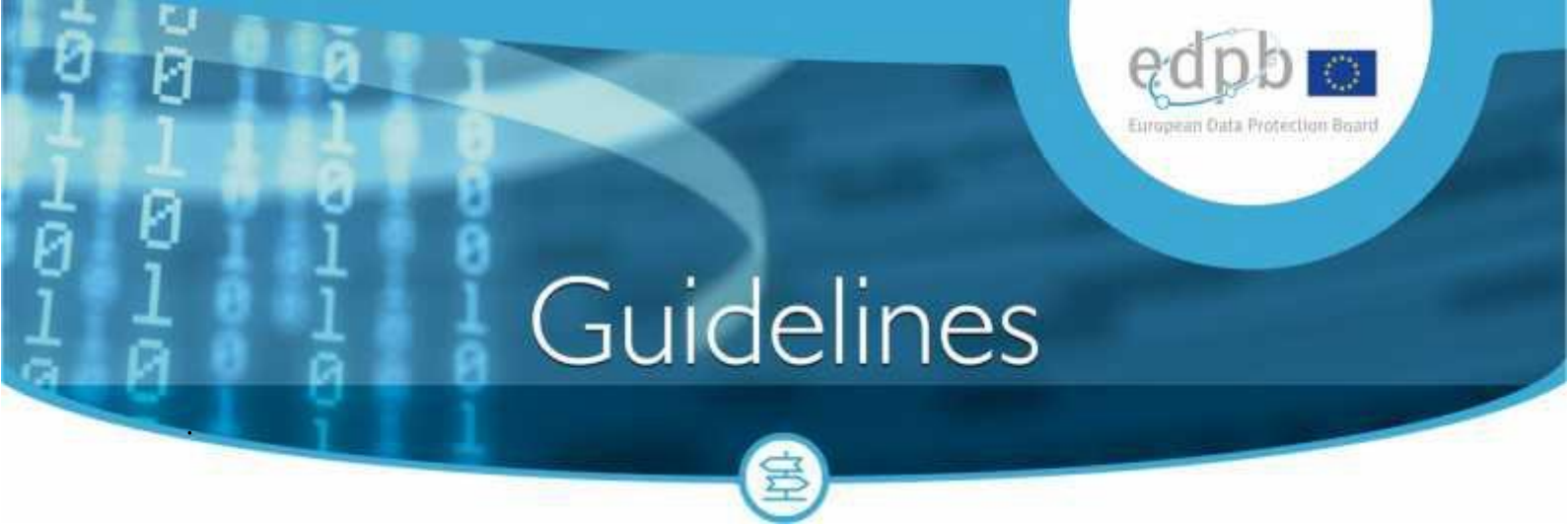

Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux

Version 2.0

Adopté le 13 avril 2021

Historique des versions

Version 2.0	13 avril 2021	Adoption des lignes directrices après consultation
Version 1.0	2 septembre 2020	Adoption des lignes directrices pour la consultation de

TABLE DES MATIÈRES

Le Conseil européen de la protection des données

Vu l'article 70, paragraphe 1, point e), du règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

1 INTRODUCTION

1. L'essor des médias sociaux a constitué une évolution importante de l'environnement en ligne au cours de la dernière décennie. De plus en plus d'individus utilisent les médias sociaux pour rester en contact avec leur famille et leurs amis, pour s'engager dans un réseau professionnel ou pour se connecter autour d'intérêts et d'idées partagés. Aux fins des présentes lignes directrices, les médias sociaux sont considérés comme des plates-formes en ligne qui permettent le développement de réseaux et de communautés d'utilisateurs, parmi lesquels des informations et des contenus sont partagés1. [1] Les principales caractéristiques des médias sociaux sont la possibilité pour les individus de s'inscrire afin de se créer des "comptes" ou des "profils", d'interagir les uns avec les autres en partageant des contenus générés par les utilisateurs ou d'autres contenus et de développer des connexions et des réseaux avec d'autres utilisateurs. [2]

2. Dans le cadre de leur modèle économique, de nombreux fournisseurs de médias sociaux proposent des services de ciblage. Les services de ciblage permettent aux personnes physiques ou morales (les "cibleurs") de communiquer des messages spécifiques aux utilisateurs des médias sociaux afin de promouvoir des intérêts commerciaux, politiques ou autres3. Une caractéristique distinctive du ciblage est l'adéquation perçue entre la personne ou le groupe ciblé et le message délivré. L'hypothèse sous-jacente est que plus l'adéquation est bonne, plus le taux de réception (conversion) est élevé et donc plus la campagne de ciblage est efficace (retour sur investissement).

3. Les mécanismes permettant de cibler les utilisateurs de médias sociaux se sont sophistiqués au fil du temps. Les organisations ont désormais la possibilité de cibler des individus sur la base d'un large éventail de critères. Ces critères peuvent avoir été élaborés sur la base de données personnelles que les utilisateurs ont activement fournies ou partagées, comme leur statut relationnel. De plus en plus, cependant, les critères de ciblage sont également élaborés sur la base de données personnelles qui ont été observées ou déduites, soit par le fournisseur de médias sociaux, soit par des tiers, et collectées (agrégées) par la plateforme ou par d'autres acteurs (par exemple, des courtiers en données) afin de soutenir les activités des organisations.

[1] Les fonctions supplémentaires fournies par les médias sociaux peuvent inclure, par exemple, la personnalisation, l'intégration d'applications, les plug-ins sociaux, l'authentification des utilisateurs, l'analyse et la publication. Les fonctions des médias sociaux peuvent constituer une offre autonome des contrôleurs ou être intégrées dans une offre de services plus large.

[2] Outre les plateformes de médias sociaux "traditionnelles", d'autres exemples de médias sociaux comprennent : les plateformes de rencontre où les utilisateurs inscrits se présentent pour trouver des partenaires qu'ils peuvent fréquenter dans la vie réelle ; des plates-formes où les utilisateurs inscrits peuvent télécharger leurs propres vidéos, les commenter et créer des liens avec celles des autres ; ou encore des jeux informatiques où les utilisateurs inscrits peuvent jouer en groupe, échanger des informations ou partager leurs expériences et leurs succès dans le jeu.

[3] Le ciblage a été défini comme "l'action de diriger ou de viser quelque chose vers un groupe particulier de personnes" et
"l'action de tenter de séduire une personne ou un groupe ou de les influencer d'une manière ou d'une autre".
h t t p s : //www.collinsdictio n ary.com/dictio
nary/english/targeting .

les options de ciblage publicitaire. En d'autres termes, le ciblage des utilisateurs de médias sociaux ne consiste pas seulement à "sélectionner" les individus ou les groupes d'individus qui sont les destinataires d'un message particulier (le "public cible"), mais il s'agit plutôt d'un processus complet mené par un ensemble de parties prenantes qui aboutit à la diffusion de messages spécifiques à des individus possédant des comptes de médias sociaux. [4]

4. La combinaison et l'analyse de données provenant de différentes sources, ainsi que la nature potentiellement sensible des données à caractère personnel traitées dans le contexte des médias sociaux [5], créent des risques pour les droits et libertés fondamentaux des personnes. Du point de vue de la protection des données, de nombreux risques sont liés à l'éventuel manque de transparence et de contrôle de l'utilisateur. Pour les personnes concernées, le traitement sous-jacent des données à caractère personnel qui aboutit à l'envoi d'un message ciblé est souvent opaque. En outre, il peut impliquer des utilisations imprévues ou non souhaitées des données à caractère personnel, ce qui soulève des questions non seulement en ce qui concerne la législation sur la protection des données, mais aussi par rapport à d'autres droits et libertés fondamentaux. Récemment, le ciblage sur les médias sociaux a suscité un intérêt accru du public et un examen réglementaire dans le contexte de la prise de décision démocratique et des processus électoraux. [6]

2 CHAMP D'APPLICATION

5. *Le* ciblage des utilisateurs de médias sociaux peut impliquer une variété d'acteurs différents qui, aux fins des présentes lignes directrices, seront divisés en quatre groupes : les fournisseurs de médias sociaux, leurs utilisateurs, les cibleurs et les autres acteurs qui peuvent être impliqués dans le processus de ciblage. L'importance d'identifier correctement les rôles et les responsabilités des différents acteurs a été récemment soulignée par les arrêts *Wirtschaftsakademie* et *Fashion ID* de la Cour de justice de l'Union européenne (CJUE). Ces deux arrêts démontrent que l'interaction entre les fournisseurs de médias sociaux et d'autres acteurs peut donner lieu à des responsabilités conjointes en vertu de la législation européenne sur la protection des données.

6. En tenant compte de la jurisprudence de la CJUE, ainsi que des dispositions du GDPR concernant les contrôleurs conjoints et la responsabilité, les présentes lignes directrices offrent des conseils concernant le ciblage des utilisateurs de médias sociaux, en particulier en ce qui concerne les responsabilités des cibleurs et des fournisseurs de médias sociaux. En cas de responsabilité conjointe, les lignes directrices chercheront à clarifier ce à quoi pourrait ressembler la répartition des responsabilités entre les cibleurs et les fournisseurs de médias sociaux sur la base d'exemples pratiques. [8]

7. L'objectif principal de ces lignes directrices est donc de clarifier les rôles et les responsabilités du fournisseur de médias sociaux et du cibleur. Pour ce faire, les lignes directrices identifient également les risques potentiels pour les droits et libertés des personnes (section 3), les principaux acteurs et leurs rôles (section 4), et abordent les questions suivantes

[4] Les messages délivrés sont généralement constitués d'images et de textes, mais peuvent également comporter des formats vidéo et/ou audio.

[5] Les données à caractère personnel traitées dans le cadre des médias sociaux peuvent constituer des "catégories particulières de données à caractère personnel". Conformément à l'article 9 du GDPR, concernent des personnes vulnérables ou sont autrement de nature hautement personnelle. Voir également le groupe de travail Article 29 sur la protection des données, Lignes directrices sur l'évaluation d'impact sur la protection des données (DPIA) et la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679, WP.
248 rév. 01, p. 9.

[6] Voir, par exemple : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf ; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recomndations-et-actions-pour-investigation-ataanalytics-in-politique-campaign/ ;
https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf ; https://www.personuvernd.is/information-in-english/greinar/nr/2880 .

[7] CJUE, Arrêt *Wirtschaftsakademie*, 5 juin 2018, C-210/16, ECLI:EU:C:2018:388 ; CJUE, Arrêt *Fashion ID*, 29 juillet 2019, C-40/17, ECLI:EU:C:2019:629.

[8] Les présentes orientations sont sans préjudice des lignes directrices 07/2020 de l'EDPB sur les concepts de responsable de traitement et de sous-traitant au titre du GDPR, adoptées le 2 septembre 2020, concernant la répartition des responsabilités dans d'autres domaines.
contexte
s

l'application des principales exigences en matière de protection des données (telles que la légalité et la transparence, l'évaluation des risques avant expédition, etc.)
ainsi que les éléments clés des accords entre les fournisseurs de médias sociaux et les personnes ciblées.

8. Néanmoins, le champ d'application des présentes lignes directrices couvre les relations entre les utilisateurs enregistrés d'un réseau social, ses fournisseurs, ainsi que les cibleurs. L'analyse approfondie de scénarios tels que les personnes qui ne sont pas enregistrées auprès des fournisseurs de médias sociaux ne relève pas du champ d'application des présentes lignes directrices.

3 RISQUES POUR LES DROITS ET LIBERTÉS DES UTILISATEURS POSÉS PAR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

9. Le GDPR souligne l'importance d'évaluer et d'atténuer correctement tout risque pour les droits et libertés des personnes résultant du traitement des données personnelles. [9] Les mécanismes qui peuvent être utilisés pour cibler les utilisateurs de médias sociaux, ainsi que les activités de traitement sous-jacentes qui permettent le ciblage, peuvent présenter des risques importants. Les présentes lignes directrices ne cherchent pas à fournir une liste exhaustive des risques possibles pour les droits et libertés des personnes. Néanmoins, l'EDPB considère qu'il est important de souligner certains types de risques et de fournir un certain nombre d'exemples de la manière dont ils peuvent se manifester.

10. Le ciblage des utilisateurs de médias sociaux peut impliquer des utilisations de données à caractère personnel qui vont à l'encontre ou au-delà des attentes raisonnables des individus et enfreint ainsi les principes et règles applicables en matière de protection des données. Par exemple, lorsqu'une plateforme de médias sociaux combine des données à caractère personnel provenant de sources tierces avec des données divulguées par les utilisateurs de sa plateforme, il peut en résulter que les données à caractère personnel sont utilisées au-delà de leur finalité initiale et d'une manière que l'individu ne pouvait raisonnablement pas anticiper. Les activités de profilage liées au ciblage pourraient impliquer une déduction d'intérêts ou d'autres caractéristiques, que la personne n'a pas activement divulgués, ce qui compromet la capacité de la personne à exercer un contrôle sur ses données personnelles. [10] En outre, un manque de transparence concernant le rôle des différents acteurs et les opérations de traitement concernées peut compromettre, compliquer ou entraver l'exercice des droits de la personne concernée.

11. Un deuxième type de risque concerne la possibilité de discrimination et d'exclusion. Le ciblage des utilisateurs de médias sociaux peut impliquer des critères qui, directement ou indirectement, ont des effets discriminatoires liés à l'origine raciale ou ethnique, à l'état de santé ou à l'orientation sexuelle d'une personne, ou à d'autres qualités protégées de la personne concernée. Par exemple, l'utilisation de tels critères dans le cadre de publicités liées à des offres d'emploi, de logement ou de crédit (prêts, hypothèques) peut réduire la visibilité des opportunités offertes aux personnes appartenant à certains groupes d'individus. Le potentiel de discrimination dans le ciblage découle de la possibilité pour les annonceurs d'exploiter la quantité et la variété considérables de données personnelles (par exemple, ~~les données démographiques,~~ comportementales et les intérêts) que les plateformes de médias sociaux recueillent sur leurs utilisateurs. [11] Recherches récentes

[9] Selon l'article 24 du RGPD, le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD, "en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques de probabilité et de gravité variables pour les droits et libertés des personnes physiques". Voir également Groupe de travail Article 29, Lignes directrices sur l'analyse d'impact sur la protection des données

(DPIA) et la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679, WP248 rev. 01, 4 octobre 2017.

[10] Voir également Contrôleur européen de la protection des données, Avis du CEPD sur la manipulation en ligne, Avis 3/2018, 19.
Mars 2018, p. 15 (" *L'inquiétude liée à l'utilisation de données issues de profils à différentes fins par le biais d'algorithmes est que les données perdent leur contexte d'origine. La réaffectation des données est susceptible d'affecter l'autodétermination informationnelle d'une personne, de réduire davantage le contrôle des personnes concernées sur leurs données, ce qui affecte la confiance dans les environnements et services numériques. "*).

[11] T. Speicher a.o., Potential for Discrimination in Online Targeted Advertising, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, *Proceedings of Machine Learning Research* PMLR 81:5-19, 2018, http://proceedings.mlr.pre ss/v81/speicher18a.html . suggère que le potentiel d'effets discriminatoires existe également sans utiliser de critères directement liés à des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD. [12]

12. Une deuxième catégorie de risque concerne la manipulation potentielle des utilisateurs. Les mécanismes de ciblage sont, par définition, utilisés afin d'influencer le comportement et les choix des individus, que ce soit au niveau de leurs décisions d'achat en tant que consommateurs ou au niveau de leurs décisions politiques en tant que citoyens engagés dans la vie civique. [13] Certaines approches de ciblage peuvent toutefois aller jusqu'à porter atteinte à l'autonomie et à la liberté des individus (par exemple, en délivrant des messages individualisés conçus pour exploiter, voire accentuer, certaines vulnérabilités, valeurs ou préoccupations personnelles). Par exemple, une analyse du contenu partagé sur les médias sociaux peut révéler des informations sur l'état émotionnel (par exemple, par l'analyse de l'utilisation de certains mots clés). Ces informations pourraient être utilisées pour cibler l'individu avec des messages spécifiques et à des moments précis auxquels il est censé être plus réceptif, influençant ainsi subrepticement son processus de pensée, ses émotions et son comportement. [14]

13. Les mécanismes de ciblage des utilisateurs de médias sociaux peuvent également être utilisés pour influencer indûment les individus en ce qui concerne le discours politique et les processus électoraux démocratiques. Alors que les campagnes politiques "traditionnelles" hors ligne visent à influencer le comportement des électeurs par le biais de messages généralement disponibles et récupérables (vérifiables), les mécanismes de ciblage en ligne disponibles permettent aux partis politiques et aux campagnes de cibler des électeurs individuels avec des messages sur mesure, spécifiques aux besoins, intérêts et valeurs particuliers du public cible16. [16] Ce ciblage peut même impliquer de la désinformation ou des messages que les individus trouvent particulièrement pénibles, et qui sont donc (plus) susceptibles de stimuler une certaine émotion ou réaction de leur part. Lorsque des messages polarisés ou mensongers (désinformation) sont destinés à des individus spécifiques, sans contextualisation ou exposition à d'autres points de vue, l'utilisation de mécanismes de ciblage peut avoir pour effet de saper le processus électoral démocratique. [17]

14. Dans le même ordre d'idées, l'utilisation d'algorithmes pour déterminer quelles informations sont affichées à quelles personnes peut avoir un effet négatif sur la probabilité d'accéder à des sources d'information diversifiées sur un sujet particulier. Cela peut à son tour avoir des conséquences négatives sur le pluralisme du débat public et l'accès à l'information. [18] Les mécanismes de ciblage peuvent être utilisés pour accroître la visibilité de certains messages, tout en accordant moins d'importance à d'autres. L'impact négatif potentiel peut se faire sentir à deux niveaux. D'une part, il existe des risques liés à ce que l'on appelle les "bulles de filtre", où les gens sont exposés à "plus d'informations identiques" et rencontrent moins d'opinions, ce qui entraîne une polarisation politique et idéologique accrue19. [19] D'autre part, les mécanismes de ciblage peuvent également créer des risques

---

[12] Idem.

[13] Contrôleur européen de la protection des données, avis 3/2018, p. 18.

[14] Voir "Experimental evidence of massive-scale emotional contagion through social networks", Adam D. I. Kramer, Jamie E. Guillory et Jeffrey T. Hancock, PNAS 17 juin 2014 111 (24) 8788-8790 ; première publication le 2 juin 2014 https://doi.org/10.1073/pnas.1320040111, disponible à : https://www.pnas.org/content/111/24/8788 Adam D. I. Kramer Core Data Science Team, Facebook, Inc, Menlo Park, CA 94025.

[15] Voir également le Conseil européen de la protection des données, Déclaration 2/2019 sur l'utilisation des données à caractère personnel dans le cadre de. campagnes politiques, 13 mars 2019, p. 1.

[16] Information Commissioner's Office (ICO), *Democracy disrupted ? Informations personnelles et influence politique*, 10 juillet 2018, p. 14.

[17] Voir également Commission européenne, Orientations de la Commission concernant l'application du droit de l'Union en matière de protection des données dans le cadre de l'Union européenne. Une contribution de la Commission européenne à la réunion des chefs d'État et de gouvernement qui se tiendra à Salzbourg les 19 et 20 novembre. Septembre 2018. Voir également L. M. Neudert et N.M. Marchal, Polarisation and the use of technology in political campagnes et communication, Service de recherche du Parlement européen, 2019, p. 22-24.

[18] Voir également la résolution du Parlement européen du 3 mai 2018 sur le pluralisme des médias et la liberté des médias dans l'Union européenne. Unioneuropéenne.

[19] Contrôleur européen de la protection des données, avis 3/2018, p. 7. de la "surcharge d'informations", selon laquelle les individus ne peuvent pas prendre de décision en connaissance de cause parce qu'ils disposent de trop d'informations et ne peuvent pas savoir si elles sont fiables.

15. La collecte de données personnelles par les fournisseurs de médias sociaux peut ne pas se limiter aux activités réalisées par les individus sur la plateforme de médias sociaux elle-même. Le ciblage des utilisateurs de médias sociaux sur la base d'informations concernant leur comportement de navigation ou d'autres activités en dehors de la plateforme de médias sociaux peut donner aux individus le sentiment que leur comportement est systématiquement surveillé. Cela peut avoir un effet paralysant sur la liberté d'expression, y compris l'accès à l'information. [20] Ces effets peuvent être exacerbés si le ciblage est également fondé sur l'analyse du contenu partagé par les utilisateurs de médias sociaux. Si les messages privés, les posts et les commentaires font l'objet d'une analyse à des fins commerciales ou politiques, cela peut également donner lieu à une autocensure.

16. L'impact négatif potentiel du ciblage peut être considérablement plus important lorsque des catégories d'individus vulnérables sont concernées, comme les enfants. Le ciblage peut influer sur la formation des préférences et des intérêts personnels des enfants, ce qui, en définitive, affecte leur autonomie et leur droit au développement. Considérant 38 du GDPR indique qu'une protection spécifique doit s'appliquer à l'utilisation des données personnelles des enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données personnelles concernant les enfants lors de l'utilisation de services offerts directement à un enfant. [21]

17. L'utilisation des médias sociaux dans l'UE est très répandue puisque 54 % des personnes âgées de 16 à 74 ans ont participé à des réseaux sociaux en 2019. D'ailleurs, ce taux de participation n'a cessé d'augmenter au fil des ans. [22] Le CEPD reconnaît que l'augmentation de la concentration sur les marchés des médias sociaux et du ciblage peut également accroître les risques pour les droits et libertés d'un nombre substantiel de personnes. Par exemple, certains fournisseurs de médias sociaux peuvent être en mesure de combiner, seuls ou en lien avec d'autres entreprises, une plus grande quantité et diversité de données personnelles. Cette capacité, à son tour, peut augmenter la possibilité d'offrir des campagnes de ciblage plus avancées. Cet aspect est pertinent tant du point de vue de la protection des

données (profilage plus approfondi des personnes concernées) que du droit de la concurrence (les capacités d'analyse inégalées fournies par la plateforme peuvent en faire un *"partenaire commercial incontournable"* pour les spécialistes du marketing en ligne). Le degré de pouvoir du marché et de l'information, à son tour, comme l'a reconnu l'EDPB, "*a le potentiel de menacer le niveau de protection des données et de liberté dont jouissent les consommateurs de services numériques*". [23]

18. La probabilité et la gravité des risques susmentionnés dépendront, entre autres, de la nature du mécanisme de ciblage et de la manière dont il est utilisé, ainsi que de la finalité exacte de son utilisation. Les éléments susceptibles d'affecter la probabilité et la gravité des risques dans le contexte du ciblage des utilisateurs de médias sociaux seront examinés plus en détail dans la section 7.

4 ACTEURS ET RÔLES

4.1 Utilisateurs

19. Les individus utilisent les médias sociaux à différents titres et à des fins différentes (par exemple, pour rester en contact avec des amis, pour échanger des informations sur des intérêts communs ou pour rechercher un emploi).

[20] Contrôleur européen de la protection des données, Avis 3/2018, p. 9 et Comité d'experts sur le pluralisme des médias et la transparence de la propriété des médias (MSI-MED), Internet et campagnes électorales, Étude sur l'utilisation d'internet dans les campagnes électorales, étude du Conseil de l'Europe DGI(2017)11, avril 2018, p. 19-21.

[21] Voir également Groupe de travail Article 29 sur la protection des données, Lignes directrices sur la prise de décision individuelle automatisée et
Le profilage aux fins du règlement 2016/679, 6 février 2018, WP251rev. 01, p. 29.

[22] https://ec. europa. eu/eurostat/fr/web/produits-eurostat-news/-/edn-20200630-2.

[23] Déclaration de l'EDPB sur les impacts de la concentration économique sur la protection des données, disponible sur le site :
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf

opportunités). Le terme "utilisateur" est généralement utilisé pour désigner les personnes qui sont inscrites au service (c'est-à-dire celles qui ont un "compte" ou un "profil"). Toutefois, de nombreux services de médias sociaux sont également accessibles aux personnes sans être inscrites (c'est-à-dire sans créer de compte ou de profil). [24]

Ces personnes ne sont généralement pas en mesure d'utiliser toutes les mêmes fonctionnalités ou services offerts aux personnes qui se sont inscrites auprès du fournisseur de médias sociaux. Les personnes qui sont ou ne sont pas inscrites auprès des fournisseurs de médias sociaux peuvent être considérées comme des "personnes concernées" au sens de l'article 4, paragraphe 1, du GDPR, dans la mesure où la personne est directement ou indirectement identifiée ou identifiable. [25]

20. La question de savoir si les personnes sont censées s'inscrire sous un vrai nom ou utiliser un surnom ou un pseudonyme peut varier selon le service de médias sociaux en question. Toutefois, il sera généralement toujours possible de cibler (ou d'isoler) l'utilisateur en question même en l'absence d'une politique relative aux noms réels, car la plupart des types de ciblage ne reposent pas sur les noms d'utilisateur mais sur d'autres types de données personnelles telles que les intérêts, les données sociographiques, le comportement ou d'autres identifiants. Les fournisseurs de médias sociaux encouragent souvent leurs utilisateurs à révéler des données du "monde réel", comme les numéros de téléphone. [26] Enfin, il convient de noter que les fournisseurs de médias sociaux peuvent également permettre le ciblage de personnes qui n'ont pas de compte chez eux. [27]

4.2 Fournisseurs de médias sociaux

21. Les fournisseurs de médias sociaux proposent un service en ligne qui permet de développer des réseaux et des communautés d'utilisateurs, parmi lesquels des informations et des contenus sont partagés. Les services de médias sociaux sont généralement proposés par le biais de navigateurs web ou d'applications dédiées, souvent après avoir demandé à l'utilisateur de fournir un ensemble de données personnelles pour constituer son "compte" ou son "profil". Ils proposent aussi souvent aux utilisateurs des "contrôles" de compte associés pour leur permettre d'accéder aux données à caractère personnel traitées dans le cadre de l'utilisation de leur compte et de les contrôler.

22. Le fournisseur de médias sociaux détermine les fonctionnalités du service. Cela implique à son tour de déterminer quelles données sont traitées, dans quel but, sous quelles conditions, ainsi que la manière dont les données à caractère personnel sont traitées. Cela permet la fourniture du service de médias sociaux mais aussi probablement la fourniture de services, tels que le ciblage, qui peuvent bénéficier aux partenaires commerciaux opérant sur la plateforme de médias sociaux ou en conjonction avec elle.

23. Le fournisseur de médias sociaux a la possibilité de recueillir de grandes quantités de données à caractère personnel relatives au comportement et aux interactions des utilisateurs et des personnes qui ne sont pas enregistrées auprès des fournisseurs de médias sociaux, ce qui lui permet d'obtenir des informations considérables sur les caractéristiques sociodémographiques, les intérêts et les préférences des utilisateurs. Il est important de noter que les "informations" basées sur l'activité des utilisateurs impliquent souvent des données personnelles déduites ou dérivées. Par exemple, lorsqu'un utilisateur interagit avec un certain contenu (par exemple en "aimant" un message sur un média social ou en regardant un contenu vidéo), cette action peut être enregistrée par le fournisseur de médias sociaux et l'on peut en déduire que l'utilisateur en question a apprécié le contenu avec lequel il a interagi.

[24] Les données à caractère personnel et les informations de profilage conservées par les fournisseurs de médias sociaux en relation avec des personnes qui ne sont pas enregistrées auprès de ces derniers sont parfois appelées "profils fantômes".

[25] Voir également le considérant (26) ("singularisation"). Voir également le groupe de travail Article 29 sur la protection des données, avis 4/2007 sur la
concept de données à caractère personnel, 20 juin 2007, WP 136, p.
12 et suivantes.

[26] Dans certains cas, les fournisseurs de médias sociaux demandent des documents supplémentaires afin de vérifier les données fournies, par exemple
par exemple en demandant aux utilisateurs de télécharger leurs cartes d'identité
ou des documents similaires.
Ce ciblage peut être rendu possible sur la base des identifiants en ligne fournis par leurs appareils,
des applications, des outils et des protocoles, tels que des adresses de protocole Internet, des identifiants de cookies ou d'autres identifiants. Cela peut laisser des traces qui, notamment lorsqu'elles sont combinées avec des identifiants uniques et d'autres informations reçues par les serveurs, peuvent être utilisées pour créer des profils des personnes physiques et les identifier. Voir également le considérant (30) du GDPR. Sur la base de cette reconnaissance, des publicités ciblées peuvent être affichées sur un site web que la personne physique visite.

24. Les fournisseurs de médias sociaux recueillent de plus en plus de données non seulement à partir des activités sur la plateforme elle-même, mais aussi à partir d'activités entreprises "hors plateforme", en combinant des données provenant de sources multiples, en ligne et hors ligne, afin de générer des informations supplémentaires. Ces données peuvent être combinées avec des données personnelles que les individus communiquent activement au fournisseur de médias sociaux (par exemple, un nom d'utilisateur, une adresse électronique, une localisation et un numéro de téléphone), ainsi qu'avec des données qui leur sont "attribuées" par la plateforme (comme des identifiants uniques).

4.3 Cibleurs

25. Les présentes lignes directrices utilisent le terme "targeter" pour désigner les personnes physiques ou morales qui utilisent les services de médias sociaux afin de diriger des messages spécifiques vers un ensemble d'utilisateurs de médias sociaux sur la base de paramètres ou de critères spécifiques. Ce qui distingue les "targeters" des autres utilisateurs des médias sociaux, c'est qu'ils sélectionnent leurs messages et/ou leur public cible en fonction des caractéristiques, des intérêts ou des préférences perçus des personnes concernées, une pratique parfois appelée "micro-ciblage". [29] Les cibleurs peuvent s'engager dans le ciblage pour promouvoir des intérêts commerciaux, politiques ou autres. Parmi les exemples typiques, citons les marques qui utilisent les médias sociaux pour faire la publicité de leurs produits, notamment pour accroître la notoriété de la marque. Les partis politiques utilisent également de plus en plus les médias sociaux dans le cadre de leur stratégie de campagne. Les organisations caritatives et autres organisations à but non lucratif utilisent également les médias sociaux pour cibler des messages destinés à des contributeurs potentiels ou pour développer des communautés.

26. Il est important de noter que les utilisateurs de médias sociaux peuvent être ciblés de différentes manières. Par exemple, le ciblage peut se faire non seulement par l'affichage d'une publicité personnalisée (par exemple, par une "bannière" affichée en haut ou sur le côté d'une page web), mais aussi - dans la mesure où cela se produit au sein de la plateforme de médias sociaux - par l'affichage dans le "fil", la "chronologie" ou l'"histoire" d'un utilisateur, où le contenu publicitaire apparaît aux côtés du contenu généré par l'utilisateur. Le ciblage peut également impliquer la création de contenu hébergé par le fournisseur de médias sociaux (par exemple, via une "page" dédiée ou une autre présence sur les médias sociaux) ou ailleurs (c'est-à-dire sur des sites web tiers). Les cibleurs peuvent avoir leurs propres sites web et applications, où ils peuvent intégrer des outils ou des fonctionnalités commerciales spécifiques aux médias sociaux, tels que des plugins ou des logins sociaux, ou en utilisant les interfaces de programmation d'applications (API) ou les kits de développement de logiciels (SDK) proposés par les fournisseurs de médias sociaux.

4.4 Autres acteurs pertinents

27. Les cibleurs peuvent utiliser directement les mécanismes de ciblage proposés par les fournisseurs de médias sociaux ou faire appel aux services d'autres acteurs, tels que les fournisseurs de services marketing, les réseaux publicitaires, les échanges publicitaires, les plateformes côté demande et côté offre, les fournisseurs de gestion de données (DMP) et les sociétés d'analyse de données. Ces acteurs font partie de l'écosystème complexe et évolutif de la publicité en ligne (parfois appelé "adtech") qui collecte et traite les données relatives aux individus (y compris les utilisateurs de médias sociaux), par exemple en suivant leurs activités sur les sites web et les applications. [30]

28. Les courtiers en données et les fournisseurs de gestion de données sont également des acteurs pertinents qui jouent un rôle important dans le ciblage des utilisateurs de médias sociaux. Les courtiers en données et les DMP se distinguent des autres sociétés adtech dans la mesure où ils traitent non seulement les données collectées au moyen de technologies de suivi, mais aussi celles collectées à partir d'autres sources, qui peuvent inclure des données en ligne et hors ligne.

[28] Le traitement de données à caractère personnel par une personne physique dans le cadre d'une activité purement personnelle ou domestique n'entre pas dans le champ d'application matériel du GDPR (art. 2(2)(c)).
Le simple fait de partager sur une page de média social des informations destinées au grand public (par exemple, des informations sur les heures d'ouverture) sans sélection préalable du public visé n'est pas considéré comme un "ciblage".
aux fins des présentes lignes directrices.
[30] Sur la description des différents acteurs, voir WP29, Avis 2/2010 sur la publicité comportementale, à la page 5. L'avis est disponible à l'adresse suivante :
https://ec.europa.eu/justice/article-29/documentation/opinion-recommndation/files/2010/wp171_en.pdf
sources. En d'autres termes, les courtiers en données et les DMP regroupent des données collectées auprès d'une grande variété de sources, qu'ils peuvent ensuite vendre à d'autres acteurs impliqués dans le processus de ciblage. [31]

29. Si chacun des autres acteurs mentionnés ci-dessus peut jouer un rôle important dans le ciblage des utilisateurs de médias sociaux, les présentes lignes directrices se concentrent sur la répartition des rôles et des obligations en matière de protection des données des fournisseurs de médias sociaux et des cibleurs. Des considérations analogues peuvent toutefois s'appliquer aux autres acteurs impliqués dans l'écosystème de la publicité en ligne, en fonction du rôle de chacun dans le processus de ciblage.

4.5 Rôles et responsabilités

30. Afin de clarifier les rôles et responsabilités respectifs des fournisseurs et des cibleurs de médias sociaux, il est important de tenir compte de la jurisprudence pertinente de la CJUE. Les arrêts rendus dans les affaires *Wirtschaftsakademie* (C-210/16), *Témoins de Jéhovah* (C-25/17) et *Fashion ID* (C-40/17) sont particulièrement pertinents ici.

31. Le point de départ de l'analyse est la définition juridique du responsable du traitement. Selon l'article 4(7) du GDPR, un "'responsable du traitement" désigne "*la personne physique ou morale [...] qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel*".

32. Dans l'affaire *Wirtschaftsakademie*, la CJUE a décidé que l'administrateur d'une page dite "fan" sur Facebook doit être considéré comme participant à la détermination des finalités et des moyens du traitement des données à caractère personnel. En effet, selon les observations présentées à la CJUE, la création d'une page fan implique la *définition de paramètres* par l'administrateur, ce qui a une *influence* sur le traitement des données à caractère personnel aux fins de l'*établissement de statistiques* fondées sur les visites de la page fan. [32] En effet, à l'aide des filtres fournis par Facebook, l'administrateur peut définir les critères selon lesquels les statistiques seront établies, voire désigner les catégories de personnes dont les données personnelles seront utilisées par Facebook :

> " *En particulier, l'administrateur de la page fan peut demander - et donc demander le traitement - des données démographiques relatives à son public cible, y compris des tendances en termes d'âge, de sexe, de relation et de profession, des informations sur les modes de vie et les centres d'intérêt du public cible et des informations sur les achats et les habitudes d'achat en ligne des visiteurs de sa page, les catégories de biens et de services qui plaisent le plus, ainsi que des données géographiques qui indiquent à l'administrateur de la page fan où faire des offres spéciales et où organiser des événements, et lui permettent plus généralement de cibler au mieux les informations qu'il propose.* "

33. Étant donné que la définition des paramètres dépend notamment du public cible de l'administrateur "et des objectifs de gestion et de promotion de ses activités", l'administrateur participe également à la détermination des finalités du traitement des données à caractère personnel. 33 L'administrateur a donc

été catégorisé comme un responsable du traitement conjointement responsable du traitement des données à caractère personnel des visiteurs de sa "page", avec le fournisseur de médias sociaux.

34. Comme cela est développé dans la section 9 des présentes lignes directrices, les responsables du traitement peuvent être impliqués à différentes étapes du traitement des données à caractère personnel et à différents degrés. Dans ces circonstances, le niveau de responsabilité de chacun d'eux doit être évalué au regard de toutes les circonstances pertinentes du cas particulier :

> "*[L]'existence d'une responsabilité conjointe n'implique pas nécessairement une responsabilité égale des différents opérateurs impliqués dans le traitement des données à caractère personnel. Au contraire, ces opérateurs peuvent être*

[31] Voir Centre de recherche sur la politique des consommateurs, "*A day in the life of data*", disponible à l'adresse suivante :
http://cprc.org.au/publication/research-report-a-day-in-the-life-of-data/
[32] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, point 36.
[33] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, point 39.

> *impliqués à des stades différents de ce traitement de données à caractère personnel et à des degrés différents, de sorte que le niveau de responsabilité de chacun d'eux doit être apprécié au regard de l'ensemble des circonstances pertinentes du cas d'espèce*. "[34]

35. Tout en concluant que l'administrateur d'une page agit en tant que responsable du traitement, conjointement avec Facebook, la CJUE a également relevé que, en l'espèce, Facebook doit être considéré comme déterminant *principalement* les finalités et les moyens du traitement des données à caractère personnel des utilisateurs de Facebook et des personnes visitant les pages de fans hébergées sur Facebook. [35]

36. Dans l'affaire *Fashion ID*, la CJUE a décidé qu'un opérateur de site web peut être considéré comme un responsable du traitement lorsqu'il intègre sur son site web un plugin social Facebook qui amène le navigateur d'un visiteur à transmettre des données à caractère personnel de ce dernier à Facebook. [36] La qualification de l'exploitant du site web en tant que responsable du traitement est toutefois limitée à l'opération ou à l'ensemble d'opérations dont il détermine effectivement les finalités et les moyens. En l'espèce, la CJUE a considéré que l'exploitant du site Internet n'est en mesure de déterminer, conjointement avec Facebook, que les finalités et les moyens de la collecte et de la communication par transmission des données à caractère personnel des visiteurs de son site Internet. En conséquence, la CJUE a jugé que, pour ce qui concerne l'intégration d'un plug-in social dans un site web, la responsabilité de l'exploitant du site web est engagée :

> " *limitée à l'opération ou à l'ensemble d'opérations de traitement de données à caractère personnel dont elle détermine effectivement les finalités et les moyens, c'est-à-dire la collecte et la communication par transmission des données en cause.* "[37]

37. La CJUE a considéré que l'exploitant du site web n'était pas un responsable du traitement pour les opérations ultérieures38 de traitement de données à caractère personnel effectuées par Facebook après leur transmission à ce dernier, car l'exploitant du site web n'était pas en mesure de déterminer les finalités et les moyens de ces opérations du fait de l'intégration du plug-in social :

> " *En revanche, à la lumière de ces informations, il apparaît d'emblée impossible que Fashion ID détermine les finalités et les moyens des opérations ultérieures de traitement des données à caractère personnel effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne peut être considérée comme un responsable de traitement à l'égard de ces opérations [...]* ". [39]

38. En cas de contrôle conjoint, conformément à l'article 26, paragraphe 1, du GDPR, les responsables du traitement sont tenus de mettre en place un arrangement qui, de manière transparente, détermine leurs responsabilités respectives en matière de respect du GDPR, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives de fournir les informations visées aux articles 13 et 14 du GDPR.

[34] Arrêt *Wirtschaftsakademie*, C-210/16, point 43 ; arrêt *Témoins de Jéhovah*, C-25/17, point 66 et arrêt *Fashion ID*, C-40/17, point 70.
[35] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, point 30.
[36] Arrêt dans l'affaire *Fashion ID*, C-40/17, points 75 et suivants et point 107.
[37] Arrêt dans l'affaire *Fashion ID*, C-40/17, point 107.
[38] Par traitement ultérieur, on entend toute opération de traitement ou ensemble d'opérations de traitement qui suit (c'est-à-dire qui prend
lieu après) la collecte des données. Chez Fashion ID, ce terme est utilisé pour désigner les traitements effectués par Facebook après leur transmission et pour lesquels Fashion ID ne doit pas être considéré comme un responsable conjoint du traitement (car il ne participe pas effectivement à la détermination des finalités et des moyens de ces traitements). Le traitement ultérieur dans un but autre que celui pour lequel les données personnelles ont été collectées n'est autorisé que dans la mesure où l'article 6(4) GDPR relatif au traitement ultérieur est respecté. Par exemple, si un détaillant en ligne collecte des données relatives à l'adresse du domicile d'une personne, un traitement ultérieur consisterait à stocker ou à supprimer ultérieurement ces informations. Toutefois, si ce détaillant en ligne décide ultérieurement de traiter ces données à caractère personnel pour enrichir le profil de la personne concernée à des fins de ciblage, cela équivaudrait à un traitement ultérieur au sens de l'article 6, paragraphe 4, du GDPR, car il implique un traitement dans un but autre que celui pour lequel elles ont été initialement collectées.
[39] Arrêt dans l'affaire *Fashion ID*, C-40/17, point 76.

39. Les sections suivantes précisent, à l'aide d'exemples spécifiques, les rôles des cibleurs et des fournisseurs de médias sociaux par rapport aux différents mécanismes de ciblage. Des considérations spécifiques sont données en particulier sur la manière dont les exigences de licéité et de limitation de la finalité s'appliquent dans ce contexte. Ensuite, les exigences concernant la transparence, les analyses d'impact sur la protection des données et le traitement de catégories particulières de données sont analysées. Enfin, les lignes directrices abordent l'obligation pour les responsables conjoints du traitement de mettre en place un arrangement approprié conformément à l'article 26 du GDPR, en tenant compte du degré de responsabilité du cibleur et du fournisseur de médias sociaux.

5 ANALYSE DES DIFFÉRENTS MÉCANISMES DE CIBLAGE

5.1 Aperçu

40. Les utilisateurs de médias sociaux peuvent être ciblés sur la base de données fournies, observées ou déduites, ainsi que sur une combinaison de celles-ci :

a) **Cibler des individus sur la base de données fournies** - Les "données fournies" font référence aux informations fournies activement par la personne concernée au fournisseur de médias sociaux et/ou au cibleur. [40] Par exemple :

- Un utilisateur de médias sociaux peut indiquer son âge dans la description de son profil d'utilisateur.
- Le fournisseur de médias sociaux, quant à lui, pourrait permettre le ciblage sur la base de ce critère.

- Un cibleur peut utiliser les informations fournies par la personne concernée au cibleur afin de cibler spécifiquement cette personne, par exemple au moyen de données

clients (telles qu'une liste d'adresses électroniques), qui seront mises en correspondance avec les données déjà détenues sur la plateforme de médias sociaux, de sorte que tous les utilisateurs qui correspondent seront ciblés par la publicité41 .

b) **Ciblage sur la base de données observées** - Le ciblage des utilisateurs de médias sociaux peut également avoir lieu sur la base de données observées. [42] Les données observées sont des données fournies par la personne concernée en vertu de l'utilisation d'un service ou d'un dispositif. [43] Par exemple, un utilisateur de médias sociaux particulier pourrait être ciblé sur la base de :

- son activité sur la plateforme de médias sociaux elle-même (par exemple le contenu que l'utilisateur a partagé, consulté ou aimé) ;
- l'utilisation des appareils sur lesquels l'application du média social est exécutée (par exemple GPS
- coordonnées, numéro de téléphone mobile) ;
- les données obtenues par un développeur d'applications tiers en utilisant les interfaces de programmation d'applications (API) ou les kits de développement de logiciels (SDK) proposés par les fournisseurs de médias sociaux ;
- les données collectées par l'intermédiaire de sites web de tiers qui ont incorporé des plugins sociaux ou des pixels ;
- les données collectées par l'intermédiaire d'autres tiers (par exemple, les parties avec lesquelles la personne concernée a interagi, acheté un produit, souscrit à des cartes de fidélité) ; ou
- les données collectées par le biais de services proposés par des sociétés détenues ou exploitées par le fournisseur de médias sociaux.

c) **Ciblage sur la base de données déduites** - Les "données déduites" ou "données dérivées" sont créées par le responsable du traitement sur la base des données fournies par la personne concernée ou telles qu'observées par le responsable du traitement. [44] Par exemple, un fournisseur de médias sociaux ou un cibleur pourrait déduire qu'une personne est susceptible d'être intéressée par une certaine activité ou un certain produit sur la base de son comportement de navigation sur le web et/ou de ses connexions réseau.

---

[40] Groupe de travail Article 29 sur la protection des données, Lignes directrices sur le droit à la portabilité des données, WP 242 rev. 01, 5 avril.
2017, p. 10.

[41] Voir par exemple la décision du tribunal administratif supérieur de Bavière h (Allemagne), Beschluss v.26.09.2018 - 5 CS 18.1157, www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018.

[42] Dans son avis 2/2010 sur la publicité comportementale en ligne, le WP29 a noté qu'"*il existe deux approches principales*
pour établir des profils d'utilisateurs : i) Les profils prédictifs sont établis par inférence à partir de l'observation du comportement individuel et collectif des utilisateurs au fil du temps, notamment en contrôlant les pages visitées et les publicités visualisées ou sur lesquelles on a cliqué. ii) Les profils explicites sont créés à partir des données personnelles que les personnes concernées fournissent elles-mêmes à un service web, par exemple en s'inscrivant" (Groupe de travail Article 29 sur la protection des données, Avis 2/2010 sur la publicité comportementale en ligne, WP 171, p. 7).

[43] Groupe de travail Article 29 sur la protection des données, Lignes directrices sur le droit à la portabilité des données, WP 242 rev. 01, 5 avril.
2017, p. 10

5.2 Ciblage sur la base des données fournies

5.2.1 Données fournies par l'utilisateur au fournisseur de médias sociaux

41. Les individus peuvent divulguer activement un grand nombre d'informations les concernant lorsqu'ils utilisent les médias sociaux. La création d'un compte de média social (ou "profil") implique la divulgation d'un certain nombre d'attributs, qui peuvent inclure le nom, la date de naissance, le sexe, le lieu de résidence, la langue, etc. Selon la nature de la plateforme de médias sociaux, les utilisateurs peuvent inclure des informations supplémentaires telles que le statut relationnel, les intérêts ou l'emploi actuel. Les données personnelles fournies par les utilisateurs de médias sociaux peuvent être utilisées par le fournisseur de médias sociaux pour élaborer des critères, ce qui permet au cibleur d'adresser des messages spécifiques aux utilisateurs des médias sociaux.

Ex ample 1 :

L'entreprise X vend des chaussures pour hommes et souhaite promouvoir une vente de sa collection d'hiver. Pour sa campagne publicitaire, elle souhaite cibler les hommes âgés de 30 à 45 ans qui ont indiqué être célibataires dans leur profil sur les médias sociaux. Elle utilise les critères de ciblage correspondants proposés par le fournisseur de médias sociaux comme paramètres pour identifier le public cible auquel sa publicité doit s'adresser. En outre, le cibleur indique que la publicité doit être affichée aux utilisateurs de médias sociaux pendant qu'ils utilisent le service de médias sociaux entre 17 heures et 20 heures. Pour permettre le ciblage des utilisateurs des médias sociaux sur la base de critères spécifiques, le fournisseur de médias sociaux a préalablement déterminé quels types de données à caractère personnel seront utilisés pour élaborer les critères de ciblage et quels critères de ciblage seront proposés. Le fournisseur de médias sociaux communique également certaines informations statistiques une fois que les publicités ont été affichées au cibleur (par exemple, pour rendre compte de la composition démographique des personnes qui ont interagi avec la publicité).

A. Rôles

42. Dans l'exemple 1, tant le cibleur que le fournisseur de médias sociaux participent à la détermination de la finalité et des moyens du traitement des données à caractère personnel. Il en résulte l'affichage de la publicité auprès du public cible.

43. En ce qui concerne la détermination de la *finalité*, la société X et le fournisseur de médias sociaux déterminent conjointement la finalité du traitement, qui est d'afficher une publicité spécifique à un ensemble d'individus (en l'occurrence des utilisateurs de médias sociaux) qui constituent le public cible, en choisissant les critères de ciblage disponibles associés à ces utilisateurs afin d'atteindre un public probablement intéressé et de

[44] *Idem.*

leur fournir un contenu publicitaire plus pertinent. En outre, il existe également un avantage mutuel découlant de la même opération de traitement, ce qui constitue un indicateur supplémentaire du fait que les objectifs poursuivis par l'entreprise X et le fournisseur de médias sociaux sont inextricablement liés. [45]

44. En ce qui concerne la détermination des *moyens*, le cibleur et le fournisseur de médias sociaux déterminent conjointement les moyens, ce qui se traduit par le ciblage. Le cibleur participe à la détermination des moyens en choisissant d'utiliser les services offerts par le fournisseur de médias

sociaux46, et en lui demandant de cibler un public sur la base de certains critères (c'est-à-dire la tranche d'âge, le statut relationnel, le moment de l'affichage). [47]

Ce faisant, le cibleur définit les critères selon lesquels le ciblage a lieu et désigne les catégories de personnes dont les données personnelles doivent être utilisées. Le fournisseur de médias sociaux, quant à lui, a décidé de traiter les données personnelles de ses utilisateurs de manière à élaborer les critères de ciblage, qu'il met à la disposition du cibleur. [48] Pour ce faire, le fournisseur de médias sociaux a pris certaines décisions concernant les moyens essentiels du traitement, tels que les catégories de données qui seront traitées, les critères de ciblage qui seront proposés et les personnes qui auront accès à (à quels types de) données à caractère personnel qui sont traitées dans le cadre d'une campagne de ciblage particulière. [49]

45. Par souci d'exhaustivité, l'EDPB note que le fournisseur de médias sociaux ne peut être considéré comme un sous-traitant au sens de l'article 4, paragraphe 8, du GDPR. Dans l'exemple 1, les critères de ciblage élaborés par le fournisseur de médias sociaux sur la base des données à caractère personnel des utilisateurs peuvent être utilisés par le fournisseur de médias sociaux pour de futures opérations de traitement, ce qui démontre que ce dernier ne peut pas être considéré comme un sous-traitant. En outre, le fournisseur de médias sociaux ne semble pas traiter les données exclusivement pour le compte de la société X et conformément à ses instructions.

46. Le contrôle conjoint entre le cibleur et le fournisseur de médias sociaux ne s'étend qu'aux traitements dont ils codéterminent effectivement les finalités et les moyens. Il s'étend au traitement des données à caractère personnel résultant de la sélection des critères de ciblage pertinents et de l'affichage de la publicité auprès du public cible. Il couvre également le traitement des données à caractère personnel entrepris par le fournisseur de médias sociaux pour rendre compte au cibleur des résultats de la campagne de ciblage. Le contrôle conjoint ne s'étend toutefois pas aux opérations impliquant le traitement de données à caractère personnel à d'autres stades intervenant avant la sélection des critères de ciblage pertinents ou après l'achèvement du ciblage et du compte rendu (par exemple, l'élaboration de nouveaux critères de ciblage par le fournisseur de médias sociaux sur la base de campagnes de ciblage achevées) et dans lesquelles le cibleur a

---

[45] Voir les lignes directrices EDPB 7/2020 sur les concepts de responsable de traitement et de sous-traitant dans le GDPR, (" *En outre, lorsque les entités n'ont pas la même finalité pour le traitement, le contrôle conjoint peut également, à la lumière de la jurisprudence de la CJUE, être établi lorsque les entités concernées poursuivent des finalités étroitement liées ou complémentaires. Tel peut être le cas, par exemple, lorsqu'un avantage mutuel découle d'un même traitement, à condition que chacune des entités concernées participe à la détermination des finalités et des moyens du traitement en question*").

[46] Voir les lignes directrices 7/2020 de l'EDPB sur les concepts de responsable du traitement et de sous-traitant dans le GDPR, ("*En outre, le choix fait par une entité d'utiliser à ses propres fins un outil ou un autre système développé par une autre entité, permettant de*
le traitement de données à caractère personnel, équivaudra vraisemblablement à une décision conjointe sur les moyens de ce traitement par ces entités. Cela découle de l'affaire Fashion ID, dans laquelle la CJUE a conclu qu'en intégrant sur son site web le bouton "Like" mis à la disposition des exploitants de sites web par Facebook, Fashion ID a exercé une influence déterminante sur les opérations de collecte et de transmission des données à caractère personnel des visiteurs de son site web à Facebook et a donc déterminé conjointement avec Facebook les moyens de ce traitement.)

[47] Voir, à cet égard, *Wirtschaftsakademie*, C-210/16, par. 39 - ECLI:EU:C:2018:388.

[48] Voir dans le même sens également *Fashion ID*, C-40/17, para. 80 : "*ces traitements sont effectués dans les les intérêts économiques tant de Fashion ID que de Facebook Ireland, pour qui le fait de pouvoir utiliser ces données à ses propres fins commerciales est la contrepartie du bénéfice pour Fashion ID*".

[49] Voir l'avis 1/2010.

[50] Voir les lignes directrices de l'EDPB 7/2020 sur les concepts de contrôleur et de sous-traitant dans le GDPR.

n'a pas participé à la détermination des buts et des moyens, de même le fournisseur de médias sociaux ne participe pas, en principe, à la phase de planification d'une campagne de ciblage avant le moment où le cibleur prend contact avec le fournisseur de médias sociaux". [51]

47. L'analyse ci-dessus reste identique même si le cibleur ne fait que préciser les paramètres de son public cible et n'a pas accès aux données personnelles des utilisateurs concernés. En effet, la responsabilité conjointe de plusieurs acteurs pour un même traitement n'exige pas que chacun d'entre eux ait accès aux données personnelles concernées. [52] Le CEPD rappelle que l'accès effectif aux données personnelles n'est pas une condition préalable à la responsabilité conjointe. [53]

B. Base juridique

48. En tant que responsables conjoints du traitement, les deux parties (le fournisseur de médias sociaux et le cibleur) doivent être en mesure de démontrer l'existence d'une base légale (article 6 GDPR) pour justifier le traitement des données personnelles dont chacun des responsables conjoints du traitement est responsable. L'EDPB rappelle qu'aucune hiérarchie spécifique n'est faite entre les différentes bases licites du GDPR : le responsable du traitement doit s'assurer que la base licite choisie correspond à l'objectif et au contexte du traitement en question. L'identification de la base licite appropriée est liée aux principes d'équité et de limitation de la finalité. [54]

49. De manière générale, deux bases juridiques pourraient justifier le traitement qui soutient le ciblage des utilisateurs de médias sociaux : le consentement de la personne concernée (article 6, paragraphe 1, point a) du GDPR) ou les intérêts légitimes (article 6, paragraphe 1, point f) du GDPR). Un responsable du traitement doit toujours examiner quelle est la base juridique appropriée dans les circonstances données. En ce qui concerne les fournisseurs de médias sociaux, l'article 6 (1) b GDPR ne peut pas fournir une base légale pour la publicité en ligne simplement parce que cette publicité finance indirectement la fourniture de leur service. [55] Il en va de même pour le cibleur, car le ciblage des utilisateurs de médias sociaux ne peut être considéré comme un aspect intrinsèque de tout service ou nécessaire à l'exécution d'un contrat avec l'utilisateur. [56]
Si la personnalisation du contenu peut, dans certaines circonstances, constituer un élément intrinsèque et attendu de certains services en ligne57, l'article 6 (1) b GDPR dans le contexte du ciblage des utilisateurs de médias sociaux est difficilement applicable, comme l'illustrent les exemples des présentes lignes directrices. [58]

---

[51] Voir également l'arrêt rendu dans l'affaire *Fashion ID*, C-40/17, point 74 ("une personne physique ou morale ne peut être considérée comme un responsable du traitement, au sens de cette disposition, dans le cadre d'opérations qui précèdent ou suivent la chaîne globale de traitement et pour lesquelles cette personne ne détermine pas la nature du traitement. 74 (" *[une] personne physique ou morale ne peut être considérée comme responsable du traitement, au sens de cette disposition, dans le cadre d'opérations antérieures ou postérieures dans la chaîne globale du traitement pour lesquelles cette personne ne détermine ni les finalités ni les moyens* ") et paragraphe 101.

[52] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, par. 38 - ECLI:EU:C:2018:388 ; arrêt dans l'affaire *Jehovah's Witnesses*,
C-25/17, par. 69 - ECLI:EU:C:2018:551.

[53] Arrêt de la CJUE du 10 juillet 2018 (C-25/17, points 68 à 72).

[54] Voir le paragraphe 18, Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du GDPR dans le cadre de l'article 6, paragraphe 1, point b), du GDPR. contexte de la fourniture de services en ligne aux personnes concernées, Version 2.0, 8 octobre 2019, disponible sur https://edpb.europa.eu/sites/edpb/files/file1/edpb_guidelines-art_6-1-b-adoptée after public consultation en.pdf

[55]Voir para. 52, 53, Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du GDPR dans le cadre de l'article 6, paragraphe 1, point b), du GDPR.

contexte de la fourniture de services en ligne aux personnes concernées, Version 2.0, 8 octobre 2019, disponible sur https://edpb.europa.eu/sites/edpb/files/file1/edpb_guidelines-art_6-1-b-adoptée_after_public_consultation_en.pdf

[56] Il y aurait un manque de nécessité si le cibleur passait à des fournisseurs de médias sociaux malgré une demande directe de la part de l'entreprise.
relation contractuelle avec son client et donc la possibilité de faire de la publicité directe.

[57] Voir p. 15 , Lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du GDPR dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, 8 octobre 2019, disponible à l'adresse suivante .
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[58] Lignes directrices 2/2019 relatives au traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la...
fourniture de services en ligne aux personnes concernées, paragraphe 57.

50. En ce qui concerne la base légale de l'intérêt légitime, l'EDPB rappelle que dans l'affaire *Fashion ID*, la CJUE a rappelé que pour qu'un traitement puisse se fonder sur l'intérêt légitime, trois conditions cumulatives doivent être réunies, à savoir59 (i) la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, (ii) la nécessité de traiter les données à caractère personnel aux fins des intérêts légitimes poursuivis, et (iii) la condition que les libertés et droits fondamentaux de la personne concernée dont les données doivent être protégées ne priment pas. La CJUE a également précisé que dans une situation de contrôle conjoint, " *il est nécessaire que chacun de ces responsables du traitement poursuive un intérêt légitime [...] à travers ces opérations de traitement pour que celles-ci soient justifiées à l'égard de chacun d'eux* ". [60]

51. En ce qui concerne l'exemple 1, le cibleur pourrait considérer que son intérêt légitime est l'intérêt économique d'avoir une publicité accrue pour ses produits grâce au ciblage des médias sociaux. Le fournisseur de médias sociaux pourrait considérer que son intérêt légitime consiste à rendre le service de médias sociaux rentable en vendant des espaces publicitaires. Pour que le cibleur et le fournisseur de médias sociaux puissent se fonder sur l'article 6, paragraphe 1, point f), du GDPR comme base juridique, il faut que les trois conditions cumulatives soient remplies, comme l'a récemment rappelé la CJUE. Même si le cibleur et le fournisseur de médias sociaux considèrent que leurs intérêts économiques sont légitimes, cela ne signifie pas nécessairement qu'ils pourront effectivement se fonder sur l'article 6, paragraphe 1, point f), du GDPR.

52. La deuxième partie du test de mise en balance implique que les contrôleurs conjoints devront établir que le traitement est nécessaire à la réalisation de ces intérêts légitimes. "Nécessaire" exige un lien entre le traitement et les intérêts poursuivis. L'exigence de "nécessité" est particulièrement pertinente dans le contexte de l'application de l'article 6, paragraphe 1, point f), afin de garantir que le traitement des données fondé sur des intérêts légitimes ne conduise pas à une interprétation indûment large de la nécessité de traiter les données. Comme dans d'autres cas, cela signifie qu'il convient d'examiner si d'autres moyens moins invasifs sont disponibles pour servir le même objectif. [61]

53. La troisième étape pour évaluer si le cibleur et le fournisseur de médias sociaux peuvent se fier à l'article
6(1)(f) GDPR comme base légale pour le traitement des données personnelles, est l'exercice de mise en balance nécessaire pour déterminer si l'intérêt légitime en jeu l'emporte sur les intérêts ou les droits et libertés fondamentaux de la personne concernée. [62]

54. L'EDPB rappelle que dans les cas où un responsable du traitement envisage d'invoquer l'intérêt légitime, les obligations de transparence et le droit d'opposition doivent être examinés attentivement. Les personnes concernées devraient avoir la possibilité de s'opposer au traitement de leurs données à des fins ciblées avant que le traitement ne soit lancé. Les utilisateurs de médias sociaux devraient non seulement avoir la possibilité de s'opposer à l'affichage de publicités ciblées lorsqu'ils accèdent à la

plateforme, mais aussi bénéficier de contrôles garantissant que le traitement sous-jacent de ses données personnelles pour la finalité visée n'a plus lieu après son opposition.

55. Le cibleur qui cherche à invoquer l'intérêt légitime devrait, pour sa part, faire en sorte que les personnes puissent facilement exprimer une objection préalable à son utilisation des médias sociaux à des fins de ciblage. Toutefois, dans la mesure où le cibleur n'a pas d'interaction directe avec la personne concernée, il devrait au moins veiller à ce que la plateforme de médias sociaux fournisse à la personne concernée des moyens d'exprimer efficacement son droit d'opposition préalable. En tant que responsables conjoints du traitement, le cibleur et le fournisseur de médias sociaux devraient préciser comment le droit d'opposition des personnes (ainsi que d'autres droits) sera pris en compte dans le contexte de l'accord conjoint (voir section 6). Si l'exercice de mise en balance fait apparaître que les intérêts ou les droits et libertés fondamentaux de la personne concernée l'emportent sur l'intérêt légitime du fournisseur de médias sociaux et du cibleur, le recours à l'article 6, paragraphe 1, point f), n'est pas possible.

56. En ce qui concerne la base légale du consentement, le responsable du traitement doit garder à l'esprit qu'il existe clairement des situations dans lesquelles le traitement ne serait pas licite sans le consentement valable des personnes concernées (article 6, paragraphe 1, point a), du GDPR). Par exemple, le WP29 a précédemment considéré qu'il serait difficile pour les responsables du traitement de justifier l'utilisation d'intérêts légitimes comme base légale pour des pratiques intrusives de profilage et de suivi à des fins de marketing ou de publicité, par exemple celles qui impliquent le suivi des individus sur plusieurs sites web, emplacements, appareils, services ou le courtage de données. [63]

57. Pour être valable, le consentement recueilli pour le traitement doit remplir les conditions énoncées aux articles
4(11) et 7 du GDPR. D'une manière générale, le consentement ne peut constituer une base juridique appropriée que si la personne concernée se voit offrir un contrôle et un véritable choix. Si le consentement est regroupé comme une partie non négociable des conditions générales, il est présumé ne pas avoir été donné librement. Le consentement doit également être spécifique, éclairé et sans ambiguïté et la personne concernée doit pouvoir refuser ou retirer son consentement sans préjudice. [64]

[59] CJUE, arrêt dans l'affaire *Fashion ID*, 29 juillet 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629.
[60] Idem, paragraphe 97.
[61] Avis 06/2014 du groupe de travail de l'article 29 sur la notion d'intérêts légitimes du responsable du traitement des données dans le cadre de... Article 7 de la directive 95/46/CE, WP217, 9 avril 2014, p. 29.
[62] Lors de l'évaluation de l'impact sur les intérêts, les droits fondamentaux et les libertés de l'individu concerné, les considérations suivantes sont particulièrement pertinentes dans le contexte du ciblage destiné aux utilisateurs des médias sociaux (i) les objectifs du ciblage, (ii) le niveau de détail des critères de ciblage utilisés (par ex, une cohorte décrite de manière générale, telle que "les personnes intéressées par la littérature anglaise", ou des critères plus détaillés permettant une segmentation et un ciblage à un niveau plus granulaire), (iii) le type (et la combinaison) de critères de ciblage utilisés (c'est-à-dire si le ciblage se concentre uniquement sur un petit aspect de la personne concernée ou s'il est de nature plus globale), et (iv) la nature (sensibilité), le volume et la source des données utilisées pour élaborer les critères de ciblage. Voir l'article 29 Avis 06/2014 du groupe de travail sur la notion d'intérêts légitimes du responsable du traitement des données en vertu de l'article 7 de la directive 95/46/CE, WP217, 9 avril 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

58. Le consentement (article 6(1)(a) GDPR) pourrait être envisagé, à condition que toutes les conditions d'un consentement valide soient remplies. L'EDPB rappelle que l'obtention du consentement n'annule ni ne diminue en aucune manière les obligations du responsable du traitement de respecter les principes de traitement consacrés par le GDPR, notamment l'article.
5 en ce qui concerne l'équité, la nécessité et la proportionnalité, ainsi que la qualité des données. Même si le traitement des données personnelles est basé sur le consentement de la personne concernée, cela ne légitimerait pas un ciblage disproportionné ou injuste. [65]

59. Enfin, le CEPD est d'avis que le traitement des données à caractère personnel décrit dans l'exemple 1 ne peut être justifié sur la base de l'article 6, paragraphe 1, point b), ni par la plateforme sociale ni par le cibleur. [66]

5.2.2 Données fournies par l'utilisateur de la plateforme de médias sociaux au cibleur

60. Le ciblage peut également impliquer des données fournies par la personne concernée au cibleur, qui utilise alors les données collectées afin de cibler la personne concernée sur les médias sociaux. Par exemple, le ciblage "par liste" se produit lorsqu'un cibleur télécharge des listes préexistantes de données à caractère personnel (telles que des adresses électroniques ou des numéros de téléphone) pour que le fournisseur de médias sociaux les compare aux informations figurant sur la plateforme. Dans ce cas,

le fournisseur de médias sociaux compare les données téléchargées par le cibleur avec les données d'utilisateur qu'il possède déjà, et tous les utilisateurs qui correspondent sont ajoutés au public cible ou en sont exclus (c'est-à-dire que le fournisseur de médias sociaux compare les données téléchargées par le cibleur avec les données d'utilisateur qu'il possède déjà).
Le fournisseur de médias sociaux peut également permettre au cibleur de "vérifier" la liste avant de la finaliser.) Le fournisseur de médias sociaux peut également permettre au cibleur de "vérifier" la liste avant de la finaliser, ce qui signifie qu'un certain traitement a lieu avant même la création de l'audience.

Exemple 2 :

Mme Jones contacte la banque X pour fixer un rendez-vous concernant un éventuel prêt hypothécaire car elle achète une maison. Elle contacte la banque par courrier électronique pour fixer le rendez-vous. Après le rendez-vous, Mme Jones décide de ne pas devenir cliente de la banque. La banque a néanmoins ajouté l'adresse électronique de Mme Jones à sa base de données d'adresses électroniques de clients. Ensuite, la banque utilise sa base de données de courriels, en permettant au fournisseur de médias sociaux de "faire correspondre" la liste des adresses électroniques qu'elle détient avec celles détenues par la plateforme de médias sociaux, afin de cibler les personnes concernées avec toute la gamme de services financiers sur la plateforme de médias sociaux.

[63] Groupe de travail Article 29, Avis sur le profilage et la prise de décision automatisée, WP 251, rév. 01, p. 15, voir également Article 29 WP, Avis sur l'intérêt légitime, p. 32 et 48 : " Dans l'ensemble, il existe un déséquilibre entre l'intérêt légitime de l'entreprise et la protection des droits fondamentaux des utilisateurs et l'article 7, point f), ne devrait pas être invoqué comme fondement juridique du traitement. L'article 7, point a), serait un motif plus approprié à utiliser, pour autant que les conditions d'un consentement valable soient remplies ".
[64] Voir Groupe de travail Article 29, Lignes directrices sur le consentement en vertu du règlement 2016/679, WP259 rev. 01.
[65] Voir Groupe de travail Article 29, Lignes directrices sur le consentement en vertu du règlement 2016/679, WP259 rev. 01, p. 3-4.
[66] Voir les lignes directrices 2/2019 sur le traitement des données à caractère personnel en vertu de l'article 6, paragraphe 1, point b), du GDPR dans le cadre de la...
fourniture de services en ligne aux personnes concernées, Version 2.0, 8 octobre 2019, disponible sur https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adoptée after public consultation en.pdf

Exemple 3 :

M. Lopez est client de la Banque X depuis près d'un an. Lorsqu'il est devenu client, il a fourni une adresse électronique et a été informé par la Banque X, au moment de la collecte, que : (a) son adresse e-mail serait utilisée pour la publicité d'offres liées aux services bancaires qu'il utilise déjà ; et (b) il peut s'opposer à ce traitement à tout moment. La banque a ajouté son adresse électronique à sa base de données de courrier électronique des clients. Ensuite, la banque utilise sa base de données d'e-mails pour cibler ses clients sur la plateforme de médias sociaux avec toute la gamme de services financiers qu'elle propose. [67]

A. Rôles

61. Dans ces exemples, le cibleur, c'est-à-dire la banque, agit en tant que responsable du traitement car il détermine les finalités et les moyens du traitement en collectant, traitant et transmettant activement les données à caractère personnel des personnes concernées au fournisseur de médias sociaux à des fins publicitaires. Le fournisseur de médias sociaux, à son tour, agit en tant que responsable du traitement parce qu'il a pris la décision d'utiliser les données à caractère personnel acquises auprès de l'utilisateur des médias sociaux (c'est-à-dire l'adresse électronique fournie lors de la création de son compte) afin de permettre au cibleur d'afficher de la publicité à un public de personnes spécifiques.

62. Le contrôle conjoint existe en ce qui concerne les opérations de traitement pour lesquelles le fournisseur de médias sociaux et le cibleur déterminent conjointement les finalités et les moyens, en l'occurrence, le téléchargement d'identifiants uniques liés au public visé, la mise en correspondance, la sélection de critères de ciblage et l'affichage ultérieur de la publicité, ainsi que tout rapport relatif à la campagne de ciblage. [68]

63. Dans les deux exemples, la banque agit en tant que contrôleur unique en ce qui concerne la collecte initiale des adresses électroniques de Mme Jones et de M. Lopez respectivement. Le fournisseur de médias sociaux ne participe en aucune manière à la détermination des moyens et des finalités de cette collecte. Le contrôle conjoint commence avec la transmission des données personnelles et la collecte simultanée de celles-ci par le fournisseur de médias sociaux. Il se poursuit tout au long de l'affichage de la publicité ciblée et se termine (dans la plupart des cas) à la fin d'une phase de déclaration ultérieure. Dans certains cas, le contrôle conjoint peut être prolongé, même jusqu'à la suppression de la phase de données, dans la mesure où le cibleur continue à participer à la détermination des finalités et des moyens.

---

[67] Dans les situations où les adresses électroniques sont utilisées pour envoyer du marketing direct aux utilisateurs, les responsables du traitement doivent également tenir compte des dispositions de l'article 13 de la directive "vie privée et communications électroniques". ".

[68] La détermination des finalités et des moyens du traitement du cibleur et du fournisseur de médias sociaux est similaire.
(bien que non identique) à l'exemple 1. En téléchargeant la liste d'adresses électroniques et en fixant les critères de ciblage supplémentaires, le cibleur définit les critères selon lesquels le ciblage a lieu et désigne les catégories de personnes dont les données personnelles doivent être utilisées. De même, le fournisseur de médias sociaux détermine quelles sont les personnes dont les données à caractère personnel seront traitées, en autorisant quelles catégories de données seront traitées, quels critères de ciblage seront proposés et qui aura accès (à quels types de) données à caractère personnel traitées dans le cadre d'une campagne de ciblage particulière. La finalité partagée qui sous-tend ces opérations de traitement ressemble à la finalité identifiée dans l'exemple 1, à savoir l'affichage d'une publicité spécifique à un ensemble d'individus (dans ce cas : les utilisateurs de médias sociaux) qui constituent le public cible.

64. La raison pour laquelle la banque agit en tant que responsable unique du traitement lorsqu'elle collecte les adresses électroniques de Mme Jones et de M. Lopez respectivement, est que la collecte des données a lieu avant la campagne de ciblage (et n'est pas inextricablement liée à celle-ci). Par conséquent, dans ce cas, il faut distinguer entre l'ensemble initial de traitements pour lesquels seule la banque est responsable du traitement et un traitement ultérieur pour lequel un contrôle conjoint existe. La responsabilité de la banque ne s'étend pas aux opérations survenant après l'achèvement du ciblage et du signalement et pour lesquelles le cibleur n'a pas participé aux finalités et aux moyens et pour lesquelles le fournisseur de médias sociaux agit en tant que seul responsable du traitement.

B. Base juridique

65. Dans l'exemple 2, l'article 6, paragraphe 1, point f, du GDPR ne fournit pas de base juridique appropriée pour justifier le traitement en l'espèce, compte tenu du contexte dans lequel les données à caractère personnel ont été fournies. En effet, Mme Jones a contacté la banque dans le seul but de fixer un rendez-vous, à la suite de quoi elle a communiqué son intention de ne pas faire usage des services offerts par la banque. Par conséquent, on peut considérer que Mme Jones ne s'attend pas raisonnablement à ce que ses données à caractère personnel soient utilisées à des fins de ciblage ("re-targeting"). En outre, un test de compatibilité au titre de l'article 6, paragraphe 4, du GDPR conduirait probablement au résultat que ce traitement n'est pas compatible avec la finalité pour laquelle les données personnelles sont initialement collectées.

66. Dans l'exemple 3, le cibleur pourrait être en mesure d'invoquer l'intérêt légitime pour justifier le traitement, compte tenu notamment du fait que M. Lopez a été : (a) informé du fait que son adresse électronique peut être utilisée à des fins de publicité via les médias sociaux pour des services liés à celui utilisé par la personne concernée ; (b) la publicité concerne des services similaires à ceux pour lesquels M. Lopez est déjà client, et (c) M. Lopez a eu la possibilité de s'opposer avant le traitement, au moment où les données personnelles ont été collectées par la banque. Cependant, l'EDPB souhaite préciser que le respect des obligations d'information conformément aux articles 13 et 14 du GDPR et la pesée des intérêts à réaliser conformément à l'article 6 (1)(f) du GDPR sont deux ensembles d'obligations différents. Par conséquent, le simple respect des obligations d'information conformément aux articles 13 et 14 du GDPR ne constitue pas une mesure de transparence à prendre en considération pour la pesée des intérêts conformément à l'article 6, paragraphe 1, point f), du GDPR.

5.3 Ciblage sur la base des données observées

67. Il existe plusieurs façons pour les fournisseurs de médias sociaux d'observer le comportement de leurs utilisateurs. Par exemple, l'observation est possible par le biais du service de médias sociaux lui-même ou peut également être possible sur des sites web externes en vertu de plug-ins sociaux ou de pixels.

Exemple 4 : ciblage basé sur les pixels

M. Schmidt navigue en ligne afin d'acheter un sac à dos. Il visite le site web "BestBags. com", consulte un certain nombre d'articles, mais décide de ne pas faire d'achat. L'opérateur de "BestBags. com" souhaite cibler les utilisateurs de médias sociaux qui ont visité son site Web sans effectuer d'achat. À cette fin, ilintègre un "pixel de suivi "[69] sur son site web, qui est mis à disposition par le fournisseur de médias sociaux. Après avoir quitté le site web de BestBags.com et s'être connecté à son compte de médias sociaux, M. Schmidt commence à voir des publicités pour les sacs à dos qu'il envisageait de commander en naviguant sur BestBags.com.

Exemple 5 : Géo-ciblage

Mme Michu a installé l'application d'un fournisseur de médias sociaux sur son smartphone. Elle se promène dans Paris pendant ses vacances. Le fournisseur de médias sociaux collecte en permanence des informations sur la localisation de Mme Michu via les fonctionnalités GPS de son smartphone [70] , en utilisant les autorisations qui ont été accordées au fournisseur de médias sociaux lors de l'installation de l'application. Mme Michu séjourne dans un hôtel qui est situé à côté d'une pizzeria. La pizzeria utilise la fonctionnalité de géociblage proposée par le fournisseur de médias sociaux pour cibler les personnes qui se trouvent à moins d'un kilomètre de ses locaux pour la première fois au cours des six derniers mois. En ouvrant l'application du fournisseur de médias sociaux sur son smartphone, Mme Michu voit une publicité de la pizzeria, décide qu'elle a faim et achète une pizza via son site web.

Exemple 6 :

Mme Ghorbani crée un compte sur une plateforme de médias sociaux. Au cours du processus d'inscription, il lui est demandé si elle consent au traitement de ses données personnelles pour voir des publicités ciblées sur sa page de média social, sur la base des données qu'elle fournit directement au fournisseur de média social (telles que son âge, son sexe et sa localisation), ainsi que sur la base de son activité sur d'autres sites web en dehors de la plateforme de média social en utilisant des cookies. Elle est informée que ces données seront collectées via des plug-ins de médias sociaux ou des pixels de suivi, les processus lui sont clairement décrits, ainsi que le fait que le ciblage implique d'autres entités qui sont conjointement responsables du respect du GDPR. Il lui est également expliqué qu'elle peut retirer son consentement à tout moment, et un lien vers la politique de confidentialité lui est fourni. Comme Mme Ghorbani souhaite voir des publicités ciblées sur sa page de médias sociaux, elle donne son consentement. Aucun cookie publicitaire n'est placé ou collecté tant que Mme Ghorbani n'a pas exprimé son consentement.

Plus tard, elle visite le site web "Thelatesthotnews. com", sur lequel est intégré un bouton de médias sociaux. Une bannière petite mais bien visible apparaît sur le bord droit de l'écran, demandant à Mme Ghorbani de consentir à la transmission de ses données personnelles au fournisseur de médias sociaux à l'aide de cookies et de plug-ins de médias sociaux. L'exploitant du site web a pris des mesures techniques pour qu'aucune donnée personnelle ne soit transférée à la plateforme de médias sociaux tant qu'elle n'a pas donné son consentement.

[69] Les pixels de suivi sont constitués de petits bouts de code qui sont intégrés au site web du cibleur. Lorsqu'une personne accède au site web du cibleur dans son navigateur, celui-ci envoie automatiquement une demande au serveur du fournisseur de médias sociaux pour obtenir le pixel de suivi. Une fois le pixel de suivi téléchargé, le fournisseur de médias sociaux est généralement en mesure de surveiller la session de l'utilisateur (c'est-à-dire le comportement de l'individu sur le ou les sites web en question). Les données observées peuvent être utilisées afin, par exemple, d'ajouter un utilisateur de médias sociaux à un public cible particulier.
[70] Un fournisseur de médias sociaux peut également être en mesure de déterminer les allées et venues de ses utilisateurs sur la base d'autres points de données, notamment l'adresse IP et les informations WiFi des appareils mobiles, ou les données dérivées de l'utilisateur (par exemple, s'ils
placer des informations sur leur emplacement sur la plateforme dans un
post).

5.3.2 Base juridique

71. Tout d'abord, étant donné que les exemples 4, 5 et 6 impliquent l'utilisation de cookies, les exigences résultant de l'article
5(3) de la directive "vie privée et communications électroniques" doivent être prises en compte.

72. À cet égard, il convient de noter que l'article 5, paragraphe 3, de la directive "vie privée et communications électroniques" exige que les utilisateurs reçoivent des informations claires et complètes, notamment sur les finalités du traitement, avant de donner leur consentement [71], sous réserve d'exceptions très limitées. [72] Une information claire et complète implique que l'utilisateur soit en mesure de déterminer facilement les conséquences de tout consentement qu'il pourrait donner et de s'assurer que le consentement donné est bien éclairé. [73] Par conséquent, le responsable du traitement devra informer les personnes concernées de toutes les finalités pertinentes du traitement - y compris tout traitement ultérieur des données à caractère personnel obtenues en accédant aux informations contenues dans l'équipement terminal.

73. Pour être valable, le consentement recueilli pour la mise en œuvre des technologies de traçage doit remplir les conditions énoncées à l'article 7 du GDPR. [74] Par exemple, le consentement n'est pas valablement constitué si l'utilisation de cookies est autorisée par le biais d'une case à cocher pré-cochée par le prestataire de services, que l'utilisateur doit désélectionner pour refuser son consentement. [75] Sur la base du considérant 32, des actions telles que le défilement ou le balayage d'une page web ou une activité similaire de l'utilisateur ne satisferont en aucun cas à l'exigence d'une action claire et affirmative : de telles actions peuvent être difficiles à distinguer d'autres activités ou interactions de l'utilisateur et il ne sera donc pas non plus possible de déterminer qu'un consentement sans ambiguïté a été obtenu. En outre, dans un tel cas, il sera difficile de fournir à l'utilisateur un moyen de retirer son consentement d'une manière aussi facile que de l'accorder. [76]

[71] Cour de justice de l'Union européenne, arrêt dans l'affaire Planet 49 Gmbh, affaire C-673/17, paragraphe 73.
[72] Voir l'avis 5/2019 sur l'interaction entre la directive "vie privée et communications électroniques" et le GDPR, en particulier en ce qui concerne le...
la compétence, les tâches et les pouvoirs des autorités chargées de la protection des données. Voir également Cour de justice de l'Union européenne, arrêt dans l'affaire Fashion ID, C-40/17, points 89-91.
[73] *Idem*, paragraphe 74.
[74] Lignes directrices EDPB 05/2020 sur le consentement au titre du règlement 2016/679, version 1.1, p. 6.

74. Tout responsable du traitement (conjoint) cherchant à se fonder sur le consentement comme base juridique est tenu de s'assurer que le consentement valide est obtenu. Dans l'affaire *Fashion ID*, la CJUE a souligné l'importance d'assurer la protection efficace et en temps utile des droits de la personne concernée, et le fait que le consentement ne doit pas être donné uniquement au responsable conjoint du traitement qui intervient ultérieurement dans le traitement. Un consentement valable doit être obtenu avant le traitement, ce qui implique que les responsables du traitement (conjoint) doivent évaluer quand et comment les informations doivent être fournies et le consentement obtenu. En d'autres termes, la question de savoir lequel des responsables conjoints du traitement doit être chargé de recueillir le consentement revient à déterminer lequel d'entre eux est impliqué en premier lieu avec la personne concernée. Dans l'exemple 6, étant donné que le placement des cookies et le traitement des données à caractère personnel ont lieu au moment de la création du compte, le fournisseur de médias sociaux doit recueillir son consentement valable avant le placement des cookies publicitaires.

75. L'EDPB rappelle également que dans le cas où le consentement demandé doit être invoqué par plusieurs responsables du traitement (conjoints) ou si les données doivent être transférées ou traitées par d'autres responsables du traitement qui souhaitent se fonder sur le consentement initial, ces organisations doivent toutes être nommées. [77] Dans la mesure où tous les responsables conjoints du traitement ne sont pas connus au moment où le fournisseur de médias sociaux demande le consentement, celui-ci devra nécessairement être complété par des informations et un consentement supplémentaires recueillis par l'opérateur du site web qui intègre le plugin de médias sociaux (c'est-à-dire *Thelatesthotnews.com* dans l'exemple 6).

76. L'EDPB souligne que le consentement qui devrait être recueilli par l'exploitant d'un site web pour la transmission de données à caractère personnel déclenchée par son site web (par l'intégration d'un plug-in social) ne concerne que l'opération ou l'ensemble d'opérations impliquant le traitement de données à caractère personnel dont l'exploitant détermine effectivement les finalités et les moyens [78] . La collecte du consentement par un exploitant de site web, c'est-à-dire "Thelatesthotnews. com" dans l'exemple 6, par exemple, n'annule ni ne diminue en aucune façon l'obligation du fournisseur de médias sociaux de s'assurer que la personne concernée a donné un consentement valable pour le traitement dont il est responsable en tant que responsable conjoint du traitement [79] , ainsi que pour tout traitement ultérieur ou complémentaire qu'il effectue et dont l'exploitant du site web ne détermine pas conjointement les finalités et les moyens (par exemple, les opérations ultérieures de profilage à des fins de ciblage).

77. En outre, tout traitement ultérieur de données à caractère personnel, y compris les données à caractère personnel obtenues par des cookies, des plug-ins sociaux ou des pixels, doit également avoir une base juridique en vertu de l'article 6 du GDPR afin d'être licite. [80]
En ce qui concerne la base juridique du traitement dans les exemples 4, 5 et 6, l'EDPB considère que

---

[75] Cour de justice de l'Union européenne, arrêt dans l'affaire Planet 49, C-637/17, paragraphe 57.
[76] Lignes directrices EDPB 05/2020 sur le consentement en vertu du règlement 2016/679, version 1.1, p. 19.
[77EDPB] Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 16, paragraphe 65.
[78] Arrêt dans l'affaire *Fashion ID*, 29 juillet 2019, C-40/17, ECLI:EU:C:2019:629, paragraphes 100-101.
[79] C'est d'autant plus vrai dans la mesure où, pour la plupart des outils de ciblage, c'est le média social qui effectue les opérations de lecture/écriture sur le terminal de l'utilisateur, car il collecte les données personnelles dans le but de
publicité ciblée. Par conséquent, il incombe au fournisseur de médias sociaux de veiller à ce qu'un consentement valable soit obtenu.
[80Opinion] 5/2019 sur l'interaction entre la directive "vie privée et communications électroniques" et le GDPR, en particulier en ce qui concerne l'application de la directive "vie privée et communications électroniques". compétence, tâches et pouvoirs des autorités chargées de la protection des données, paragraphe 41.

L'intérêt légitime ne peut pas servir de base juridique appropriée, étant donné que le ciblage repose sur le suivi du comportement des individus sur des sites web et dans des lieux différents à l'aide de technologies de suivi. [81]

78. Par conséquent, dans ces circonstances, la base juridique appropriée pour tout traitement ultérieur en vertu de l'article 6 GDPR est également susceptible d'être le consentement de la personne concernée. En effet, lors de l'évaluation de la conformité à l'article 6 GDPR, il faut tenir compte du fait que le traitement dans son ensemble implique des activités spécifiques pour lesquelles le législateur de l'UE a cherché à fournir une protection supplémentaire. [82] En outre, les responsables du traitement doivent tenir compte de l'impact sur les droits des personnes concernées lors de l'identification de la base juridique appropriée afin de respecter le principe d'équité. [83]

5.4 Ciblage sur la base de données inférées

79. Les données déduites font référence aux données créées par le responsable du traitement sur la base des données fournies par la personne concernée (que ces données aient été observées ou fournies activement par la personne concernée, ou une combinaison des deux). [84] Les déductions sur les personnes concernées peuvent être faites à la fois par le fournisseur de médias sociaux et par le cibleur.

80. Par exemple, en surveillant le comportement de ses utilisateurs sur une longue période, tant sur les médias sociaux qu'en dehors (par exemple, les pages visitées, le temps passé sur chaque page, le nombre de reconnexions à cette page, les mots recherchés, les hyperliens suivis, les "j'aime" donnés), le fournisseur de médias sociaux pourrait être en mesure de déduire des informations concernant les intérêts et autres caractéristiques de l'utilisateur des médias sociaux. Dans le même ordre d'idées, un cibleur pourrait également être en mesure de déduire des données sur des individus spécifiques et d'utiliser ces connaissances lorsqu'il le cible pour afficher des publicités sur sa page de média social.

Exemple 7 :

Mme Delucca "aime" souvent les photos publiées par la galerie d'art "Beautifulart" du peintre impressionniste Pataolito sur sa page de médias sociaux. Le Musée Z cherche à attirer des personnes qui s'intéressent aux peintures impressionnistes en raison de sa prochaine exposition. Le musée Z utilise les critères de ciblage suivants proposés par le fournisseur de médias sociaux : "intéressé par l'impressionnisme", sexe, âge et lieu de résidence. Mme Delucca reçoit ensuite une publicité ciblée du Musée Z concernant l'exposition à venir du Musée Z sur sa page de médias sociaux.

[81] Groupe de travail Article 29, Avis sur le profilage et la prise de décision automatisée, WP 251, rév. 01, p. 15, voir également Article 29 WP, Avis sur l'intérêt légitime, p. 32 et 48 : "Dans l'ensemble, il existe un déséquilibre entre l'intérêt légitime de l'entreprise et la protection des droits fondamentaux des utilisateurs et l'article 7, point f), ne devrait pas être invoqué comme fondement juridique du traitement. L'article 7, point a), serait un motif plus approprié à utiliser, pour autant que les conditions d'un consentement valable soient remplies".

[82] Avis 5/2019 sur l'interaction entre la directive "vie privée et communications électroniques" et le GDPR, en particulier en ce qui concerne l'application de la directive "vie privée et communications électroniques". compétence, tâches et pouvoirs des autorités chargées de la protection des données, paragraphe 41.

[83] Conseil européen de la protection des données, G u id e lin e s 2/20 19 surlaprotection des données personnelles en vertude l'article 6, paragraphe 1, point b) G DP R dans le c o n t e xtde la p r ov is io nd e s s e r v ic e so n lin e sà d a t a s u bj e ct s , Version 2.0, 8 octobre 2019, paragraphe. 1.

[84] Voir également Groupe de travail Article 29 sur la protection des données, Lignes directrices sur le droit à la portabilité des données, WP 242 rev. 01,

5 avril 2017, p. 10.

Exemple 8 :

M. Leon a indiqué sur sa page de médias sociaux qu'il s'intéresse au sport. Il a téléchargé une application sur son téléphone portable pour suivre les derniers résultats de ses jeux sportifs préférés, a défini sur son navigateur la page www.livesportsresults.com comme page d'accueil sur son ordinateur portable, utilise souvent son ordinateur de bureau au travail pour rechercher les derniers résultats sportifs sur internet. Il visite également un certain nombre de sites de jeux d'argent en ligne. Le fournisseur de médias sociaux suit l'activité en ligne de M. Leon sur les sites suivants ses multiples appareils, à savoir son ordinateur portable, son téléphone mobile et son ordinateur de bureau. Sur la base de cette activité et de toutes les informations fournies par M. Leon, le fournisseur de médias sociaux en déduit qu'il sera intéressé par les paris en ligne. En outre, la plateforme de médias sociaux a développé des critères de ciblage permettant aux entreprises de cibler les personnes susceptibles d'être impulsives et ayant un revenu plus faible. La société de paris en ligne "bestpaydayloans" souhaite cibler les utilisateurs intéressés par les paris et susceptibles de parier massivement. Elle choisit donc les critères proposés par le fournisseur de médias sociaux pour cibler le public auquel sa publicité doit s'adresser.

5.4.1 Rôles

81. En ce qui concerne la détermination des rôles des différents acteurs, l'EDPB note ce qui suit : dans l'exemple 7, il existe un contrôle conjoint entre le musée Z et le fournisseur de médias sociaux concernant le traitement des données à caractère personnel à des fins de publicité ciblée, compte tenu de la collecte de ces données via la fonction "j'aime" de la plateforme de médias sociaux, et de l'"analyse" effectuée par le fournisseur de médias sociaux afin de proposer le critère de ciblage ("intéressé par l'impressionnisme") au cibleur dans le but d'afficher finalement la publicité. [85]

82. Dans l'exemple 8, un contrôle conjoint existe entre "bestpaydayloans" et le fournisseur de médias sociaux en ce qui concerne les opérations de traitement déterminées conjointement, en l'occurrence la sélection de critères de ciblage et l'affichage ultérieur de la publicité, ainsi que tout rapport relatif à la campagne de ciblage.

5.4.2 Base juridique

83. Le ciblage des utilisateurs de médias sociaux sur la base de données déduites à des fins publicitaires implique généralement le profilage. [86] Le WP29 a précédemment précisé que, selon le GDPR, le profilage est un traitement automatisé de données à caractère personnel qui vise à évaluer des aspects personnels, notamment pour analyser ou faire des prédictions sur des individus, ajoutant que "*[l]'utilisation du mot "évaluer" suggère que le profilage implique une certaine forme d'évaluation ou de jugement sur une personne*". [87] Le profilage peut être licite par référence à l'une des bases juridiques de l'article 6, paragraphe 1, du GDPR, sous réserve de la validité de cette base juridique.

84. Dans l'exemple 7, l'article 5, paragraphe 3, de la directive "vie privée et communications électroniques" est applicable, dans la mesure où l'affichage de la publicité sur la page de Mme Delucca relative au peintre Pataolito nécessite une opération de lecture/écriture pour faire correspondre ce "like" aux informations détenues précédemment sur elle par le fournisseur de médias sociaux. Le consentement sera donc requis pour ces opérations.

85. En ce qui concerne l'exemple 8, l'EDPB rappelle que dans le cas d'une prise de décision automatisée produisant des effets juridiques ou affectant de manière significative la personne concernée, comme

le prévoit l'article 22 du GDPR, les responsables du traitement peuvent se fonder sur les exceptions suivantes :

- le consentement explicite d'une personne concernée ;
- la nécessité de la prise de décision automatisée pour la conclusion ou l'exécution d'un contrat ; ou
- l'autorisation du droit de l'Union ou des États membres auquel le responsable du traitement est soumis.

86. *Le* WP29 a déjà déclaré que "*dans de nombreux cas typiques, la décision de présenter une publicité ciblée fondée sur le profilage n'aura pas d'effet significatif similaire sur les personnes (...). Toutefois, il est possible qu'elle le fasse, en fonction des caractéristiques particulières du cas, notamment :*

le caractère intrusif du processus de profilage, y compris le suivi des personnes sur différents sites web, appareils et services ;

les attentes et les souhaits des personnes concernées ;

la manière dont l'annonce est diffusée ; ou

en utilisant la connaissance des vulnérabilités des personnes concernées ciblées. "[88]

87. Lorsque le profilage effectué par le fournisseur de médias sociaux est susceptible d'avoir un "effet similaire" sur une personne concernée, l'article 22 est applicable. Le responsable du traitement (ou les responsables conjoints du traitement, selon le cas) devra évaluer dans chaque cas si le ciblage aura un "effet significatif similaire" sur une personne concernée, en se référant aux faits spécifiques du ciblage.

88. Dans les circonstances décrites dans l'exemple 8, l'affichage de publicités pour des paris en ligne peut relever du champ d'application de l'article 22 du GDPR (ciblage de personnes financièrement vulnérables qui s'intéressent à des paris en ligne susceptibles d'affecter de manière significative et négative leur situation financière). Par conséquent, conformément à l'article 22, un consentement explicite serait requis. En outre, l'utilisation de techniques de suivi déclenche l'applicabilité de l'article 5, paragraphe 3, de la directive "vie privée et communications électroniques", ce qui entraîne l'exigence d'un consentement préalable. Enfin, l'EDPB rappelle que pour que le traitement soit licite, le responsable du traitement doit procéder à une évaluation au cas par cas, et que l'obtention du consentement ne réduit pas les autres obligations de respecter les exigences de loyauté, de nécessité, de proportionnalité et de qualité des données, comme indiqué à l'article 5 du GDPR.

[85] En ce qui concerne les pages de médias sociaux, les conditions de contrôle conjoint peuvent également être remplies en ce qui concerne les informations statistiques fournies par le fournisseur de médias sociaux à l'administrateur de la page : voir CJUE C-210/16, *Wirtschaftsakademie*.
[86] L'EDPB note que le profilage peut également avoir eu lieu dans des exemples précédents.
[87] Lignes directrices sur la prise de décision individuelle automatisée et le profilage aux fins du règlement 2016/679,
WP251rev. 01, p. 7.

6 TRANSPARENCE ET DROIT D'ACCÈS

89. L'article 5, paragraphe 1, point a), du GDPR dispose que les données à caractère personnel sont traitées de manière licite, loyale et transparente à l'égard de la personne concernée. L'article 5, paragraphe 1, point b), du GDPR dispose également que les données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes. Les articles 12, 13 et 14 du GDPR contiennent des dispositions spécifiques sur les obligations de transparence du responsable du traitement des données. Enfin, le considérant 39 indique qu'" *il devrait être transparent pour les personnes physiques que des données à caractère personnel les concernant sont collectées, utilisées, consultées ou traitées d'une autre manière et dans quelle mesure ces données sont ou seront traitées* ". [89]

90. Les informations présentées aux personnes concernées concernant la manière dont leurs données personnelles sont traitées doivent, dans tous les cas, être concises, transparentes, sous une forme intelligible et facilement accessible, en utilisant un langage clair et simple.

91. L'EDPB rappelle que la simple utilisation du mot "publicité" ne suffirait pas à informer les utilisateurs que leur activité est suivie à des fins de publicité ciblée. Les personnes devraient être informées de manière transparente des types d'activités de traitement effectuées et de ce que cela signifie concrètement pour la personne concernée. Les personnes concernées devraient être informées dans un langage facilement compréhensible si un profil sera établi sur la base de leur comportement en ligne sur la plateforme ou sur le site web du cibleur, respectivement, par la plateforme sociale et par le cibleur, en fournissant des informations aux utilisateurs sur les types de données à caractère personnel collectées pour établir ces profils et permettre en fin de compte le ciblage et la publicité comportementale.

92. Selon l'article 26, paragraphe 1, du GDPR, *les* responsables conjoints du traitement " *déterminent de manière transparente leurs responsabilités respectives en ce qui concerne le respect des obligations découlant du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs devoirs respectifs de fournir les informations visées aux articles 13 et 14, au moyen d'un arrangement entre eux, à moins que, et dans la mesure où, les responsabilités respectives des responsables du traitement soient déterminées par le droit de l'Union ou de l'État membre auquel les responsables du traitement sont soumis. L'arrangement peut désigner un point de contact pour les personnes concernées*".

---

[88] Lignes directrices sur la prise de décision individuelle automatisée et le profilage aux fins du règlement 2016/679, WP251rev. 01, p. 22.

[89] Voir également le groupe de travail Article 29, Lignes directrices sur la transparence en vertu du règlement 2016/679, WP260 rev. 01, 11.
Avril 2018, h t t p s : // e c . e u ro p a . e u /n e w s ro o m /Art ic l e 29/ it e m - d e t a il. c f m ? it e m _ id = 622 227.

[90] Les utilisateurs devraient recevoir les informations pertinentes directement sur l'écran, de manière interactive et, lorsque cela est approprié ou nécessaire, par le biais d'avis superposés. [91]

6.1 Essence de l'arrangement et informations à fournir (article 26 (2) GDPR)

93. Une autre expression du principe de transparence est l'obligation de mettre l'essence de l'accord de contrôle conjoint à la disposition de la personne concernée, conformément à l'article 26, paragraphe 2, du GDPR. En effet, l'article 26 GDPR exige que les responsables conjoints du traitement prennent des mesures appropriées pour s'assurer que les personnes concernées sont informées de la répartition des responsabilités.

94. En principe, les informations fournies à la personne concernée doivent couvrir tous les aspects du ou des traitements de données dont les responsables conjoints sont conjointement responsables. En effet, la personne concernée a le droit de recevoir toutes les informations (y compris celles concernant les traitements ultérieurs envisagés en cas de contrôle conjoint) dès le départ, afin que les informations soient justes et appropriées. Plus précisément, cet accord conjoint doit garantir que la personne concernée recevra les informations requises par les articles 13 et 14 du GDPR, notamment en ce qui concerne les finalités communes ou étroitement liées, les périodes de conservation, la transmission à des tiers, etc. L'arrangement doit indiquer clairement où se situent les responsabilités à cet égard. Pour répondre à ces exigences, cet arrangement doit contenir (ou faire référence) à des informations claires et complètes concernant le traitement auquel il se rapporte, avec des explications, le cas échéant, sur les différentes phases et acteurs du traitement. [92]

95. Bien que les deux responsables conjoints du traitement soient soumis à l'obligation d'informer en cas de responsabilité conjointe, ils peuvent convenir mutuellement que l'un d'entre eux sera chargé de fournir les informations initiales aux personnes concernées, en particulier dans les cas où un seul des responsables du traitement interagit avec les utilisateurs avant le traitement, par exemple sur son site web93 . Cet échange d'informations à fournir à la personne concernée devrait faire partie intégrante de l'accord conjoint (par exemple, une annexe). Dans le cas où l'un des responsables du traitement conjoint ne dispose pas de toutes les informations en détail parce que, par exemple, il ne connaît pas l'exécution technique exacte des activités de traitement, l'autre responsable du traitement conjoint fournit toutes les informations nécessaires pour lui permettre de fournir à la personne concernée des informations complètes conformément aux articles
13 et 14 du GDPR.

96. L'EDPB note que les responsables du traitement ne sont pas directement responsables de la fourniture des informations requises par les articles 13 et 14 du GDPR en ce qui concerne les traitements ultérieurs qui ne relèvent pas du champ d'application du contrôle conjoint. Par conséquent, le cibleur n'est pas directement responsable de la fourniture des informations relatives à tout traitement ultérieur qui sera effectué par la plateforme de médias sociaux. [94]

---

[90] Réf. aux lignes directrices de l'EDPB sur la transparence en vertu du règlement 2016/679.
[91] Groupe de travail Article 29, Lignes directrices sur le consentement dans le cadre du règlement 2016/679, WP259 rév. 01., para 24, 35.
[92] Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", WP 169, p. 28.
[93] CJUE *Fashion ID*, paragraphes 102, 105.
[94] Comme le précisent les lignes directrices 7/2020 de l'EDPB sur les concepts de responsable du traitement et de sous-traitant dans le cadre du GDPR, chaque
l'obligation du responsable du traitement de veiller à ce que les données ne soient pas traitées ultérieurement d'une manière incompatible avec l'obligation d'information.

97. Toutefois, l'EDPB souligne que le responsable conjoint du traitement qui a l'intention d'utiliser ultérieurement les données à caractère personnel a des obligations spécifiques d'information pour ce traitement ultérieur lorsqu'il n'y a pas de responsabilité conjointe, conformément à l'article 14, paragraphe 4, du GDPR, ainsi que des obligations de compatibilité du traitement ultérieur en vertu de l'article 6, paragraphe 4.Par exemple, le cibleur et le fournisseur de médias sociaux pourraient convenir que le cibleur fournira certaines informations au nom du fournisseur de médias sociaux. Le fournisseur de médias sociaux reste toutefois responsable en dernier ressort de s'assurer que la personne concernée a reçu les informations pertinentes en rapport avec toutes les activités de traitement qu'il contrôle.

Dans l'exemple 3 (M. Lopez étant ciblé pour une publicité pour la banque X sur sa page de médias sociaux suite au téléchargement par la banque de son adresse électronique vers le fournisseur de médias sociaux), la banque doit informer M. Lopez que son adresse électronique sera utilisée pour la publicité, via le fournisseur de médias sociaux, d'offres liées aux services de la banque. Tout traitement ultérieur par le fournisseur de médias sociaux doit être licite et compatible avec les finalités pour lesquelles la Banque a collecté les données.

En outre, dans la mesure où le fournisseur de médias sociaux a l'intention de traiter ultérieurement l'e-mail de M. Lopez à une autre fin, il doit s'assurer que M. Lopez reçoit les informations requises par l'article 14(4) GDPR avant de le faire.

Le fournisseur de médias sociaux et la Banque peuvent convenir que la Banque fournira à M. Lopez les informations pertinentes pour le compte du fournisseur de médias sociaux. Même si c'est le cas, le fournisseur de médias sociaux reste toutefois responsable en dernier ressort de s'assurer que la personne concernée a reçu les informations pertinentes en rapport avec toutes les activités de traitement dont il est (seul) responsable. Cette obligation ne s'appliquerait pas si M. Lopez a déjà été informé par la Banque de ce traitement, conformément à l'article 14, paragraphe 5, point a), du GDPR.

Ces obligations de transparence sont à considérer sans préjudice des obligations spécifiques applicables aux considérations de base juridique.

98. Chaque responsable conjoint du traitement est chargé de veiller à ce que l'essence de l'arrangement soit mise à la disposition de la personne concernée. En pratique, l'essence de l'arrangement devrait être directement disponible sur la plateforme, mentionnée dans sa politique de confidentialité, et également rendue directement accessible par un lien, par exemple, dans la page du cibleur sur la plateforme de médias sociaux ou dans des liens tels que " pourquoi est-ce que je vois cette publicité ? ”.

6.2 Droit d'accès (article 15)

99. Les responsables du traitement des données doivent permettre aux utilisateurs d'exercer facilement et pleinement les droits des personnes concernées. Un outil facile à utiliser et efficace doit être mis à la disposition de la personne concernée afin de lui permettre d'exercer facilement et à tout moment l'ensemble de ses droits, notamment le droit à l'effacement, le droit d'opposition et le droit d'accès en vertu de la loi sur la protection des données.

aux fins pour lesquelles elles ont été initialement collectées par le responsable du traitement qui partage les données. La bonne pratique veut que le responsable du traitement qui a l'intention de traiter des données à caractère personnel à d'autres fins fournisse des moyens suffisants à l'autre responsable du traitement qui transmet les données à caractère personnel pour s'assurer qu'il existe effectivement une base juridique, qui serait probablement le consentement, et que les personnes concernées ont été correctement informées, car cela permettrait au responsable du traitement de s'assurer que le transfert au fournisseur de médias sociaux est légal.

Article 15 du GDPR. [95] Les paragraphes suivants se concentrent sur la manière dont et par qui le droit d'accès devrait être accommodé dans le contexte du ciblage des utilisateurs de médias sociaux. [96]

100. En général, pour satisfaire aux exigences de l'article 15 (1) GDPR et pour assurer une transparence totale, les responsables du traitement peuvent envisager de mettre en œuvre un mécanisme permettant aux personnes concernées de vérifier leur profil, y compris les détails des informations et des sources utilisées pour l'élaborer. La personne concernée devrait être en mesure de connaître l'identité de la personne ciblée, et les responsables du traitement devraient faciliter l'accès aux informations concernant le ciblage, y compris les critères de ciblage utilisés, ainsi que les autres informations requises par l'article 15.
GDPR. [97]

101. En ce qui concerne le type d'accès à fournir aux personnes concernées, le considérant 63 conseille que *"[l]orsque cela est possible, le responsable du traitement devrait être en mesure de fournir un accès à distance à un système sécurisé qui permettrait à la personne concernée d'accéder directement à ses données à caractère personnel.*" Les caractéristiques spécifiques des fournisseurs de médias sociaux - l'environnement en ligne, l'existence d'un compte d'utilisateur - suggèrent la possibilité d'accorder facilement à la personne concernée un accès à distance aux données à caractère personnel la concernant conformément à l'article
15 (1), (2) GDPR. En l'espèce, l'accès à distance peut être considéré comme la "mesure la plus appropriée" au sens de l'article 12, paragraphe 1, du GDPR, compte tenu également du fait qu'il s'agit d'une situation typique "où la prolifération des acteurs et la complexité technologique de la pratique font qu'il est difficile pour la personne concernée de savoir et de comprendre si, par qui et dans quel but des données à caractère personnel la concernant sont collectées" (voir le considérant 58, qui ajoute explicitement la "publicité en ligne" comme exemple concret). En outre, s'ils le demandent, les utilisateurs de médias sociaux qui ont été ciblés devraient également recevoir une copie des données à caractère personnel les concernant, conformément à l'article 15, paragraphe 3, du GDPR.

102. Conformément à l'article 15, paragraphe 1, point c), du GDPR, l'utilisateur a notamment accès aux informations sur "*les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires situés dans des pays tiers ou des organisations internationales*". Selon l'article 4, paragraphe 9, le terme "destinataire" désigne une personne physique ou morale, une autorité publique, un service ou un autre organisme, auquel les données à caractère personnel sont communiquées, qu'il s'agisse d'un tiers ou non. Un cibleur ne sera pas nécessairement un "destinataire" des données à caractère personnel (voir l'exemple 1), car les données à caractère personnel peuvent ne pas lui être divulguées, mais il recevra des statistiques sur les clients ciblés sous une forme agrégée ou anonymisée, par exemple dans le cadre de sa campagne ou d'un examen des performances de celle-ci. Néanmoins, dans la mesure où le cibleur agit en tant que contrôleur conjoint, il doit être identifié comme tel auprès de l'utilisateur des médias sociaux.

103. Bien que l'article 15 du GDPR ne soit pas explicitement identifié dans l'article 26(1) du GDPR, la formulation de cet article fait référence à toutes les "responsabilités en matière de conformité" en vertu du GDPR, ce qui inclut l'article 15 du GDPR.

104. Afin de permettre aux personnes concernées d'exercer leurs droits de manière efficace et facilement accessible, l'accord entre le fournisseur de médias sociaux et le cibleur peut désigner un point de contact unique pour les personnes concernées. Les responsables conjoints du traitement sont en principe libres de déterminer entre eux qui doit être chargé de répondre et de se conformer aux demandes des personnes concernées, mais ils ne peuvent pas

[95] L'article 15, paragraphes 1 et 2, du GDPR détaille les informations à fournir à la personne concernée qui demande l'accès à ses données. L'article 15, paragraphes 3 et 4, du GDPR réglemente le droit d'obtenir une copie.

[96] Voir EDPB, Guidelines on transparency under Regulation 2016/679, p. 35.

[97] Pour plus de détails concernant les informations conformément à l'art. 15 RGPD dans le cadre du profilage, voir l'art. 29
Groupe de travail sur la protection des données, WP 251rev. 01, p. 17 pour ("L'*article 15 donne à la personne concernée le droit d'obtenir des précisions sur les données à caractère personnel utilisées pour le profilage, y compris les catégories de données utilisées pour établir un profil. Outre les informations générales sur le traitement, le responsable du traitement est tenu, en vertu de l'article 15, paragraphe 3, de mettre à disposition les données utilisées pour créer le profil, ainsi que l'accès aux informations sur le profil et les détails sur les segments dans lesquels la personne concernée a été placée*"). Il est important que ces informations soient adaptées à la situation particulière de la personne concernée et qu'elles complètent les informations déjà fournies en vertu des articles 1er et 14.

exclure la possibilité pour la personne concernée d'exercer ses droits à l'égard et contre chacun d'entre eux (article 26 (3) du RGPD). Par conséquent, les cibleurs et les fournisseurs de médias sociaux doivent s'assurer qu'un mécanisme approprié est en place pour permettre aux personnes concernées d'obtenir l'accès à leurs données personnelles d'une manière conviviale (y compris les critères de ciblage utilisés) et toutes les informations requises par l'article 26, paragraphe 3, du GDPR.
15 du GDPR.

7 ÉVALUATIONS D'IMPACT SUR LA PROTECTION DES DONNÉES (DPIA)

105. En principe, avant d'entamer les opérations de ciblage envisagées, les deux responsables conjoints du traitement doivent vérifier la liste des traitements "susceptibles d'entraîner un risque élevé" adoptée au niveau national en application de l'article
35(4) et les considérants (71), (75) et (91) du GDPR pour déterminer si le ciblage désigné correspond à l'un des types de traitements soumis à l'obligation de réaliser un DPIA. Pour évaluer si les opérations de ciblage envisagées sont "susceptibles d'entraîner un risque élevé" et si une DPIA est requise, les critères identifiés dans les lignes directrices sur la DPIA doivent également être pris en compte98, ainsi que les listes que les autorités de contrôle ont établies des types d'opérations de traitement qui sont soumises à l'exigence d'une analyse d'impact sur la protection des données (conformément à l'article 35(4)).

106. Dans certains cas, la nature du produit ou du service faisant l'objet de la publicité, le contenu du message ou la manière dont la publicité est diffusée peuvent produire des effets sur les individus dont l'impact doit être évalué de manière plus approfondie. Cela peut être le cas, par exemple, pour des produits destinés à des personnes vulnérables. Des risques supplémentaires peuvent apparaître en fonction des objectifs de la campagne publicitaire et de son caractère intrusif, ou si le ciblage implique le traitement de données personnelles observées, déduites ou dérivées.

107. Outre les obligations spécifiquement visées à l'article 26 (1) du GDPR, les contrôleurs conjoints doivent également prendre en compte d'autres obligations lors de la détermination de leurs obligations respectives. Comme indiqué dans les lignes directrices de l'EDPB sur les DPIA "Lorsque le traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives".

108. En conséquence, les deux responsables conjoints du traitement doivent évaluer si une évaluation des besoins en matière de protection des données est nécessaire. Si c'est le cas, ils sont tous deux responsables de l'exécution de cette obligation. L'EDPB rappelle que l'évaluation doit porter sur l'ensemble du traitement des données à caractère personnel, ce qui signifie qu'en principe, les deux responsables conjoints du traitement doivent prendre part à la réalisation de l'évaluation. Dans ce contexte, les deux responsables du traitement doivent s'assurer qu'ils disposent d'un niveau d'information suffisant sur le traitement pour effectuer le DPIA requis. [99]Cela implique que "chaque responsable du traitement doit exprimer ses besoins et partager les informations utiles sans compromettre les secrets (par exemple : protection des secrets commerciaux, de la propriété intellectuelle, des informations commerciales confidentielles) ni divulguer les vulnérabilités". [100]

109. En pratique, il est possible que les responsables conjoints du traitement décident que l'un d'entre eux sera chargé d'effectuer le DPIA en tant que tel. Cela doit alors être précisé dans l'accord conjoint, sans préjudice de l'existence d'une responsabilité conjointe en tant que telle. Il se peut en effet que l'un des responsables du traitement soit mieux placé pour évaluer certaines opérations de traitement. Par exemple, ce contrôleur peut, en fonction du contexte,

[98] Voir les lignes directrices de l'EDPB sur l'évaluation d'impact sur la protection des données (DPIA) et la détermination du caractère approprié du traitement.
" susceptible d'entraîner un risque élevé " aux fins du règlement 2016/679, wp248rev. 0.
[99] L'EDPB réitère qu'un DPIA n'est pas nécessaire lorsque la nature, la portée, le contexte et les finalités du traitement sont très similaires à ceux du traitement pour lequel un DPIA a été réalisé. Dans de tels cas, les résultats de
Il est possible d'utiliser le DPIA pour des traitements similaires, voir Groupe de travail Article 29 sur la protection des données, Lignes directrices sur l'analyse d'impact sur la protection des données (DPIA) et la détermination du fait que le traitement est "susceptible d'entraîner un risque élevé" aux fins du règlement 2016/679, WP 248 rev.01, p. 12.
[100] *Idem*, page 8.

être celui qui a le plus haut degré de contrôle et de connaissance du processus de ciblage, notamment sur le back-end du système déployé, ou sur les moyens de traitement.

110. Chaque EFDP doit inclure les mesures envisagées pour traiter les risques, y compris les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des données à caractère personnel, et à démontrer la conformité avec le GDPR en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes concernées. Si les risques identifiés ne peuvent être suffisamment traités (c'est-à-dire que les risques résiduels restent élevés), les responsables conjoints du traitement sont chacun chargés d'assurer une consultation préalable des autorités de contrôle compétentes. Si le ciblage devait enfreindre le GDPR, notamment parce que les risques n'ont pas été suffisamment identifiés ou atténués, le ciblage ne doit pas avoir lieu.

Exemple 9 : Le parti politique "Letschangetheworld" souhaite encourager les utilisateurs des médias sociaux à voter pour un candidat politique particulier lors des prochaines élections. Il souhaite cibler les personnes âgées vivant dans les zones rurales du pays, qui vont régulièrement à l'église et qui n'ont pas voyagé à l'étranger au cours des deux dernières années.

111. Il existe un contrôle conjoint entre la plateforme de médias sociaux et le parti politique, pour la mise en correspondance du profil et l'affichage de la publicité ciblée. L'évaluation de la nécessité d'une évaluation des risques avant expédition doit être effectuée à la fois par le parti politique Letschangetheworld et par la plateforme de médias sociaux. En effet, dans cet exemple, ils ont tous deux une connaissance suffisante des critères utilisés pour cibler les personnes afin de voir que le traitement est susceptible d'entraîner un risque élevé.

112. Si une évaluation préliminaire des données personnelles est nécessaire, l'accord conjoint doit aborder la question de savoir comment les responsables du traitement doivent la réaliser et veiller à ce qu'un échange pertinent de connaissances ait lieu. Dans cet exemple, il se peut que la plateforme de médias sociaux soit mieux placée pour évaluer certaines opérations de traitement, dans la mesure où le parti politique se contente de sélectionner des critères de ciblage généraux.

8 CATÉGORIES PARTICULIÈRES DE DONNÉES

8.1. Qu'est-ce qui constitue une catégorie spéciale de données ?

113. Le GDPR prévoit une protection spécifique pour les données à caractère personnel qui sont particulièrement sensibles au regard des droits et libertés fondamentaux des individus. Ces données sont définies à l'article 9 du GDPR comme des catégories particulières de données à caractère personnel et comprennent les données relatives à la santé, l'origine raciale ou ethnique, la biométrie, les convictions religieuses ou philosophiques, les opinions politiques, l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle d'une personne.

114. Les responsables du traitement ne peuvent traiter des catégories particulières de données que s'ils peuvent remplir l'une des conditions énoncées à l'article 9, paragraphe 2, du GDPR, comme avoir obtenu le consentement explicite de la personne concernée ou si les données ont été manifestement rendues publiques par la personne concernée. Outre les conditions de l'article 9 GDPR, le traitement des catégories particulières de données doit reposer sur une base juridique prévue à l'article 6 GDPR et être effectué conformément aux principes fondamentaux énoncés à l'article 5 GDPR.

115. En outre, le traitement de catégories particulières de données à caractère personnel est pertinent pour évaluer les mesures appropriées conformément aux articles 24, 25, 28 et 32 du GDPR, mais aussi pour déterminer si une DPIA doit être réalisée conformément à l'article 35 du GDPR, et si un délégué à la protection des données doit être désigné en vertu de l'article 37 du GDPR.

116. Dans le contexte des médias sociaux et du ciblage, il est nécessaire de déterminer si le traitement des données personnelles implique des "catégories spéciales de données" et si ces données sont traitées par le fournisseur de médias sociaux, le cibleur ou les deux. Si des catégories spéciales de données personnelles sont traitées, il faut déterminer si et dans quelles conditions le fournisseur de médias sociaux et le cibleur peuvent légalement traiter ces données.

117. Si le fournisseur de médias sociaux traite la catégorie spéciale de données à des fins de ciblage, il doit trouver une base juridique pour le traitement à l'article 6 GDPR et s'appuyer sur une exemption à l'article 9(2) GDPR, comme le consentement explicite conformément à l'article 9(2)(a) GDPR. Si un cibleur engage un fournisseur de médias sociaux et demande à ce dernier de cibler les utilisateurs sur la base de cette catégorie spéciale de données, le cibleur sera conjointement responsable avec le fournisseur de médias sociaux du traitement des données de la catégorie spéciale.

118. L'analyse juridique suivante examine les différentes situations dans lesquelles un tel traitement peut avoir lieu et leurs implications juridiques.

8.1.1 Catégories spéciales de données explicites

119. Parfois, les données à caractère personnel traitées relèvent clairement de la définition des catégories spéciales de données, par exemple dans le cas d'une déclaration directe sur l'appartenance d'une personne à un certain parti politique ou à une association religieuse.

Ex am p l e 1 0 :

Mme Flora indique explicitement dans son profil de médias sociaux qu'elle est membre du parti politique GreenestPlanet. L'organisation environnementale "Vive la Terre" souhaite cibler les utilisateurs des médias sociaux qui sont membres du parti politique GreenestPlanet afin de leur adresser des messages ciblés.

120. Dans l'exemple 10, le fournisseur de médias sociaux et l'organisation environnementale agissent en tant que responsables conjoints du traitement. [101] Dans la mesure où l'organisation environnementale demande au fournisseur de médias sociaux de cibler les utilisateurs en fonction de leurs opinions politiques, les deux responsables du traitement contribuent au traitement de catégories particulières de données telles que définies par l'article 9 du GDPR. Le traitement de ces données est en principe interdit conformément à l'article 9, paragraphe 1. Tant le fournisseur de médias sociaux que l'organisation environnementale doivent donc pouvoir invoquer l'une des exemptions prévues à l'article 9, paragraphe 2, pour leur traitement. En outre, ils doivent tous deux disposer d'une base juridique conformément à l'article 6. Parmi les exemptions prévues à l'article 9, paragraphe 2, il apparaît que les seules exemptions applicables dans cette situation seraient l'obtention du consentement explicite de la personne concernée, en vertu de l'article 9, paragraphe 2, point a), du GDPR, ou l'exemption selon laquelle Mme Flora a manifestement rendu publiques les données à caractère personnel, en vertu de l'article 9, paragraphe 2, point e), du GDPR.

8.1.2 Catégories spéciales de données déduites et combinées

121. Les suppositions ou déductions concernant des données de catégorie spéciale, par exemple qu'une personne est susceptible de voter pour un certain parti après avoir visité une page prêchant des opinions libérales, constitueraient également une catégorie spéciale de données à caractère personnel. De même, comme l'a déclaré précédemment l'EDPB, "le *profilage peut créer une catégorie spéciale de*

données par déduction à partir de données qui ne constituent pas une catégorie spéciale de données en soi, mais qui le deviennent lorsqu'elles sont combinées à d'autres données. Par exemple, il peut être possible de déduire l'état de santé d'une personne à partir des enregistrements de ses achats alimentaires combinés à des données sur la qualité et le contenu énergétique des aliments". [102]

122. Par exemple, le traitement d'une simple déclaration, ou d'une seule donnée de localisation ou similaire, qui révèle qu'un utilisateur a (une fois ou à quelques reprises) visité un lieu habituellement fréquenté par des personnes ayant certaines convictions religieuses ne sera généralement pas considéré en soi comme un traitement de catégories particulières de données. Toutefois, il peut être considéré comme un traitement de catégories particulières de données si ces données sont combinées avec d'autres données ou en raison du contexte dans lequel les données sont traitées ou des fins auxquelles elles sont utilisées.

Exemple 1

Le profil du compte de médias sociaux de M. Novak ne révèle que des informations générales telles que son nom et son domicile, mais une mise à jour de statut révèle qu'il a fréquemment visité la City Church où il a assisté à un service religieux. Par la suite, la City Church souhaite cibler ses visiteurs avec des messages religieux afin d'encourager les chrétiens à rejoindre la congrégation. Dans ces circonstances, l'utilisation des données à caractère personnel contenues dans la mise à jour du statut de M. Novak à des fins de ciblage équivaut au traitement de catégories particulières de données à caractère personnel.

123.

Si un fournisseur de médias sociaux ou un cibleur utilise des données observées pour classer les utilisateurs comme ayant certaines convictions religieuses, philosophiques ou politiques - que la catégorisation soit correcte/vraie ou non - cette catégorisation de l'utilisateur doit évidemment être considérée comme un traitement de catégorie spéciale de données à caractère personnel dans ce contexte. Tant que la catégorisation permet un ciblage basé sur des données de catégorie spéciale, la façon dont la catégorie est étiquetée importe peu.

124. Dans l'exemple 12, la grande quantité d'informations et l'absence de mesures visant à empêcher le ciblage fondé sur des données de catégorie spéciale impliquent qu'un traitement de catégories spéciales de données a lieu. Toutefois, le simple fait qu'un fournisseur de médias sociaux traite de grandes quantités de données qui pourraient être utilisées pour déduire des catégories spéciales de données ne signifie pas automatiquement que le traitement relève de l'article 9.
GDPR. L'article 9 ne sera pas déclenché si le traitement du fournisseur de médias sociaux n'entraîne pas la déduction de catégories spéciales de données et si le fournisseur de médias sociaux a pris des mesures pour empêcher que ces données puissent être déduites ou utilisées pour le ciblage. En tout état de cause, le traitement d'un grand nombre de données à caractère personnel concernant les utilisateurs peut entraîner des risques spécifiques pour les droits et libertés des personnes physiques, qui doivent être traités par la mise en œuvre de mesures de sécurité appropriées, comme le prescrit l'article 32 du GDPR, et également en tenant compte du résultat de l'évaluation des risques avant expédition qui doit être effectuée conformément à l'article 35 du GDPR

[101] Voir l'analyse au chapitre 5.2.1.
[102] Groupe de travail Article 29 sur la protection des données, Lignes directrices sur la prise de décision individuelle automatisée et le profilage.
aux fins du règlement 2016/679, WP251rev. 01, page 15.

125. Dans l'exemple 13, l'offre ainsi que l'utilisation de la catégorie de ciblage "intéressé par la politique libérale de gauche" équivaut à un traitement de catégories spéciales de données, car cette catégorie pourrait facilement être utilisée comme proxy pour cibler les personnes qui ont des convictions politiques libérales de gauche. En attribuant une opinion politique inférée à un utilisateur, le fournisseur de médias sociaux traite des catégories spéciales de données. Aux fins de l'article 9 du GDPR, il n'est pas pertinent de savoir si l'utilisateur est en fait un partisan de la politique libérale de gauche. Il n'est pas non plus pertinent que la catégorie de ciblage soit nommée "intéressé par..." et non "partisan de...", puisque l'utilisateur est placé dans la catégorie de ciblage sur la base d'intérêts politiques inférés.

Ex am p l e 1 4 :

M. Svenson passe un test d'aptitude professionnelle développé, contenant une évaluation psychologique, par la société "YourPerfectJob" qui est mis à disposition sur une plateforme de médias sociaux et utilise l'interface de programmation d'applications (API) fournie par le fournisseur de médias sociaux. YourPerfectJob recueille des données sur l'éducation de M. Svenson, sa situation professionnelle, son âge, ses loisirs, ses publications, son adresse électronique et ses relations. YourPerfectJob obtient les données par le biais de l'API conformément aux "autorisations" accordées par M. Svenson par le biais de son compte de média social. L'objectif déclaré de l'application est de prédire quel serait le meilleur parcours professionnel pour un utilisateur spécifique.

Sans que le fournisseur de médias sociaux le sache ou l'approuve, YourPerfectJob utilise ces informations pour déduire un certain nombre d'aspects personnels, notamment ses traits de personnalité, son profil psychologique et ses convictions politiques. YourPerfectJob décide ensuite d'utiliser ces informations pour cibler M. Svenson au nom d'un parti politique, en utilisant la fonction de ciblage par e-mail du fournisseur de médias sociaux, sans ajouter aucun autre critère de ciblage proposé par le fournisseur de médias sociaux.

Dans l'exemple 14, le cibleur traite des catégories spéciales de données à caractère personnel, alors que le fournisseur de médias sociaux ne le fait pas. En effet, l'évaluation et l'identification des convictions politiques de M. Svenson se font sans l'intervention du fournisseur de médias sociaux. [103] En plus de déclencher l'interdiction générale de l'article 9 du GDPR, le ciblage mentionné dans l'exemple 14 constitue également une violation des exigences concernant la loyauté, la transparence et la limitation de la finalité. En effet, M. Svenson n'est pas correctement informé du fait que les données personnelles le concernant seront traitées à des fins de ciblage politique, ce qui, par ailleurs, ne semble pas compatible avec un test d'aptitude professionnelle.

126. Bien que les activités de traitement du fournisseur de médias sociaux dans l'exemple 14 ne constituent pas un traitement de catégories spéciales de données au sens de l'article 9 du GDPR, le fournisseur de médias sociaux est responsable de l'intégration des garanties nécessaires dans le traitement afin de répondre aux exigences du GDPR et de protéger les droits des personnes concernées conformément aux articles 24 et 25.
GDPR

[103] Dans l'exemple 14, il n'y a pas de contrôle conjoint entre le fournisseur de médias sociaux et YourPerfectJob au moment de la collecte des données à caractère personnel, car ils ne déterminent pas conjointement les finalités de la collecte et du traitement ultérieur ou ultérieur des données à caractère personnel aux fins de Yourperfectjob à ce stade du traitement. L'EDPB tient à rappeler que l'analyse des rôles et des responsabilités doit être effectuée au cas par cas et que la conclusion sur cet exemple spécifique ne préjuge en rien de tout autre travail que l'EDPB pourrait effectuer sur les API. La situation serait bien sûr différente si le fournisseur de médias

sociaux, en plus de mettre les données personnelles à disposition, participait également à la détermination de la finalité poursuivie par YourPerfectJob. En tout état de cause, le contrôle conjoint existe toujours entre le cibleur et le fournisseur de médias sociaux en ce qui concerne l'utilisation du ciblage par liste.

8.2 L'exception de l'article 9, paragraphe 2, des catégories particulières de données rendues manifestement publiques

127. L'article 9, paragraphe 2, point e), du GDPR autorise le traitement de catégories particulières de données dans les cas où les données ont été manifestement rendues publiques par la personne concernée. Le mot "manifestement" implique qu'il doit y avoir un seuil élevé pour invoquer cette exemption. L'EDPB note que la présence d'un seul élément ne suffit pas toujours à établir que les données ont été "manifestement" rendues publiques par la personne concernée. En pratique, une combinaison des éléments suivants ou d'autres éléments peut devoir être prise en compte pour que les responsables du traitement puissent démontrer que la personne concernée a clairement manifesté son intention de rendre les données publiques, et une évaluation au cas par cas est nécessaire. Les éléments suivants peuvent être pertinents pour contribuer à cette évaluation :

(i) les paramètres par défaut de la plateforme de médias sociaux (c'est-à-dire si la personne concernée a pris une mesure spécifique pour changer ces paramètres privés par défaut en paramètres publics) ; ou

(ii) la nature de la plate-forme de médias sociaux (c'est-à-dire si cette plate-forme est intrinsèquement liée à l'idée de se connecter avec des connaissances proches de la personne concernée ou de créer des relations intimes (comme les plates-formes de rencontres en ligne), ou si elle est destinée à fournir un champ plus large de relations interpersonnelles, comme les relations professionnelles, ou le microblogging, le partage de médias, les plates-formes sociales pour partager des critiques en ligne, etc. ; ou

iii) l'accessibilité de la page où les données sensibles sont publiées (c'est-à-dire si les informations sont accessibles au public ou si, par exemple, la création d'un compte est nécessaire avant d'accéder aux informations) ; ou

iv) la visibilité de l'information lorsque la personne concernée est informée du caractère public de l'information qu'elle publie (c'est-à-dire s'il y a par exemple une bannière continue sur la page, ou si le bouton de publication informe la personne concernée que l'information sera rendue publique...) ; ou

(v) si la personne concernée a publié elle-même les données sensibles ou si, au contraire, les données ont été publiées par un tiers (par exemple, une photo publiée par un ami qui révèle des données sensibles) ou déduites.

128. L'EDPB note que la présence d'un seul élément ne suffit pas toujours à établir que les données ont été "manifestement" rendues publiques par la personne concernée. En pratique, une combinaison de ces éléments ou d'autres peut devoir être prise en compte pour que les responsables du traitement puissent démontrer que la personne concernée a clairement manifesté son intention de rendre les données publiques.

Exemple 1 5 :

M. Jansen a ouvert un compte sur une plateforme de médias sociaux de microblogging. En remplissant son profil, il a indiqué qu'il était homosexuel. Étant conservateur, il a choisi de rejoindre des groupes conservateurs, sachant qu'il a été informé lors de son inscription que les messages qu'il échange sur la plateforme sont publics. Un parti politique conservateur souhaite cibler les personnes qui partagent

les mêmes affiliations politiques et la même orientation sexuelle que M. Jansen en utilisant les outils de ciblage des médias sociaux.

129. Étant donné que l'orientation sexuelle des membres est par défaut "privée" et que M. Jansen n'a pris aucune mesure pour la rendre publique, elle ne peut être considérée comme ayant été manifestement rendue publique. En outre, les données relatives à son affiliation politique n'ont pas été rendues manifestement publiques, en dépit (i) de la nature de la plateforme de médias sociaux de microblogging, qui est destinée à partager des informations avec le grand public, et (ii) du fait qu'il a été informé du caractère public des messages qu'il publie sur les forums. En outre, bien qu'il ait rejoint des forums publics relatifs au conservatisme, il ne peut être ciblé sur la base de ces données sensibles, car c'est la plateforme de médias sociaux qui fait une déduction sur l'appartenance politique de M. Janssen, et ce n'était pas l'intention spécifique de la personne concernée de rendre ces données manifestement publiques, d'autant plus que cette déduction peut se révéler fausse. Il ne peut paspeuvent donc être ciblés sur la base de données relatives à l'appartenance politique. En d'autres termes, les circonstances de chaque cas spécifique doivent être prises en compte pour évaluer si les données ont manifestement été rendues publiques par la personne concernée. [104]

9 CONTRÔLE ET RESPONSABILITÉ DE CONTRÔLE EN CONTRÔLE CONJOINT

9.1 Accord sur le traitement conjoint et détermination des responsabilités (article 26 du GDPR)

130. L'article 26 (1) du GDPR exige que les contrôleurs conjoints déterminent - de manière transparente - leurs responsabilités respectives en matière de respect des obligations du GDPR dans le cadre d'un arrangement, y compris, comme expliqué ci-dessus, les exigences de transparence.

131. En termes de champ d'application, l'EDPB considère que l'arrangement entre les cibleurs et les fournisseurs de médias sociaux devrait englober toutes les opérations de traitement dont ils sont conjointement responsables (c'est-à-dire qui sont sous leur contrôle conjoint). En concluant un arrangement qui n'est que superficiel et incomplet, les cibleurs et les fournisseurs de médias sociaux ne respecteraient pas les obligations qui leur incombent en vertu de l'article 26 du GDPR.

> Par exemple, dans l'exemple 4, l'accord devrait couvrir l'ensemble du traitement des données à caractère personnel en cas de contrôle conjoint, c'est-à-dire de la collecte des données à caractère personnel dans le cadre de la visite par M. Schmidt du site web "BestBags.com" avec un pixel de suivi, à l'affichage de la publicité sur sa page de médias sociaux, ainsi que tout rapport éventuel relatif à la campagne de ciblage.

132. Afin d'élaborer un arrangement complet, le fournisseur de médias sociaux et le cibleur doivent tous deux être conscients et disposer d'informations suffisamment détaillées concernant les opérations spécifiques de traitement des données qui ont lieu. L'arrangement entre le cibleur et le fournisseur de médias sociaux doit donc contenir (ou faire référence à) toutes les informations nécessaires pour permettre aux deux parties de se conformer à leurs obligations en vertu du GDPR, y compris leur obligation de respecter les principes en vertu de l'article 5(1) GDPR et leur obligation de démontrer leur conformité conformément à l'article 5(2) GDPR.

133. Si, par exemple, le responsable du traitement envisage d'invoquer l'article 6, paragraphe 1, point f), du GDPR comme base juridique, il est nécessaire, entre autres, de connaître l'étendue du traitement des

données afin de pouvoir évaluer si l'intérêt du ou des responsables du traitement l'emporte sur les intérêts ou les libertés et droits fondamentaux des personnes concernées. Sans informations suffisantes concernant le traitement, une telle évaluation ne peut être effectuée. On ne saurait trop insister sur l'importance d'inclure ou de référencer les informations nécessaires dans le cadre d'un accord conjoint, en particulier dans les situations où l'une des parties a presque exclusivement la connaissance et l'accès aux informations nécessaires pour que les deux parties se conforment au GDPR.

Par exemple, dans l'exemple 1, lorsque l'entreprise X évalue si elle peut se fonder sur l'intérêt légitime comme base juridique pour cibler les hommes âgés de 30 à 45 ans qui ont indiqué être célibataires, il est nécessaire qu'elle ait accès à des informations suffisantes concernant le traitement effectué par la plateforme de médias sociaux, y compris, par exemple, en ce qui concerne les éléments supplémentaires suivants mesures (telles que le droit d'opposition préalable) mises en place par ce dernier, afin de garantir que des mesures légitimes de protection de l'environnement soient prises.
les intérêts de la personne concernée ne prévalent pas sur ses intérêts ou ses droits et libertés

Afin de garantir que les droits de la personne concernée puissent être pris en compte de manière efficace, l'EDPB estime que la finalité du traitement et la base juridique correspondante devraient également être reflétées dans l'accord conjoint entre les cibleurs et les fournisseurs de médias sociaux qui sont des responsables conjoints du traitement. Bien que le GDPR n'empêche pas les contrôleurs conjoints d'utiliser une base juridique différente pour les différents traitements qu'ils effectuent, il est recommandé d'utiliser, dans la mesure du possible, la même base juridique pour un outil de ciblage particulier et pour une finalité particulière. En effet, si chaque étape du traitement est traitée sur une base juridique différente, cela rendrait l'exercice des droits impraticable pour la personne concernée (par exemple, pour une étape, il y aurait un droit à la portabilité des données, pour une autre, un droit d'opposition).

134 En tant que contrôleurs, le cibleur et le fournisseur de médias sociaux sont tous deux responsables du respect du principe de limitation de la finalité et doivent donc intégrer des dispositions appropriées à cette fin dans l'accord conjoint.

135 Par exemple, si le cibleur souhaite utiliser les données personnelles qui lui ont été fournies par la personne concernée afin de
de cibler sur les médias sociaux, il doit prendre des mesures appropriées pour garantir que les données fournies ne seront pas utilisées ultérieurement par le fournisseur de médias sociaux d'une manière incompatible avec ces finalités, à moins que le consentement valable de la personne concernée n'ait été obtenu conformément à l'article 6, paragraphe 4, du GDPR.

Dans l'exemple 3, la banque X doit s'assurer que l'accord conjoint avec la plateforme de médias sociaux contient des dispositions appropriées pour que l'adresse électronique de M. Lopez ne soit pas utilisée à d'autres fins que la publicité d'offres liées aux services bancaires qu'il utilise déjà, sans le consentement de M. Lopez.

136 De même, le fournisseur de médias sociaux doit s'assurer que l'utilisation des données à des fins de ciblage par les cibleurs est conforme aux principes de limitation de la finalité, de transparence et

Parmi les autres obligations qui devraient être prises en compte par le cibleur et le fournisseur de médias sociaux dans le cadre de leur accord conjoint, on peut citer : les autres principes généraux de protection des données contenus dans l'article 5
GDPR, la sécurité du traitement, la protection des données par conception et par défaut, les notifications et communications des violations de données personnelles, les évaluations d'impact sur la protection des données, le recours à des sous-traitants et les transferts vers des pays tiers.

137. Enfin, l'accord conjoint entre le fournisseur de médias sociaux et le cibleur doit contenir des informations spécifiques sur la manière dont les obligations prévues par le GDPR seront remplies en pratique. S'il n'y a pas de clarté sur la manière dont les obligations doivent être remplies, en particulier en ce qui concerne les droits des personnes concernées, tant le cibleur que le fournisseur de médias sociaux seront considérés comme agissant en violation de l'article 26, paragraphe 1, du GDPR. En outre, dans de tels cas, les deux responsables (conjoints) du traitement n'auront pas mis en œuvre les dispositions de l'article 26, paragraphe 1, du GDPR.

9.2 Niveaux de responsabilité

138. L'EDPB observe que les cibleurs qui souhaitent utiliser les outils de ciblage fournis par un fournisseur de médias sociaux peuvent être confrontés à la nécessité d'adhérer à des arrangements prédéfinis, sans aucune possibilité de négocier ou d'apporter des modifications (conditions "à prendre ou à laisser"). L'EDPB considère qu'une telle situation ne nie pas la responsabilité conjointe du fournisseur de médias sociaux et du cibleur et ne peut servir à exempter l'une ou l'autre des parties de ses obligations au titre du GDPR. Les deux parties à l'accord conjoint sont également tenues de veiller à ce que la répartition des responsabilités reflète dûment leurs rôles et relations respectifs vis-à-vis des personnes concernées, de manière pratique, véridique et transparente.

139. Il est important de souligner qu'un arrangement en vertu de l'article 26 du GDPR ne peut pas annuler les obligations légales qui incombent à un contrôleur (conjoint). Alors que les responsables conjoints du traitement doivent, conformément à l'article 26 du GDPR, s'acquitter de leurs obligations légales. 26 GDPR " *déterminent leurs responsabilités respectives en matière de conformité* " au GDPR, chaque responsable de traitement reste, par principe, responsable de la conformité du traitement. Cela signifie que chaque responsable du traitement est - *entre autres* - responsable du respect des principes énoncés à l'article 5, paragraphe 1, du GDPR, y compris le principe de licéité établi à l'article 5, paragraphe 1, point a), du GDPR.

140. Toutefois, le degré de responsabilité du cibleur et du fournisseur de médias sociaux par rapport à des obligations spécifiques peut varier. Dans l'affaire *Wirtschaftsakademie*, la CJUE a noté que " *l'existence d'une responsabilité conjointe n'implique pas nécessairement une responsabilité égale des différents opérateurs impliqués dans le traitement des données à caractère personnel. [...] ces opérateurs peuvent être impliqués à des stades différents de ce traitement de données à caractère personnel et à des degrés différents, de sorte que le niveau de responsabilité de chacun d'eux doit être apprécié au regard de l'ensemble des circonstances pertinentes du cas d'espèce*". [105]

[104] Le WP29 a précisé, dans son avis sur certaines questions clés de la directive relative à l'application de la loi (WP 258, 29/11/2017, p. 10), que l'expression " manifestement rendu public par la personne concernée " doit être interprétée comme impliquant que la personne concernée était consciente que les données respectives seront accessibles au public, ce qui signifie à tout le monde, y compris aux autorités ; par conséquent, " En cas de doute, il convient d'appliquer une interprétation étroite... ".

141. En d'autres termes, bien que les responsables conjoints du traitement soient tous deux responsables du respect des obligations prévues par le GDPR, et que la personne concernée puisse exercer ses droits à l'encontre de chacun des responsables du traitement, leur niveau de responsabilité doit être évalué sur leur rôle réel dans le traitement. Dans l'affaire *Google Spain*, la CJUE a précisé qu'un responsable du traitement doit s'assurer, " *dans le cadre de ses responsabilités, pouvoirs et capacités* ", que le traitement des données à caractère personnel répond aux exigences de la législation de l'UE en matière de protection des données. [106]

142. Lorsqu'il s'agit d'évaluer le niveau de responsabilité des cibleurs et des fournisseurs de médias sociaux, plusieurs facteurs peuvent être pertinents, tels que la capacité d'influencer le traitement sur un plan pratique, ainsi que la connaissance réelle ou constructive de chacun des responsables conjoints du traitement. Il est également important de préciser à quel stade du traitement et dans quelle mesure ou à quel degré le cibleur et le fournisseur de médias sociaux sont responsables du traitement. [107]

Dans l'exemple 1, l'entreprise X met en place une campagne publicitaire afin que les utilisateurs correspondant à des critères de ciblage spécifiques puissent recevoir des publicités pour l'entreprise sur la plateforme de médias sociaux. Toutefois, bien qu'elle définisse les paramètres de la campagne publicitaire, elle ne recueille pas et ne dispose pas d'informations sur les utilisateurs.

Il n'a pas accès aux données personnelles et n'a pas non plus de contact direct avec la personne concernée. Chacun de ces
Les éléments peuvent être pertinents lors de l'évaluation du niveau (ou "degré") ou de la responsabilité du cibleur et du fournisseur de médias sociaux dans le cas où une violation du GDPR est établie (par exemple, en cas de manque de transparence envers la personne concernée ou de manquement à la légalité du traitement). Comme indiqué précédemment, nonobstant, les deux parties sont tenues de prendre des mesures appropriées afin de satisfaire aux exigences du GDPR et

Dans l'exemple 3, qui concerne le ciblage par liste, la situation est légèrement différente de celle de l'exemple 1.
Dans l'exemple 3, la banque a initialement collecté les données personnelles et les a partagées avec le fournisseur de médias sociaux à des fins de ciblage. Dans ce cas, le cibleur a volontairement provoqué l'étape de collecte et de transmission du traitement des données. Chacun de ces éléments doit être pris en compte pour évaluer le niveau de responsabilité de chaque acteur et doit être

[105] Arrêt de la CJUE du 05 juin 2018, Wirtschaftsakademie, C-210/16, point 43.
[106] Voir également CJUE, C-131/12, Google Spain ("responsabilités, pouvoirs et capacités").
[107] L'EDPB considère que dans une variété de cas, une évaluation basée sur les critères mentionnés ci-dessus (par exemple, la données utilisées pour établir les critères de ciblage, le rapprochement de la personne concernée, la collecte du consentement) aboutira probablement au résultat que c'est le fournisseur de médias sociaux qui a une plus grande influence factuelle sur le traitement et qui a donc un degré de responsabilité plus élevé, selon le mécanisme de ciblage spécifique utilisé.

De même, dans l'exemple 4, en cas de ciblage par pixel, il convient de tenir compte du fait que l'exploitant du site web permet la transmission de données à caractère personnel au fournisseur de médias sociaux. C'est en effet le site web "BestBags. com" qui intègre un pixel de suivi sur son site web afin de pouvoir cibler M. Schmidt, bien qu'il ait décidé de ne pas faire d'achat108. Le site web participe donc activement à la collecte et à la transmission des données. Toutefois, en tant que responsable conjoint du traitement, le fournisseur de médias sociaux est également tenu de prendre des mesures appropriées pour répondre aux exigences du GDPR et protéger les droits des personnes concernées contre les formes illicites de traitement. Dans ce cas, si le consentement de la personne concernée est demandé, les responsables conjoints du traitement doivent convenir de la manière

143. Lorsqu'il s'agit d'évaluer le niveau de responsabilité du fournisseur de médias sociaux, l'EDPB observe que plusieurs mécanismes de ciblage reposent sur le profilage et/ou d'autres activités de traitement entreprises au préalable par le fournisseur de médias sociaux. C'est le fournisseur de médias sociaux qui décide de traiter les données personnelles de ses utilisateurs de manière à élaborer les critères de ciblage qu'il met à la disposition des cibleurs. Pour ce faire, le fournisseur de médias sociaux a pris de manière indépendante certaines décisions concernant le traitement, telles que les catégories de données à traiter, les critères de ciblage à proposer et les personnes qui auront accès (à quels types de) données personnelles traitées dans le cadre d'une campagne de ciblage particulière. Ces activités de traitement doivent également être conformes au GDPR, avant l'offre de tout service de ciblage.

144. Les exemples mentionnés dans les paragraphes précédents indiquent l'importance de répartir clairement les responsabilités dans l'accord de traitement conjoint entre les fournisseurs de médias sociaux et les cibleurs. Même si les termes de l'accord doivent en tout état de cause refléter le niveau de responsabilité de chaque acteur, un accord complet qui reflète dûment le rôle et les capacités de chaque partie est nécessaire non seulement pour se conformer à l'article 26 du GDPR, mais aussi pour respecter les autres règles et principes du GDPR.

145. Enfin, l'EDPB note que, dans la mesure où les termes de l'accord conjoint entre le fournisseur de médias sociaux et le cibleur ne lient pas les autorités de contrôle, ces dernières peuvent exercer leur droit d'accès à l'information. leurs compétences et pouvoirs à l'égard de l'un ou l'autre des contrôleurs conjoints, pour autant que le contrôleur conjoint en question soit soumis à la compétence de cette autorité de contrôle.

[108] En outre, BestBags.com ayant intégré le pixel de suivi des médias sociaux sur son site web, elle est également responsable du respect des exigences de la directive "vie privée et communications électroniques" concernant cet outil, ce qui, étant donné que le pixel facilite également le traitement des données à caractère personnel, revêt également de l'importance lors de la détermination du niveau de responsabilité