobile, par exemple IDFA pour iOS et identifiant publicitaire (‘Ad ID’) pour Android…, identifiants indirects d’adresse IP et autres informations considérées comme des points de données Internet standard tels que l’horodatage (« *timestamp* ») et la chaîne User-Agent (« *user agent string* » ), ce qui inclue des informations à propos du navigateur et du système d’exploitation à partir desquelles Tapad peut déduire le type, la marque ou le modèle de l'appareil. Tapad reçoit ces informations sur l'événement par le biais d'une page Web ou d'une application, sur laquelle une publicité peut être placée, un pixel Tapad déclenché, ou directement de nos partenaires [Tapad]. »

18. Les données fournies en réponse aux demandes d'accès par le personnel de Privacy International comprenaient : tapad_device_id ; horodatage ; url_or_app, user_agent, ainsi que ip_address.

19. La politique de confidentialité de Tapad fournit des informations supplémentaires à propos des données pouvant être collectées par Tapad pour la gestion du Device Graph, les statistiques ainsi que le ciblage des publicités :

    - « Horodatage
    - Chaîne User-Agent (« *user agent string* ») spécifiant les informations du navigateur et du système d'exploitation
    - Adresse IP
    - Identifiant unique d'appareil pseudonymisé, stocké dans un cookie du navigateur, pouvant être facilement réinitialisé ou désactivé (‘opt out’) à la demande de l'utilisateur
    - Autres identifiants d'appareil pseudonymisés, tels que IDFA pour iOS et Android Ad ID pour Android, qui peuvent facilement être réinitialisés à la demande de l'utilisateur.
    - URL ou identifiants d'applications (« *app ID* ») d'une page Web ou d'une application sur laquelle une publicité peut être placée ou sur lesquels un pixel Tapad est déclenché. Dans l'UE, l'URL de la page Web est entièrement supprimée et non stockée par Tapad.
    - Données anonymes pouvant être extrapolées à partir d'une adresse IP. Par exemple, nous pouvons être en mesure de déterminer l'emplacement général d'un utilisateur et donc de déduire des informations démographiques.

[135] https://www.tapad.com/privacy-policy

- Identificateur d'utilisateur brouillées, tel que l'adresse électronique (ou le numéro de téléphone uniquement au Pakistan, en Thaïlande, au Bangladesh et en Malaisie).
- Identifiants statistiques uniques calculés par nos partenaires à partir d'informations relatives à un appareil mobile, à un navigateur ou à un système d'exploitation dont ils collectent les données à l'aide de technologies autres que les cookies. Par exemple, une tablette et un ordinateur portable présentant des caractéristiques similaires, telles que l'adresse IP, l'agent utilisateur, les paramètres de police, la résolution d'écran et les plug-ins, peuvent être considérés comme appartenant à la même personne. Plusieurs utilisateurs peuvent partager un identifiant statistique ou un utilisateur peut avoir plusieurs identifiants statistiques dans un Device Graph. »

### D. Sources de données à caractère personnel

20. Les ressources du Tapad Graph fournissent des informations supplémentaires sur les sources d'identité du consommateur pour le Tapad Graph.[136] La quantité de sources de données est vaste : **«** Tapad ingère plus d'1 million de signaux par minute provenant de plus de 130 partenaires d'intégration, avec des intégrations manuelles supplémentaires disponibles en fonction des besoins du client ». Le Tapad Graph contient des données provenant de « 4,2 milliards d'appareils dans le monde ». En ce qui concerne la diversité :


(réf. Tapad https://go.tapad.com/hubfs/Data%20Sourcing_1-Sheet.pdf )

21. Le Tapad Graph n'est pas la seule source de données et, selon sa politique de confidentialité, Tapad :

«.. complète nos données de segments d'utilisateurs et de Device Graph **avec des informations d'autres partenaires de données**. Les informations fournies par ces partenaires de données sont généralement constituées de données démographiques et de données d'intérêts déduites. Tapad ne

[136] Sources d'identité du consommateur Tapad https://go.tapad.com/hubfs/Data%20Sourcing_1-Sheet.pdf

collecte ni n'utilise aucune donnée, y compris des données sur les intérêts déduits, que nous considérons comme sensible, telle qu'une information précise reflétant l'état de santé ou un traitement médical passé, présent ou futur de l'utilisateur, y compris ses antécédents génétiques, génomiques et médicaux familiaux ; certains aspects de la vie personnelle ou de la situation financière d'un utilisateur ; ou l'utilisation de, ou l'intérêt pour, les jeux d'argent, les boissons alcoolisées, ou les produits ou services « réservés aux adultes ». Tapad collabore avec **Blue Kai**, **eXelate et d'autres sociétés pour recevoir des informations sur les catégories de santé et de bien-être non sensibles**. Vous pouvez consulter **les listes représentatives** de ces catégories disponibles chez Blue Kai en cliquant ici[137] et depuis eXelate en cliquant ici[138]." »

22. La liste BlueKai comprend, par exemple, « antidouleur », « soins des pieds », « protection sanitaire », diverses catégories de « gestion du poids », « couches », « soulagement des allergies », « médecine », « croyants aux antalgiques génériques », « médicaments de marque », « nutrition et contrôle du poids pour hommes », « nutrition et contrôle du poids des femmes », diverses catégories de professions de la santé, antalgiques pour enfants », « **rééducation** » et « aide au sommeil ».[139] (Emphase ajoutée)

23. La liste Exelate [140] comprend les catégories suivantes :

- « À propos de moi » : revenu du ménage ; sexe (femme/homme) ; âge (tranches de 10 ans) ; style de vie (propriétaires/locataires) ; lieu (rural, suburbain, etc.) ; famille (avec ou sans enfants).
- « Mes intérêts actuels » divisé en catégories puis en sous-catégories :
  - « Achats » ;
  - « Voyages » ;
  - « Services » comprend « Finances et assurances - **Dettes** » et « Finances et assurances - **Prêts** », ainsi que « Médecine et santé » et « **Organisations religieuses** » ; « Santé » ;
  - « Carrières » ; et
  - « Divers » comprend « **Communauté asiatique** » ; « Jeux occasionnels » ; « **Hispanophones** » ; et « Célibataires » (Emphase ajoutée)

### E. Destinataires des données à caractère personnel

24. La politique de confidentialité de Tapad stipule ce qui suit en ce qui concerne les parties avec lesquelles les données sont partagées :

« Nous partageons les données que nous conservons dans notre Device Graph avec nos clients et nos plateformes partenaires. De plus, nous transférons des données à notre prestataire de services , qui agissent [sic]

[137] http://www.bluekai.com/health-related-categories.pdf
[138] http://exelate.com/privacy/opt-in-opt-out/
[139] http://www.bluekai.com/health-related-categories.pdf
[140] http://exelate.com/privacy/opt-in-opt-out/

comme notre responsable du traitement. Nos clients, plateformes partenaires et prestataire de services sont situés aux États-Unis, au Canada, au Japon, en Malaisie, à Singapour, au Pakistan, au Bangladesh, en Turquie (bientôt), dans l'UE et dans l'EEE (Suède, Norvège, Allemagne, Royaume-Uni, Irlande, Belgique et Pays-Bas). »

25. Aucune information supplémentaire n'est fournie sur l'identité des clients et des partenaires. À la demande de Privacy International, Tapad a répondu :

« … Nous partageons des données pseudonymes avec nos clients et nos plateformes partenaires, qui se composent de **spécialistes du marketing** et de **fournisseurs adtech**. Veuillez bien comprendre qu'en raison d'obligations de confidentialité, nous ne pouvons pas vous fournir les noms de nos clients et partenaires. Toutefois, comme vous le savez, l'article 15, paragraphe 1, alinéa c) du RGPD nous autorise par contre à divulguer des catégories de destinataires. De plus, nous transférons des données à nos prestataire de services cloud, qui agissent en tant que processeurs de données pour notre compte [Tapad] » (Emphase ajoutée)

### F. Preuve du profilage

26. Comme indiqué ci-dessus et dans la politique de confidentialité de Tapad, le profilage est au cœur des objectifs de Tapad :

- Déduire l'éligibilité de l'appareil pour les **segments d'intérêts et** démographiques
- Fournir des nouvelles informations
- Fournir aux clients et aux partenaires des informations et des **déductions réalisées sur Device Graph concernant les intérêts des utilisateurs**, leur permettant de cibler leurs publicités, de personnaliser leur contenu, d'analyser les comportements et de se livrer à d'autres services similaires
- Données sources pour la modélisation d'audiences similaires

27. Comme Tapad l'indique explicitement dans sa politique de confidentialité, les données sont utilisées pour la « Création de profils via la création d'audiences de manière automatique, mais sans effet juridique pour l'utilisateur ».

28. La nature des profils / segments créés par Tapad n'est pas claire.

29. Tapad traite également les profils/segments d'autres partenaires, comme indiqué dans les exemples de BlueKai et d'Exelate ci-dessus.

### G. Base légale

30. La politique de confidentialité de Tapad fournit des informations en tant que base légale du traitement de Tapad, reposant sur le consentement et les intérêts légitimes.

« Pour traiter légalement des données à caractère personnel, Tapad doit suivre deux exigences distinctes découlant de deux actes juridiques différents dans la législation européenne :

a) Pour stocker et accéder aux informations stockées sur l'appareil d'un utilisateur (les cookies), vous devez obtenir **son consentement**. Pour ce « consentement aux cookies », Tapad s'appuie sur les fournisseurs de sites Web (éditeurs) et les oblige contractuellement à ne transmettre que les données obtenues légalement. Tapad remplit ainsi son obligation découlant de la directive « vie privée et communications électroniques ».

b) Pour le traitement ultérieur et la création du Device Graph basé sur diverses données (y compris les données de cookie ci-dessus), Tapad utilise l'**intérêt légitime** comme base légale pour le traitement. Par ce biais, Tapad remplit son obligation aux fins du RGPD, car le traitement dépasse le placement initial du cookie. L'intérêt légitime du traitement de Tapad est la personnalisation des communications promotionnelles destinées aux internautes, qui fait partie intégrante de l'écosystème en vertu duquel le contenu Internet librement disponible est financé par les recettes publicitaires. »

31. En ce qui **concerne le consentement**, Tapad a également informé Privacy International qu'il faisait partie du cadre de consentement d'IAB de l'UE.[141]

32. En ce qui concerne l'**intérêt légitime**, Tapad a fourni à Privacy International les explications supplémentaires suivantes :

> « De plus, Tapad demande à tous ses partenaires de ne transmettre que les données obtenues légalement. Cela sert, entre autres, l'intérêt légitime de Tapad d'utiliser et d'implémenter les données dans son Device Graph, ce qui sert alors encore l'intérêt légitime des spécialistes du marketing pour commercialiser leurs produits.
>
> Tapad permet de mesurer le marketing et la publicité sur plusieurs services. Pour ce faire, Tapad a développé un algorithme probabiliste permettant de connecter les appareils des utilisateurs finaux en fonction de leurs identifiants en ligne récurrents pseudonymisés. Il est important de souligner que Tapad n'utilise qu'un nombre très limité de ces identifiants en ligne et ne collecte, n'accepte ni n'utilise aucun identifiant direct qui permettrait d'identifier directement toute personne concernée. Toutes les données utilisées par Tapad sont donc des données pseudonymes. Ce concept est au cœur du produit Tapad et doit toujours être pris en compte lors de l'évaluation des activités de traitement de Tapad.
> Selon le considérant 47 du RGPD, le marketing direct peut déjà être considéré comme réalisé pour un intérêt légitime par la société de publicité. Cela doit donc s'appliquer à fortiori au suivi pseudonyme sur

[141] https://advertisingconsent.eu et consentement à la publicité Tapad IAB

Internet, où, contrairement au marketing mené par le marketeur, l'identité réelle de la personne concernée est inconnue.

Grâce à sa technologie brevetée, Tapad permet la connexion d'identifiants pseudonymisés qui permettent de mieux diffuser et mesurer les publicités personnalisées sur Internet et servent ainsi les intérêts légitimes des publicitaires. En outre, la publication de publicités sur Internet fait partie intégrante de la préservation de la validité du consentement Internet, ce qui est dans l'intérêt de tout utilisateur d'internet.

Tapad a réalisé une analyse d'impact complète sur la protection des données et un test d'équilibrage approfondi. Des facteurs tels que la transparence, une variété d'options de retrait d'accès appropriées et faciles, ainsi que le traitement strict de données uniquement pseudonymes nous amènent à conclure que les intérêts des publicitaires ne sont pas outrepassés par les droits et intérêts des personnes concernées. »

33. Tapad se sert également de **l'option de « désinscription** », où « [c]omme les applications mobiles et les navigateurs Web ont des identifiants différents, vous devrez vous désinscrire séparément de chaque environnement. À ce stade, nous [Tapad] ne répondons pas aux signaux du navigateur « ne pas suivre » ('Do Not Track')... La désactivation du navigateur Web Tapad consiste à remplacer votre identifiant de cookie unique par une valeur de désactivation générique… Ainsi, si vous essayez de vous désabonner en effaçant les cookies ou en supprimant le cache de contenu de votre appareil, Tapad ne pourra pas reconnaître votre appareil comme étant désinscrit, et si vous visitez ensuite l'un de ses partenaires du site Web de Tapad, vous risquez d'obtenir un nouveau cookie Tapad. » En outre, « L'option de désinscription ci-dessus ne sera activée que si vous y accédez à partir d'un navigateur compatible Javascript et si les cookies tiers sont activés. Ces deux technologies sont nécessaires pour que nous puissions fournir une option de désinscription persistante. D'autres technologies, telles que le stockage local HTML5, peuvent également être utilisées afin de rendre la désinscription aussi persistant que possible. »

34. À ce propos, Tapad a également indiqué dans sa politique de confidentialité que : « Nous demandons à tous nos partenaires fournisseurs de mettre à jour leurs politiques de confidentialité destinées au consommateur afin de s'assurer qu'il est notifié de la collecte de données entre appareils. Cela inclut le traitement complet des désabonnements destinés aux consommateurs de manière rapide et complète lorsque nous communiquons avec un consommateur par le biais de médias rémunérés, de publicité ou de toute activité sur site. »

### H. Données à caractère personnel sensibles

35. La politique de confidentialité de Tapad stipule que Tapad ne collecte pas de :

« Données à caractère personnel sensibles, telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, la santé et des informations sur la vie sexuelle. »

36. La politique indique également que :

    « Tapad ne collecte ni n'utilise aucune donnée, y compris des données sur les intérêts déduits, que nous considérons comme sensible, telle qu'une information précise reflétant l'état de santé ou un traitement médical passé, présent ou futur de l'utilisateur, y compris ses antécédents génétiques, génomiques et médicaux familiaux ; certains aspects de la vie personnelle ou de la situation financière d'un utilisateur ; ou l'utilisation de, ou l'intérêt pour, les jeux d'argent, les boissons alcoolisées, ou les produits ou services " réservés aux adultes " ».

37. La liste des partenaires Tapad est non exhaustive et les deux exemples cités, Blue Kai et eXelate, incluent diverses catégories liées à la santé, notamment la Rééducation (figurant dans la liste Blue Kai) et les catégories de la liste eXelate incluent les intérêts dans les services financiers pour les dettes et les prêts, les organisations religieuses, ainsi que des catégories diverses incluant la communauté asiatique et les hispanophones.