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

Version 2.0

Adoptées le 13 avril 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 2.0	13/04/2021	Adoption des lignes directrices après consultation publique
Version 1.0	02/09/2020	Adoption des lignes directrices pour consultation publique

TABLE DES MATIÈRES

Le comité européen de la protection des données

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

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES:

1 INTRODUCTION

1. L'essor des médias sociaux représente une évolution importante de l'environnement en ligne au cours des dix dernières années. De plus en plus de personnes utilisent les médias sociaux pour rester en contact avec leur famille et leurs amis, pour se constituer un réseau professionnel ou pour créer des liens autour d'idées et d'intérêts communs. Aux fins des présentes lignes directrices, les médias sociaux sont considérés comme des plateformes en ligne qui permettent le développement de réseaux et de communautés d'utilisateurs, via lesquels des informations et des contenus sont partagés[1]. L'une des principales caractéristiques des médias sociaux consiste à permettre aux personnes de s'inscrire en vue de créer des «comptes» ou des «profils» personnels, d'interagir les uns avec les autres en partageant du contenu produit par les utilisateurs ou autre et de créer des liens 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 certains messages aux utilisateurs des médias sociaux afin de promouvoir

[1] Les fonctions supplémentaires offertes par les médias sociaux peuvent inclure, par exemple, la personnalisation, l'intégration d'applications, les modules sociaux, l'authentification des utilisateurs, l'analyse et les publications. Les fonctions liées aux médias sociaux peuvent constituer une offre autonome des responsables du traitement ou être intégrées dans une offre de services plus large.

[2] Outre les plateformes de médias sociaux «traditionnelles», il existe d'autres exemples de médias sociaux, à savoir: les plateformes de rencontre via lesquelles des utilisateurs inscrits se présentent pour trouver des partenaires avec lesquels ils peuvent se donner rendez-vous dans la vie réelle; des plateformes depuis lesquelles des utilisateurs enregistrés peuvent télécharger leurs propres vidéos, les commenter et les associer à d'autres vidéos; ou des jeux informatiques auxquels les utilisateurs inscrits peuvent jouer ensemble en groupe, échanger des informations ou partager dans le cadre du jeu leurs expériences et leurs réussites.

des intérêts commerciaux, politiques ou autres[3]. L'une des caractéristiques propres au ciblage est l'adéquation perçue entre la personne ou le groupe ciblé et le message délivré. L'hypothèse sous-jacente est que plus la correspondance 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 sont devenus de plus en plus sophistiqués au fil du temps. Les organisations peuvent désormais cibler des individus sur la base de toute une série de critères. Ces critères peuvent avoir été établis sur la base de données à caractère personnel que les utilisateurs ont activement communiquées ou partagées, telles que leur état civil. Toutefois, les critères de ciblage sont également de plus en plus établis sur la base de données à caractère personnel qui ont été observées ou déduites, soit par le fournisseur de médias sociaux, soit par des tiers, et collectées (agrégées) par la plateforme ou d'autres acteurs (p. ex. des courtiers en données) à l'appui des 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 l'intention des individus qui disposent de comptes sur les réseaux sociaux[4].

4. La combinaison et l'analyse de données émanant de différentes sources, ainsi que la nature potentiellement sensible des données à caractère personnel traitées dans le cadre des médias sociaux[5], créent des risques pour les libertés et les droits fondamentaux des individus. 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 individus concernés, le traitement sous-jacent des données à caractère personnel qui aboutit à l'envoi d'un message ciblé est souvent opaque. Il peut en outre supposer des utilisations non prévues ou non souhaitées de données à caractère personnel, ce qui soulève des questions non seulement en ce qui concerne la législation en matière de protection des données, mais aussi par rapport à d'autres libertés et droits fondamentaux. Récemment, le ciblage opéré par les médias sociaux a suscité un intérêt accru auprès du public et a fait l'objet d'un examen réglementaire dans le cadre du processus décisionnel et des processus électoraux démocratiques[6].

2 CHAMP D'APPLICATION

5. Le ciblage des utilisateurs de médias sociaux peut inclure toute une série d'acteurs différents qui, aux fins des présentes lignes directrices, seront subdivisés en quatre groupes: les fournisseurs de médias

[3] Le ciblage a été défini comme «l'action de diriger ou d'orienter quelque chose vers un groupe particulier de personnes» et «l'action de tenter d'attirer une personne ou un groupe ou de les influencer d'une manière ou d'une autre». https://www.collinsdictionary.com/dictionary/english/targeting.

[4] Les messages délivrés consistent généralement en des images et des éléments textuels, mais peuvent également contenir des supports vidéo et/ou audio.

[5] Les données à caractère personnel traitées dans le cadre des médias sociaux peuvent former des «catégories particulières de données à caractère personnel», en vertu de l'article 9 du RGPD, se rapporter à des individus vulnérables ou être par ailleurs de nature très personnelle. Voir également les lignes directrices du groupe de travail «Article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, p. 9.

[6] Voir, par exemple: https://edpb.europa.eu/sites/default/files/files/file1/201902_edpb_statementonelections_fr.pdf; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/; https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0638&from=FR; https://www.personuvernd.is/information-in-english/greinar/nr/2880.

sociaux, leurs utilisateurs, les cibleurs et les autres acteurs susceptibles de participer au processus de ciblage. L'importance d'établir correctement les rôles et responsabilités des différents acteurs a été récemment mise en évidence dans les arrêts rendus par la Cour de justice de l'Union européenne (CJUE) dans les affaires Wirtschaftsakademie et Fashion ID.[7] 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 du droit de l'Union en matière de protection des données.

6. Compte tenu de la jurisprudence de la CJUE, ainsi que des dispositions du RGPD relatives aux responsables conjoints du traitement et à la responsabilité, les présentes lignes directrices fournissent des orientations concernant le ciblage des utilisateurs de médias sociaux, notamment en ce qui concerne les responsabilités des cibleurs et des fournisseurs de médias sociaux. En cas de responsabilité conjointe, les lignes directrices viseront à clarifier la répartition des responsabilités entre les cibleurs et les fournisseurs de médias sociaux sur la base d'exemples pratiques[8].

7. Le principal objectif des présentes lignes directrices est donc de clarifier le rôle et les responsabilités du fournisseur de médias sociaux et du cibleur. Pour ce faire, les lignes directrices recensent également les risques potentiels pour les libertés et droits des individus (section 3), les principaux acteurs et leurs rôles (section 4) et abordent l'application des principales exigences en matière de protection des données (telles que la licéité et la transparence, l'analyse d'impact relative à la protection des données, etc.) ainsi que les éléments clés des accords entre les fournisseurs de médias sociaux et les cibleurs.

8. Le champ d'application des présentes lignes directrices couvre néanmoins les liens entre les utilisateurs enregistrés sur un réseau social, ses fournisseurs, ainsi que les cibleurs. L'analyse approfondie de scénarios, tels que des situations dans lesquelles les individus ne sont pas enregistrés auprès des fournisseurs de médias sociaux, ne relève pas du champ d'application des présentes lignes directrices.

3 RISQUES POUR LES DROITS ET LES LIBERTÉS DES UTILISATEURS RÉSULTANT DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

9. Le RGPD souligne l'importance d'évaluer et d'atténuer correctement tout risque qui pèse sur les droits et libertés des personnes résultant du traitement des données à caractère personnel[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 visent pas à fournir une liste exhaustive des risques potentiels pour les droits et libertés des personnes. Néanmoins, le CEPD estime qu'il est important de mettre l'accent sur

[7] CJUE, arrêt du 5 juin 2018 dans l'affaire Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388; CJUE, arrêt du 29 juillet 2019 dans l'affaire Fashion ID, C-40/17, ECLI:EU:C:2019:629.

[8] Les présentes lignes directrices sont sans préjudice des lignes directrices 07/2020 du CEPD sur les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 2 septembre 2020, concernant la répartition des responsabilités dans d'autres contextes.

[9] Selon l'article 24 du RGPD, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD, «compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques». Voir également les lignes directrices du groupe de travail «Article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP248 rév. 01 du 4 octobre 2017.

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 comprendre des utilisations de données à caractère personnel qui vont à l'encontre ou au-delà des attentes raisonnables des individus et enfreignent 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 objectif initial et d'une manière que l'individu ne pouvait raisonnablement pas anticiper. Les activités de profilage liées au ciblage peuvent permettre de déduire des intérêts ou d'autres caractéristiques que l'individu n'a pas activement révélés, ce qui compromet la capacité de l'individu à exercer un contrôle sur ses données à caractère personnel[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 des personnes concernées.

11. Un deuxième type de risque concerne la possibilité de discrimination et d'exclusion. Le ciblage des utilisateurs de médias sociaux peut inclure des critères qui, directement ou indirectement, ont des effets discriminatoires liés à la race ou l'origine ethnique, à l'état de santé ou à l'orientation sexuelle d'une personne, voire 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 perspectives pour les personnes appartenant à certains groupes d'individus. Le potentiel de discrimination dans le ciblage découle de la capacité des annonceurs à exploiter la quantité et la variété considérables de données à caractère personnel (p. ex. les données démographiques, comportementales et les intérêts) que les plateformes de médias sociaux recueillent sur leurs utilisateurs[11]. De récentes recherches suggèrent que le potentiel d'effets discriminatoires existe également sans le recours à des critères directement liés à des catégories spéciales de données personnelles au sens de l'article 9 du RGPD[12].

12. Une deuxième catégorie de risques concerne la manipulation éventuelle des utilisateurs. Les mécanismes de ciblage sont, par définition, utilisés afin d'influencer le comportement et les choix des individus, qu'il s'agisse de leurs décisions d'achat en tant que consommateurs ou 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 individuelles (p. ex. 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 (p. ex. par l'analyse de l'utilisation de certains mots-clés). Ces informations pourraient être utilisées pour cibler l'individu avec des messages

[10] Voir également l'avis du contrôleur européen de la protection des données, de la CEPD, sur la manipulation en ligne, avis 3/2018, 19 mars 2018, p. 15 («*La préoccupation liée à l'utilisation des données des 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 en matière d'information d'une personne, de réduire encore le contrôle des personnes concernées sur leurs données, et d'affecter ainsi la confiance envers les environnements et services numériques.*»).

[11] T. Speicher et al., 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.press/v81/speicher18a.html.

[12] Idem.

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

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 visant à cibler les utilisateurs des médias sociaux peuvent également être utilisés pour influencer indûment les individus lorsqu'il s'agit du discours politique et des processus électoraux démocratiques[15]. Alors que les campagnes politiques «traditionnelles» hors ligne visent à influencer le comportement des électeurs au moyen de messages qui sont 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 personnalisés sur mesure, spécifiques aux besoins, intérêts et valeurs particuliers du public cible[16]. Ce ciblage peut même porter sur la désinformation ou des messages que les individus peuvent trouver particulièrement troublants, et qui sont donc (davantage) susceptibles de stimuler une certaine émotion ou réaction de leur part. Lorsque des messages polarisants ou mensongers (désinformation) sont destinés à des personnes spécifiques, avec peu ou sans contextualisation ou exposition à d'autres points de vue, l'utilisation de mécanismes de ciblage peut avoir pour effet de compromettre 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 nuire à la probabilité d'accéder à des sources d'information diversifiées sur un sujet particulier. Cela peut en retour avoir des conséquences négatives sur le pluralisme au sein du débat public ainsi que sur l'accès à l'information[18]. Les mécanismes de ciblage peuvent être utilisés pour augmenter la visibilité de certains messages, tout en donnant moins d'importance à d'autres. L'impact négatif qui peut en découler peut être ressenti à deux niveaux. D'une part, il existe des risques liés à ce que l'on appelle les «bulles de filtrage» au sein desquelles les gens sont toujours exposés au «même type d'informations» et confrontés à moins d'opinions, d'où une polarisation politique et idéologique accrue[19]. D'autre part, les mécanismes de ciblage peuvent également créer des risques de «saturation de l'information», les individus ne pouvant pas prendre une décision éclairée parce qu'ils disposent de trop d'informations sans pour autant pouvoir évaluer leur fiabilité.

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

---

[14] Voir Adam D. I. Kramer, Jamie E. Guillory et Jeffrey T. Hancock, «Experimental evidence of massive-scale emotional contagion through social networks», PNAS 17 juin 2014 111 (24) 8788-8790; publié pour la première fois le 2 juin 2014 https://doi.org/10.1073/pnas.1320040111, disponible à l'adresse suivante: 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 la déclaration 2/2019 du comité européen de la protection des données sur l'utilisation des données à caractère personnel dans le cadre de campagnes politiques, 13 mars 2019, p. 1.

[16] Bureau du commissionnaire à l'information (ICO), *Democracy disrupted? Personal information and political influence*, 10 juillet 2018, p. 14.

[17] Voir également, Commission européenne, les Orientations de la Commission relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral, La contribution de la Commission européenne à la réunion des chefs d'État et de gouvernement à Salzbourg les 19 et 20 septembre 2018. Voir aussi L.M. Neudert et N.M. Marchal, *Polarisation and the use of technology in political campaigns and communication*, service de recherche du Parlement européen, 2019, p. 22 à 24.

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

[19] Contrôleur européen de la protection des données, avis 3/2018, p. 7.

sur la liberté d'expression, y compris l'accès à l'information[20]. Ces effets peuvent être exacerbés si le ciblage est également basé sur l'analyse du contenu partagé par les utilisateurs des médias sociaux. Si les messages privés, les publications et les commentaires sont soumis à une analyse en vue d'une utilisation commerciale ou politique, cela peut également donner lieu à une autocensure.

16. Le potentiel impact négatif du ciblage peut être considérablement plus important lorsque des catégories d'individus vulnérables sont concernées, comme les enfants. Le ciblage peut influencer la formulation des préférences et des intérêts personnels des enfants, ce qui affecte en fin de compte leur autonomie et leur droit au développement. Le considérant 38 du RGPD indique qu'une protection spécifique devrait s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant[21].

17. L'utilisation des médias sociaux dans l'UE est répandue puisque 54 % des 16-74 ans étaient actifs sur les réseaux sociaux en 2019. D'ailleurs, ce taux de fréquentation 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 est également susceptible d'accroître les risques pour les droits et libertés d'un nombre important d'individus. Par exemple, certains fournisseurs de médias sociaux peuvent être en mesure de combiner, seuls ou en lien avec d'autres entreprises, une quantité et une diversité plus importantes de données à caractère personnel. Cette capacité, à son tour, peut accroître 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 commerçants en ligne). Le degré de pouvoir du marché et de l'information, à son tour, comme l'a reconnu le CEPD, «*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 de survenue 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 des titres divers 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 des opportunités d'emploi). Le terme «utilisateur» est généralement utilisé pour désigner les personnes qui sont enregistrées auprès du service (c'est-à-dire celles qui ont un «compte» ou un

[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 leur propriété (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 à 21.
[21] Voir également les lignes directrices du groupe de travail «Article 29» sur la protection des données, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251rev.01, p. 29.
[22] https://ec.europa.eu/eurostat/fr/web/products-eurostat-news/-/edn-20200630-2.
[23] Déclaration du comité européen de la protection des données sur les conséquences de la concentration économique sur la protection des données, disponible à l'adresse suivante: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_fr.pdf

«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 les mêmes fonctions ou services que ceux offerts aux individus qui se sont inscrits auprès du fournisseur de médias sociaux. Les individus qui sont enregistrés auprès des fournisseurs de médias sociaux et ceux qui ne le sont pas peuvent être considérés comme des «personnes concernées» au sens de l'article 4, paragraphe 1, du RGPD dans la mesure où la personne est directement ou indirectement identifiée ou identifiable[25].

20. Le fait que les personnes soient censées s'inscrire sous leur vrai nom ou utiliser un surnom ou un pseudonyme peut varier selon le service de médias sociaux en question. Toutefois, il sera en règle générale toujours possible de cibler (ou d'isoler) l'utilisateur en question même en l'absence d'une politique de nom réel, car la plupart des types de ciblage ne reposent pas sur les noms d'utilisateur mais sur d'autres types de données à caractère personnel 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 de «la vie réelle», telles que des numéros de téléphone[26]. Enfin, il convient de noter que les fournisseurs de médias sociaux peuvent également permettre le ciblage d'individus qui ne possèdent pas de compte auprès du fournisseur de médias sociaux[27].

4.2 Fournisseurs de médias sociaux

21. Les fournisseurs de médias sociaux offrent un service en ligne qui permet le développement de réseaux et de communautés d'utilisateurs, entre lesquels des informations et des contenus sont partagés. Les services de médias sociaux sont généralement proposés via des navigateurs web ou des applications dédiées, souvent après avoir demandé à l'utilisateur de fournir un ensemble de données à caractère personnel pour constituer son «compte» ou son «profil». Ils proposent aussi souvent aux utilisateurs des «contrôles» associés à leur compte pour leur permettre d'accéder aux données à caractère personnel traitées dans le cadre de l'utilisation de leur compte et de pouvoir exercer un contrôle sur ces dernières.

22. Le fournisseur de médias sociaux détermine les fonctionnalités du service. Il s'agit alors de déterminer quelles données sont traitées, à quelle fin, sous quelles conditions, ainsi que les modalités de traitement des données à caractère personnel. 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 conjointement à cette dernière.

[24] Les données à caractère personnel et les informations de profilage conservées par les fournisseurs de médias sociaux concernant les individus qui ne sont pas enregistrés auprès de ces derniers sont parfois appelées «profils fantômes».

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

[26] Dans certains cas, les fournisseurs de médias sociaux demandent la production de documents supplémentaires pour vérifier les données fournies, par exemple en demandant aux utilisateurs de télécharger leurs cartes d'identité ou des documents similaires.

[27] Ce ciblage peut être rendu possible sur la base d'identifiants en ligne fournis par leurs appareils, applications, outils et protocoles, tels que des adresses de protocole Internet, des témoins de connexion («cookies») ou d'autres identifiants. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes. Voir également le considérant 30 du RGPD. Sur la base de cette reconnaissance, des publicités ciblées peuvent être affichées sur un site Internet que la personne visite.

23. Le fournisseur de médias sociaux a la possibilité de recueillir de grandes quantités de données à caractère personnel relativement au comportement et aux interactions des utilisateurs et des individus qui ne sont pas enregistrés 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 «aperçus» basés sur l'activité de l'utilisateur supposent souvent des données à caractère personnel déduites ou dérivées. Par exemple, lorsqu'un utilisateur interagit avec un certain contenu (p. ex. en «aimant» une publication 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 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 à caractère personnel que les individus communiquent activement au fournisseur de médias sociaux (p. ex. un nom d'utilisateur, une adresse électronique, un lieu 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 «cibleur» 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[28]. Ce qui distingue les «cibleurs» des autres utilisateurs des médias sociaux est le fait 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 «microciblage»[29]. Les cibleurs peuvent se livrer au ciblage aux fins de 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 leur 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 elles aussi les médias sociaux pour cibler leurs messages en direction de contributeurs potentiels ou pour développer des communautés.

26. Il est important de noter que les utilisateurs des médias sociaux peuvent être ciblés de différentes manières. Par exemple, le ciblage peut se faire non seulement à travers l'affichage d'une publicité personnalisée (par exemple, par une «bannière» affichée en haut ou sur le côté d'une page Internet), mais aussi, dans la mesure où cela se produit au sein de la plateforme de médias sociaux, par l'affichage dans le «feed» [flux], la «timeline» [fil d'actualité] ou la «story» [actualité à la une] d'un utilisateur, où le contenu publicitaire apparaît aux côtés du contenu généré par l'utilisateur. Le ciblage peut également porter sur la création de contenu hébergé par le fournisseur de médias sociaux (par exemple, par une «page» dédiée ou une autre forme de présence sur les médias sociaux) ou ailleurs (c'est-à-dire sur des sites Internet tiers). Les cibleurs peuvent disposer de leurs propres sites Internet et applications, sur lesquels ils ont la possibilité d'intégrer des outils ou des fonctionnalités

[28] Le traitement de données à caractère personnel effectué par une personne physique dans le cadre d'une activité purement personnelle ou domestique ne relève pas du champ d'application matériel du RGPD [article 2, paragraphe 2, point c)].

[29] Aux fins des présentes lignes directrices, le simple fait de partager sur une page de média social des informations destinées au grand public (p. ex. des informations sur les horaires d'ouverture) sans sélection préalable du public visé ne serait pas considéré comme un «ciblage».

commerciales spécifiques aux médias sociaux, tels que des modules ou des logins sociaux, ou en utilisant les interfaces de programmation d'applications (API) ou les kits de développement logiciel (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 de marketing, les réseaux d'annonces, les bourses d'annonces, les plateformes axées sur la demande et sur l'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 (que l'on appelle parfois «adtech») qui collecte et traite les données relatives aux individus (y compris les utilisateurs de médias sociaux) en suivant, par exemple, leurs activités sur les sites Internet 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 fournisseurs de gestion de données se distinguent des autres sociétés *adtech* dans la mesure où ils traitent non seulement les données collectées au moyen de technologies de traçage, mais aussi celles collectées à partir d'autres sources, qui peuvent inclure des sources en ligne et hors ligne. En d'autres termes, les courtiers en données et les fournisseurs de gestion de données regroupent des données collectées auprès d'une grande variété de sources, qu'ils peuvent ensuite vendre à d'autres acteurs associés au processus de ciblage[31].

29. S'il est vrai que 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 participant à 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 de médias sociaux et des cibleurs, il est important de tenir compte de la jurisprudence pertinente de la CJUE. Les arrêts rendus dans les affaires Wirtschaftsakademie (C-210/16), Jehovan todistajat (C-25/17) et Fashion ID (C-40/17) sont particulièrement pertinents en l'espèce.

31. Le point de départ de l'analyse est la définition juridique du responsable du traitement. Au sens de l'article 4, paragraphe 7, du RGPD, on entend par «*responsable du traitement», «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'arrêtWirtschaftsakademie, la CJUE a décidé que l'administrateur d'une page appelée «page fan» sur Facebook doit être considéré comme participant à la détermination des finalités et des moyens du traitement des données à caractère personnel. Il ressort des indications soumises à la CJUE que la création d'une page fan implique de la part de son administrateur une *action de paramétrage*, qui

[30] Pour la description des différents acteurs, voir avis 2/2010 du GT29 sur la publicité comportementale, en page 5. L'avis est disponible à l'adresse suivante: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[31] Voir Centre de recherche sur le consommateur (de l'anglais *Consumer Policy Research Centre*), «*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/

influe sur le traitement de données à caractère personnel aux fins de *l'établissement des statistiques* établies à partir des visites de la page fan[32]. À l'aide des filtres fournis par Facebook, l'administrateur peut définir les critères à partir desquels ces statistiques doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données à caractère personnel par Facebook:

> «*En particulier, l'administrateur de la page fan peut demander à obtenir – et donc que soient traitées – des données démographiques concernant son audience cible, notamment des tendances en matière d'âge, de sexe, de situation amoureuse et de profession, des informations sur le style de vie et les centres d'intérêt de son audience cible ainsi que des informations concernant les achats et le comportement d'achat en ligne des visiteurs de sa page, les catégories de produits ou de services qui l'intéressent le plus, de même que des données géographiques qui permettent à l'administrateur de la page fan de savoir où effectuer des promotions spéciales ou organiser des événements et, de manière plus générale, de cibler au mieux son offre d'informations.*»

33. Comme la définition de l'action de paramétrage dépend notamment de l'audience cible de l'administrateur «ainsi que d'objectifs de gestion ou 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 qualifié de responsable du traitement de données à caractère personnel des visiteurs de sa «page», conjointement avec le fournisseur de médias sociaux.

34. Comme indiqué davantage à la section 9 des présentes lignes directrices, les responsables du traitement peuvent être associés à différentes étapes du traitement des données à caractère personnel et à différents degrés. Dans ces conditions, le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce:

> «*[L]'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement des données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce*.»[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 en l'occurrence que Facebook doit être considéré comme déterminant, *à titre principal*, les finalités et les moyens du traitement des données à caractère personnel des utilisateurs de Facebook ainsi que des personnes ayant visité les pages fan hébergées sur Facebook[35].

36. Dans l'arrêt Fashion ID, la CJUE la CJUE a décidé que le gestionnaire d'un site Internet peut être considéré comme un responsable du traitement lorsqu'il insère un module social Facebook sur son site Internet qui amène le navigateur d'un visiteur à transmettre des données à caractère personnel de ce dernier à Facebook[36]. La qualification du gestionnaire d'un site Internet en tant que responsable du traitement est cependant limitée à l'opération ou à l'ensemble des opérations dont il détermine effectivement les finalités et les moyens. Dans ce cas particulier, la CJUE a considéré que le

[32] Arrêt dans l'affaire Wirtschaftsakademie, C-210/16, point 36.
[33] Arrêt dans l'affaire Wirtschaftsakademie, C-210/16, point 39.
[34] Arrêt dans l'affaire Wirtschaftsakademie, C-210/16, point 43; Arrêt dans l'affaire Jehovan todistajat, C-25/17, point 66 et arrêt dans l'affaire 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.

gestionnaire d'un site Internet est uniquement capable de déterminer, conjointement avec Facebook, 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 arrêté que, en ce qui concerne l'insertion d'un module social sur un site Internet, la responsabilité du gestionnaire d'un site internet est:

> «*limitée à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens, à savoir la collecte et la communication par transmission des données en cause.*»[37]

37. La CJUE a considéré que le gestionnaire d'un site Internet n'était pas un responsable du traitement pour les opérations de traitement de données à caractère personnel ultérieures[38] effectuées par Facebook après leur transmission à cette dernière, car le gestionnaire d'un site Internet n'était pas en mesure de déterminer les finalités et les moyens de ces opérations du fait de l'insertion du module social:

> «*En revanche, au regard desdites informations, il apparaît, de prime abord, exclu que Fashion ID détermine les finalités et les moyens des opérations de traitement de données à caractère personnel ultérieures, effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne saurait être considérée comme étant responsable de ces opérations[...]*.»[39]

38. En cas de contrôle conjoint, conformément à l'article 26, paragraphe 1 du RGPD, 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 RGPD, 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 RGPD.

39. Les sections suivantes clarifient, 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 relatives à la protection des données et les traitements portant sur des catégories particulières de données sont analysées. Enfin, les lignes directrices traitent de l'obligation pour les responsables conjoints du traitement de mettre en place un dispositif approprié conformément à l'article 26 du RGPD, en tenant compte du degré de responsabilité du cibleur et du fournisseur de médias sociaux.

---

[37] Arrêt dans l'affaire Fashion ID, C-40/17, point 107.

[38] Le traitement ultérieur correspond à toute opération de traitement ou ensemble d'opérations de traitement qui suit (c'est-à-dire qui a lieu après) la collecte de données. Chez Fashion ID, le terme est utilisé pour désigner les opérations de traitement effectuées par Facebook après leur transmission et pour lesquelles 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 pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées n'est autorisé que dans la mesure où l'article 6, paragraphe 4 du RGPD 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 consistera 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 RGPD, car il s'agirait dès lors d'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.

5 ANALYSE DES DIFFÉRENTS MÉCANISMES DE CIBLAGE

5.1 Vue d'ensemble

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 personnes 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 pourrait utiliser les informations fournies par la personne concernée au cibleur afin de cibler cette personne de manière spécifique, par exemple au moyen de données client (telles qu'une liste d'adresses électroniques), à mettre en correspondance avec les données déjà détenues sur la plateforme de médias sociaux, conduisant à ce que tous les utilisateurs qui correspondent soient ciblés par la publicité[41].

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 grâce à l'utilisation du service ou du dispositif[43]. Par exemple, un utilisateur particulier de médias sociaux 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, coordonnées GPS, 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 logiciel (SDK) proposés par les fournisseurs de médias sociaux;
- les données collectées par l'intermédiaire de sites Internet de tiers qui ont incorporé des modules sociaux ou des pixels;

[40] Lignes directrices du groupe de travail «Article 29» sur la protection des données, 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 du Land de Bavière (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 grandes méthodes de constitution de profils d'utilisateurs: i) les profils prédictifs sont établis par déduction en observant le comportement individuel et collectif des utilisateurs dans le temps, notamment en suivant les pages visitées et les publicités qu'ils ont vues ou sur lesquelles ils ont cliqué. ii) Les profils explicites sont établis à partir des données à caractère personnel que les personnes concernées fournissent elles-mêmes à un service Internet, notamment par leur inscription*» (Groupe de travail «Article 29» sur la protection des données, avis 2/2010 sur la publicité comportementale en ligne, WP 171, p. 7).
[43] Lignes directrices du groupe de travail «Article 29» sur la protection des données, sur le droit à la portabilité des données, WP 242 rev.01, 5 avril 2017, p. 10.

- 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 l'intermédiaire 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 peut 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 Internet et/ou de ses connexions au réseau.

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 communiquer activement un grand nombre d'informations les concernant lorsqu'ils utilisent les médias sociaux. La création d'un compte de média social (ou «profil») entraîne la communication 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 à caractère personnel fournies par les utilisateurs des médias sociaux peuvent être utilisées par le fournisseur de médias sociaux pour élaborer des critères permettant au cibleur d'adresser des messages spécifiques aux utilisateurs des médias sociaux.

Exemple1:

L'entreprise X vend des chaussures pour hommes et souhaite promouvoir la 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 établir le public cible auquel sa publicité doit s'adresser. En outre, le cibleur indique que la publicité doit être affichée à l'intention des utilisateurs des médias sociaux pendant qu'ils utilisent le service de médias sociaux entre 17 heures et 20 heures. Pour permettre le ciblage des utilisateurs de 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 à l'intention du cibleur (p. ex., 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 à l'intention du public cible.

[44] *Idem.*

43. En ce qui concerne la détermination de la *finalité*, l'entreprise X et le fournisseur de médias sociaux déterminent conjointement la finalité du traitement, qui consiste à afficher une publicité spécifique à l'intention d'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 lui 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 montrant 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 aboutit au ciblage. Le cibleur participe à la détermination des moyens en choisissant d'utiliser les services offerts par le fournisseur de médias sociaux[46], et en lui demandant de cibler un public en fonction 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 pour lesquelles les données à caractère personnel seront utilisées. Le fournisseur de médias sociaux, quant à lui, a décidé de traiter les données à caractère personnel 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 à traiter, les critères de ciblage à proposer et les personnes qui auront accès aux données à caractère personnel (et les types de données) traitées dans le cadre d'une campagne de ciblage particulière[49].

45. Dans un souci d'exhaustivité, le CEPD note que le fournisseur de médias sociaux ne peut être considéré comme un sous-traitant au sens de l'article 4, paragraphe 8, du RGPD. [50] Dans l'exemple 1, les critères de ciblage, tels qu'élaborés par le fournisseur de médias sociaux sur la base des données à caractère personnel de l'utilisateur, 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 qualifié de sous-traitant. En outre, le fournisseur de médias sociaux ne semble pas traiter les données exclusivement pour le compte de l'entreprise X et conformément à ses instructions.

---

[45] Voir les lignes directrices 7/2020 du CEPD sur les concepts de responsable du traitement et de sous-traitant au titre du RGPD, («*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'il existe un bénéfice mutuel découlant de la même opération de traitement, à condition que chacune des entités concernées participe à la détermination des finalités et des moyens de l'opération de traitement en question*»).

[46] Voir les lignes directrices 7/2020 du CEPD sur les concepts de responsable du traitement et de sous-traitant au titre du RGPD, («*En outre, le choix fait par une entité d'utiliser à ses propres fins un outil ou autre système développé par une autre entité, permettant 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 Internet la fonction «J'aime» mise à la disposition des exploitants de sites Internet 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 Internet à Facebook et a donc déterminé conjointement avec Facebook les moyens de ce traitement*»).

[47] Voir, à cet égard, l'arrêt Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, point 39.

[48] Voir dans le même registre également l'arrêt Fashion ID, C-40/17, point 80: «*ces opérations de traitement étant effectuées dans l'intérêt économique tant de Fashion ID que de Facebook Ireland, pour qui le fait de pouvoir disposer de ces données à ses propres fins commerciales constitue la contrepartie de l'avantage offert à Fashion ID*».

[49] Voir également l'avis 1/2010.

[50] Voir les lignes directrices 7/2020 du CEPD sur les concepts de responsable du traitement et de sous-traitant au titre du RGPD.

46. Le contrôle conjoint entre le cibleur et le fournisseur de médias sociaux ne s'étend qu'aux opérations de traitement 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 effectué 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 de la communication (p. ex. 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 n'a pas participé à la détermination des finalités et des moyens, de même que le fournisseur de médias sociaux, en principe, ne participe pas 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 se contente de spécifier les paramètres de son public cible et n'a pas accès aux données à caractère personnel des utilisateurs concernés. En effet, la responsabilité conjointe de plusieurs acteurs pour un même traitement ne présuppose pas que chacun d'eux ait accès aux données à caractère personnel concernées[52]. Le CEPD rappelle que l'accès effectif aux données à caractère personnel 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 juridique (article 6 du RGPD) pour justifier le traitement des données à caractère personnel dont chacun des responsables conjoints du traitement est chargé. Le CEPD rappelle qu'aucune hiérarchie spécifique n'est établie entre les différentes bases légales du RGPD: le responsable du traitement doit s'assurer que la base juridique retenue correspond à l'objectif et au contexte de l'opération de traitement en question. La détermination de la base juridique appropriée est liée aux principes de loyauté et de limitation de la finalité[54].

49. D'une manière générale, deux bases juridiques peuvent 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 RGPD] ou les intérêts légitimes [article 6, paragraphe 1, point f), du RGPD]. 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, paragraphe 1, point b), du RGPD ne peut 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

[51] Voir également l'arrêt dans l'affaire Fashion ID, C-40/17, point 74 («*[une] personne physique ou morale ne saurait être considérée comme étant responsable, au sens de ladite disposition, des opérations antérieures ou postérieures de la chaîne de traitement dont elle ne détermine ni les finalités ni les moyens.*») et point 101.
[52] Arrêt dans l'affaire Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, point 38; arrêt dans l'affaire Jehovan todistajat, C-25/17, ECLI:EU:C:2018:551, point 69.
[53] Arrêt de la CJUE du 10 juillet 2018 (C-25/17, points 68 à 72).
[54] Voir le paragraphe 18 des lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD 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/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf
[55] Voir les paragraphes 52 et 53 des lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, 8 octobre 2019, disponible à l'adresse suivante:

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 ligne[57], l'article 6, paragraphe 1, point b), du RGPD dans le contexte du ciblage des utilisateurs de médias sociaux est difficilement applicable, comme l'illustrent les exemples des présentes lignes directrices[58].

50. En ce qui concerne la base légale de l'intérêt légitime, le CEPD rappelle que dans l'arrêt Fashion ID, la CJUE a rappelé que pour qu'un traitement puisse se fonder sur l'intérêt légitime, trois conditions cumulatives doivent être remplies, à savoir[59]: 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 du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi, et iii) la condition que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas. La CJUE a également précisé que dans une situation de contrôle conjoint, «*il est nécessaire que chacun de ces responsables poursuive, avec ces opérations de traitement, un intérêt légitime [...], afin que celles-ci soient justifiées dans son chef*»[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 RGPD 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 RGPD.

52. Sur la base de la deuxième partie du critère de mise en balance des intérêts légitimes, les responsables conjoints du traitement devront donc 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 donne pas lieu 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 atteindre le même objectif[61].

---

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf

[56] Il y aurait une absence de nécessité si le cibleur passait aux fournisseurs de médias sociaux malgré une relation contractuelle directe avec son client et donc la possibilité d'une publicité directe.

[57] Voir le paragraphe 15 des lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD 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/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf

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

[59] CJUE, arrêt dans l'affaire Fashion ID, 29 juillet 2019, C-40/17, paragraphe 95 - ECLI:EU:C:2019:629.

[60] Idem, paragraphe 97.

[61] Avis 06/2014 du groupe de travail «Article 29» sur la notion d'intérêt légitime du responsable du traitement des données en vertu de l'article 7 de la directive 95/46/CE, WP217, 9 avril 2014, p. 29.

53. La troisième étape pour évaluer si le cibleur et le fournisseur de médias sociaux peuvent se fonder sur l'article 6, paragraphe 1, point f), du RGPD comme base juridique pour le traitement des données à caractère personnel, est la mise en balance des intérêts légitimes nécessaire pour déterminer si l'intérêt légitime en jeu l'emporte sur les intérêts ou les droits et les libertés fondamentaux de la personne concernée[62].

54. Le CEPD rappelle que dans les cas où un responsable du traitement envisage d'invoquer l'intérêt légitime, les obligations de transparence et le droit de s'opposer doivent être examinés attentivement. Les personnes concernées doivent avoir la possibilité de s'opposer au traitement de leurs données à des fins ciblées avant que le traitement ne soit lancé. Les utilisateurs des 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 disposer de contrôles garantissant que le traitement sous-jacent de leurs données à caractère personnel à des fins de ciblage n'a plus lieu après leur opposition.

55. Le cibleur qui cherche à se prévaloir de l'intérêt légitime doit, 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 doit au moins veiller à ce que la plateforme de médias sociaux fournisse à la personne concernée les moyens d'exprimer efficacement son droit de s'opposer préalable. En tant que responsables conjoints du traitement, le cibleur et le fournisseur de médias sociaux doivent préciser comment le droit de s'opposer des personnes (ainsi que d'autres droits) sera pris en compte dans le cadre de l'accord conjoint (voir section 6). Si la 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 RGPD]. Par exemple, le GT29 a précédemment considéré qu'il serait difficile pour les responsables du traitement de justifier le recours à des 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 d'individus sur plusieurs sites Internet, emplacements, dispositifs, services ou courtage de données[63].

[62] Lors de l'évaluation de l'impact sur les intérêts, les droits et les libertés fondamentaux de la personne concernée, les considérations suivantes sont particulièrement pertinentes dans le contexte du ciblage dirigé vers les utilisateurs des médias sociaux: i) les objectifs du ciblage, ii) le niveau de détail des critères de ciblage utilisés (p. 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 détaillé), 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'avis 06/2014 du groupe de travail «Article 29» sur la notion d'intérêt légitime du responsable du traitement des données en vertu de l'article 7 de la directive 95/46/CE, WP 217, 9 avril 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[63] Avis du groupe de travail «Article 29» sur le profilage et la prise de décision automatisée, WP 251, rév. 01, p. 15, voir également l'avis du WP «Article 29» 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».

57. Pour être valable, le consentement recueilli pour le traitement doit remplir les conditions énoncées à l'article 4, paragraphe 11, et à l'article 7 du RGPD. 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 présenté comme une partie non négociable des conditions générales, l'on considère qu'il n'a pas 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].

58. Le consentement (Article 6, paragraphe 1, point a), du RGPD) pourrait être envisagé, à condition que toutes les conditions d'un consentement valide soient remplies. Le CEPD rappelle que l'obtention d'un consentement n'annule pas ou ne diminue pas de quelque façon que ce soit l'obligation imposée au responsable du traitement de respecter les principes relatifs au traitement énoncés dans le RGPD, notamment en son article 5 concernant la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données. Même si le traitement des données à caractère personnel 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 porter sur 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 des utilisateurs qu'il possède déjà et tous les utilisateurs qui correspondent sont ajoutés ou exclus du public cible (c'est-à-dire le «groupe» de personnes auquel la publicité sera diffusée sur la plateforme de médias sociaux). 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.

Exemple2:

M[me] 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. À la suite de ce rendez-vous, M[me] Jones décide de ne pas devenir cliente de la banque. La banque a néanmoins ajouté l'adresse électronique de M[me] Jones à sa base de données de courriers électroniques des clients. Ensuite, la banque utilise sa base de données d'adresses électroniques, en permettant au fournisseur de médias sociaux de «faire correspondre» la liste d'adresses électroniques

[64] Voir lignes directrices du groupe de travail «Article 29» sur le consentement au sens du règlement 2016/679, WP259, rév. 01.
[65] Voir lignes directrices du groupe de travail «Article 29» sur le consentement au sens du règlement 2016/679, WP 259 rév. 01, p. 3 et 4.
[66] Voir les lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD 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/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf

qu'elle détient avec celles de la plateforme de médias sociaux, afin de cibler les personnes concernées avec la gamme complète de services financiers sur la plateforme de médias sociaux.

Exemple3:

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 électronique serait utilisée pour la publicité d'offres liées aux services bancaires qu'il utilise déjà; et b) il peut s'opposer à tout moment à ce traitement. La banque a ajouté son adresse électronique à sa base de données de d'adresse électronique des clients. Ensuite, la banque utilise sa base de données de courriers électroniques pour cibler ses clients sur la plateforme de médias sociaux avec la gamme complète 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, quant à lui, 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 de 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 l'intention d'un public d'individus 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 toute communication relative à la campagne de ciblage[68].

63. Dans les deux exemples, la banque agit en tant que responsable du traitement unique en ce qui concerne la collecte initiale des adresses électroniques de M[me] 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 par la transmission des données à caractère personnel et leur collecte simultanée par le fournisseur de médias sociaux. Elle 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

[67] Dans les situations où les adresses électroniques sont utilisées à des fins de prospection directe 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 définissant les critères de ciblage supplémentaires, le cibleur définit les critères selon lesquels le ciblage a lieu et désigne les catégories de personnes pour lesquelles les données à caractère personnel seront utilisées. Le fournisseur de médias sociaux détermine également à qui appartiennent les données à caractère personnel qui seront traitées, en autorisant les catégories de données qui seront traitées, les critères de ciblage qui seront proposés et les personnes qui auront accès aux données à caractère personnel (et les types de données) traitées dans le cadre d'une campagne de ciblage particulière. La finalité partagée qui sous-tend ces opérations de traitement ressemble à la finalité établie dans l'exemple 1, à savoir l'affichage d'une publicité spécifique à l'intention d'un ensemble d'individus (dans ce cas: les utilisateurs de médias sociaux) qui constituent le public cible.

phase de communication ultérieure. Dans certains cas, le contrôle conjoint peut être prolongé, même jusqu'à la phase de suppression des données, dans la mesure où le destinataire continue à participer à la détermination des finalités et des moyens.

64. La raison pour laquelle la banque agit en tant que responsable du traitement unique lors de la collecte des adresses électroniques de M[me] 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 faite la distinction entre l'ensemble initial d'opérations de traitement pour lesquels seule la banque est responsable de traitement et un traitement ultérieur pour lequel un contrôle conjoint existe. La responsabilité de la banque ne s'étend pas aux opérations survenant après la fin du ciblage et de la communication 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 contrôleur.

B. Base juridique

65. Dans l'exemple 2, l'article 6, paragraphe 1, point f), du RGPD 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, M[me] Jones a contacté la banque dans le seul but de fixer un rendez-vous, à la suite duquel elle a fait part de son intention de ne pas utiliser les services offerts par la banque. Par conséquent, on peut considérer que M[me] Jones ne s'attend raisonnablement pas à ce que ses données à caractère personnel soient utilisées à des fins de ciblage («reciblage»). En outre, un test de compatibilité au titre de l'article 6, paragraphe 4, du RGPD aboutirait probablement à la conclusion que ce traitement n'est pas compatible avec la finalité pour laquelle les données à caractère personnel 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 était: 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 à caractère personnel ont été collectées par la banque. Toutefois, le CEPD souhaite préciser que le respect des obligations d'information conformément aux articles 13 et 14 du RGPD et la pesée des intérêts à réaliser conformément à l'article 6, paragraphe 1, point f), du RGPD sont deux ensembles d'obligations différents. Par conséquent, le simple respect des obligations d'information conformément aux articles 13 et 14 du RGPD 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 RGPD.

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 l'intermédiaire du service de médias sociaux lui-même ou peut également être possible sur des sites Internet externes en vertu de modules sociaux ou de pixels.

Exemple4: Ciblage par pixel

M. Schmidt navigue en ligne afin d'acheter un sac à dos. Il visite le site Internet «BestBags.com», regarde un certain nombre d'articles, mais décide de ne pas faire d'achat. Le gestionnaire de «BestBags.com» souhaite cibler les utilisateurs de médias sociaux qui ont visité son site Internet sans

effectuer d'achat. À cette fin, il intègre sur son site Internet un «pixel de suivi»[69], mis à disposition par le fournisseur de médias sociaux. Après avoir quitté le site Internet 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 d'acheter en surfant sur BestBags.com.

Exemple5: Ciblage géographique

M^me^ 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 M^me^ 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. M^me^ Michu séjourne dans un hôtel situé à côté d'une pizzeria. La pizzeria utilise la fonctionnalité de ciblage géographique 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, M^me^ Michu voit une publicité de la pizzeria, décide qu'elle a faim et achète une pizza via son site Internet.

Exemple 6:

M^me^ Ghorbani se crée un compte sur une plateforme de médias sociaux. Lors de son inscription, la plateforme lui demande si elle consent au traitement de ses données à caractère personnel aux fins de l'affichage sur son compte de publicités ciblées à partir des données qu'elle communique directement au fournisseur de médias sociaux en question (par exemple, son âge, son sexe et sa ville) et compte tenu de son activité sur d'autres sites web en dehors de la plateforme de médias sociaux, qui utilisent des cookies. Elle est informée que ces données seront collectées par des modules de médias sociaux ou des pixels espions. Les processus mis en œuvre lui sont clairement décrits, tout comme le fait que ce ciblage fait appel à d'autres entités, qui sont conjointement responsables de garantir le respect du RGPD. Il lui est également indiqué qu'elle peut retirer son consentement à tout moment et un lien vers la politique de confidentialité de la plateforme de médias sociaux lui est fourni. Souhaitant voir des publicités ciblées sur son compte de médias sociaux, M^me^ Ghorbani accorde son consentement. Aucun cookie publicitaire n'est déposé ou collecté tant que M^me^ Ghorbani n'a pas accordé son consentement.

Plus tard, elle consulte le site «Thelatesthotnews.com», sur lequel un bouton de médias sociaux est intégré. Une bannière de petite taille, mais bien visible, apparaît en bas à droite de l'écran, demandant à M^me^ Ghorbani si elle consent à la transmission de ses données à caractère personnel au fournisseur de médias sociaux au moyen de cookies et de modules de médias sociaux. Le gestionnaire du site web

[69] Les pixels de suivi sont constitués de petits extraits de code qui sont intégrés dans le site Internet de la personne ciblée. Lorsqu'une personne accède au site Internet du cibleur dans son navigateur, celui-ci envoie automatiquement une requête 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 Internet 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 la localisation de ses utilisateurs sur la base d'autres points de données, y compris l'adresse IP et les informations WiFi des appareils mobiles, ou des données provenant de l'utilisateur (p. ex. s'il communique des informations sur sa localisation sur la plateforme dans une publication).

a mis en place des mesures techniques garantissant qu'aucune donnée à caractère personnel n'est transférée à la plateforme de médias sociaux tant que l'internaute n'a pas accordé son consentement.

5.3.1 Rôles

68. Dans l'exemple 4, 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, qui se traduit par l'affichage de publicités à destination de M. Schmidt.

69. En ce qui concerne la détermination de la finalité, Bestbags.com et le fournisseur de médias sociaux déterminent conjointement la finalité du traitement, qui consiste à afficher une publicité spécifique sur la plateforme de médias sociaux à destination des internautes constituant le public cible. En intégrant le pixel dans son site web, Bestbags.com exerce une influence décisive sur les moyens du traitement. La collecte et la transmission des données à caractère personnel des visiteurs du site web au fournisseur de médias sociaux n'auraient pas eu lieu sans l'intégration de ce pixel. Le fournisseur de médias sociaux, d'autre part, a développé et fournit le code logiciel (pixel) permettant la collecte automatique, la transmission et l'évaluation à des fins marketing des données à caractère personnel à ses propres fins. En conséquence, il existe un contrôle conjoint à l'égard de la collecte des données à caractère personnel et de leur transmission au moyen de pixels, ainsi qu'à l'égard de la correspondance et de l'affichage ultérieur de publicités destinées à M. Schmidt sur la plateforme de médias sociaux, et concernant tout rapport relatif à la campagne de ciblage. Un contrôle conjoint existe également, pour des raisons semblables, dans l'exemple 6.

70. Dans l'exemple 5, parce qu'elle définit les paramètres de ciblage publicitaire en fonction de ses besoins commerciaux (par exemple, ses horaires d'ouverture et la géolocalisation des personnes se trouvant à proximité de son établissement durant cette plage horaire), la pizzeria exerce une influence décisive sur le traitement des données à caractère personnel aussi doit-elle être considérée comme participant à la détermination des finalités et moyens du traitement des données. Le fournisseur de médias sociaux, quant à lui, collecte les informations sur la localisation de M^{me} Michu (par GPS) afin de permettre l'affichage de publicités ciblées basées sur la localisation. En conséquence, il existe un contrôle conjoint entre le cibleur et la plateforme de médias sociaux en ce qui concerne la collecte et l'analyse de la localisation de M^{me} Michu ainsi que l'affichage de la publicité en vue de cibler cette dernière (en tant que personne apparaissant à moins de 1 km de la pizzeria pour la première fois depuis 6 mois) avec la publicité.

5.3.2 Base juridique

71. Tout d'abord, compte tenu de l'utilisation de cookies dans les exemples 4, 5 et 6, les exigences tirées de l'article 5, paragraphe 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 une information claire et complète, entre autres sur les finalités du traitement, avant de donner leur accord[71], à quelques exceptions très limitées[72]. Une information claire et complète signifie que l'utilisateur doit être en position de déterminer facilement les conséquences de l'octroi de son accord et garantit que le

[71] Arrêt de la Cour de justice de l'Union européenne, Planet 49 GmbH, affaire C-673/17, point 73.
[72] Voir l'avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données. Voir aussi l'arrêt de la Cour de justice de l'Union européenne dans l'affaire Fashion ID, C-40/17, points 89 à 91.

consentement accordé est éclairé[73]. Dès lors, le responsable du traitement devra informer les personnes concernées de toutes les finalités pertinentes du traitement, notamment tout traitement ultérieur des données à caractère personnel obtenues en accédant aux informations se trouvant dans l'équipement terminal.

73. Pour être valable, le consentement recueilli pour la mise en application des technologies de suivi doit remplir les conditions énoncées à l'article 7 du RGPD[74]. Par exemple, le consentement n'est pas valablement constitué si l'utilisation des cookies est autorisée au moyen d'une case à cocher pré-cochée par le prestataire de services, que l'utilisateur doit décocher pour refuser son consentement[75]. Sur la base du considérant 32, des actions telles que faire défiler une page web ou naviguer sur une page web ou une activité similaire de l'utilisateur ne satisferont dans aucune circonstance à l'exigence d'un acte positif clair: il peut être difficile de distinguer ces actes d'une autre activité ou interaction par un utilisateur et, dès lors, il ne sera pas non plus possible de déterminer qu'un consentement univoque a été obtenu. En outre, dans ce cas, il sera difficile de permettre à l'utilisateur de retirer son consentement aussi facilement qu'il l'a donné[76].

74. Tout responsable (conjoint) du traitement cherchant à s'appuyer sur le consentement comme base juridique doit s'assurer que le consentement obtenu est valable. Dans l'arrêt Fashion ID, la CJUE a souligné l'importance de garantir la protection efficace et en temps utile des droits de la personne concernée et que le consentement ne doit pas être donné qu'au seul responsable conjoint du traitement intervenant ultérieurement. Un consentement valable doit être obtenu avant le traitement, ce qui signifie que les responsables (conjoints) du traitement doivent évaluer le moment et la façon dont les informations devraient être fournies et le consentement devrait être obtenu. Autrement dit, la question de savoir lequel des responsables conjoints du traitement devrait obtenir le consentement revient à déterminer lequel d'entre eux intervient en premier auprès de la personne concernée. Dans l'exemple 6, le dépôt de cookies et le traitement des données à caractère personnel ont lieu au moment de la création du compte: le fournisseur de médias sociaux doit obtenir son consentement valable avant de pouvoir déposer les cookies publicitaires.

75. Le CEPD rappelle également que si le consentement sollicité sert de base à plusieurs responsables (conjoints) du traitement ou si les données sont transférées à, ou traitées par, d'autres responsables qui souhaitent se fonder sur le consentement original, ces organisations devront 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, ce dernier devra nécessairement être complété par des informations et un consentement supplémentaires recueillis par le gestionnaire du site web intégrant le module de médias sociaux (c'est-à-dire *Thelatesthotnews.com* dans l'exemple 6).

76. Le CEPD souligne que le consentement devant être recueilli par le gestionnaire du site web pour la transmission de données à caractère personnel déclenchée par son site web (par l'intégration d'un module de médias sociaux) ne concerne que l'opération ou l'ensemble d'opérations nécessitant le traitement de données à caractère personnel dont le gestionnaire détermine effectivement les finalités et les moyens[78]. Le recueil du consentement par un gestionnaire de site web, c'est-à-dire

[73] *Idem*, point 74.
[74] Lignes directrices 5/2020 du CEPD sur le consentement au sens du règlement (UE) 2016/679, version 1.1, p. 6.
[75] Arrêt de la Cour de justice de l'Union européenne, Planet 49, affaire C-637/17, point 57.
[76] Lignes directrices 5/2020 du CEPD sur le consentement au sens du règlement (UE) 2016/679, version 1.1, p. 19.
[77] Lignes directrices 5/2020 du CEPD sur le consentement au sens du règlement (UE) 2016/679, version 1.1, p. 16, point 65.
[78] Arrêt du 29 janvier 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, points 100 et 101.

«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 accordé un consentement valable pour le traitement dont il est responsable en tant que responsable conjoint[79], ainsi que pour tout traitement ultérieur ou complémentaire qu'il effectue et pour lequel le gestionnaire du site web ne détermine pas conjointement les finalités et les moyens (ex.: opérations de profilage ultérieures à des fins de ciblage).

77. De plus, tout traitement ultérieur des données à caractère personnel, y compris les données à caractère personnel obtenues par l'intermédiaire de cookies, de modules de médias sociaux ou de pixels, doit également avoir une base juridique en vertu de l'article 6 du RGPD afin d'être licite[80]. En ce qui concerne la base juridique du traitement dans les exemples 4, 5 et 6, le CEPD considère que l'intérêt légitime ne peut pas servir de base juridique appropriée, étant donné que le ciblage repose sur le suivi du comportement des internautes sur des sites web et dans des lieux différents à l'aide de technologies de suivi[81].

78. Dès lors, dans pareilles circonstances, la base juridique appropriée pour tout traitement ultérieur au titre de l'article 6 du RGPD est également susceptible d'être le consentement de la personne concernée. En effet, lors de l'évaluation de la conformité avec l'article 6 du RGPD, il convient de tenir compte du fait que le traitement dans son ensemble suppose des activités spécifiques pour lesquelles le législateur de l'Union a cherché à fournir une protection supplémentaire[82]. De plus, lorsqu'ils déterminent la base juridique appropriée, les responsables du traitement doivent tenir compte de l'incidence sur les droits des personnes concernées, afin de respecter le principe de loyauté[83].

5.4 Ciblage sur la base des données déduites

79. Les données déduites désignent les données créées par le responsable du traitement à partir des données fournies par la personne concernée (que ces données aient été observées ou fournies de manière active par la personne concernée, ou une combinaison de ces deux possibilités)[84]. Les déductions sur les personnes concernées peuvent être effectuées aussi bien par le fournisseur de médias sociaux que par le cibleur.

[79] Ceci 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 à caractère personnel à des fins de publicité ciblée. Par conséquent, le fournisseur de médias sociaux est tenu de s'assurer qu'un consentement valable est obtenu.

[80] Avis 5/2019 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, point 41.

[81] Avis du groupe de travail «Article 29» sur le profilage et la prise de décision automatisée, WP 251, rév. 01, p. 15, voir également l'avis du WP «Article 29» 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 relatif aux interactions entre la directive «vie privée et communications électroniques» et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de protection des données, point 41.

[83] Comité européen de la protection des données, lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, version 2.0, 8 octobre 2019, point 1.

[84] Voir également les lignes directrices du groupe de travail «article 29» sur la protection des données relatives au droit à la portabilité des données, WP 242 rév. 01, 5 avril 2017, p. 10.

80. À titre d'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 mentions «j'aime» données), le fournisseur de médias sociaux peut parvenir à déduire des informations concernant les intérêts et d'autres caractéristiques de l'utilisateur des médias sociaux. Dans le même ordre d'idées, un cibleur pourrait aussi parvenir à déduire des données sur une personne en particulier et utiliser ces connaissances pour la cibler et afficher des publicités sur son compte de médias sociaux.

Exemple 7:

M[me] Delucca attribue souvent des mentions «j'aime» aux photos du peintre impressionniste Pataolito postées par la galerie d'art Beautifulart sur sa page de médias sociaux. Le musée Z cherche à attirer les internautes intéressés par les peintures impressionnistes en vue de sa prochaine exposition. Il emploie les critères de ciblage suivants, proposés par le fournisseur de médias sociaux: «intéressé(e) par l'impressionnisme», genre, âge et lieu de résidence. M[me] Delucca reçoit alors sur sa page de médias sociaux des publicités ciblées du musée Z en lien avec la prochaine exposition du musée.

Exemple 8:

M. Leon a indiqué sur sa page de médias sociaux qu'il s'intéressait au sport. Il a téléchargé une application sur son téléphone portable pour suivre les derniers résultats de ses matchs préférés, a défini la page www.livesportsresults.com comme page d'accueil sur le navigateur de son ordinateur portable et utilise souvent son ordinateur de bureau au travail pour faire des recherches internet sur les derniers résultats sportifs. Il consulte également plusieurs sites de jeu d'argent en ligne. Le fournisseur de médias sociaux suit l'activité en ligne de M. Leon sur ses différents appareils, à savoir, son ordinateur portable, son téléphone portable et son ordinateur de bureau. D'après son activité et toutes les informations fournies par M. Leon, le fournisseur de médias sociaux 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 des revenus plus faibles. La société de pari en ligne «bestpaydayloans» souhaite cibler les utilisateurs désireux de faire des paris et susceptibles de parier beaucoup. Elle sélectionne donc les critères proposés par le fournisseur de médias sociaux pour cibler le public à qui ses publicités seront affichées.

5.4.1 Rôles

81. En ce qui concerne la détermination des rôles des différents acteurs, le CEPD note ce qui suit: dans l'exemple 7, un contrôle conjoint existe entre le musée Z et le fournisseur de médias sociaux en ce qui concerne le traitement de données à caractère personnel aux fins de l'affichage de publicités ciblées, compte tenu de la collecte de ces données au moyen de la fonctionnalité «j'aime» sur la plateforme de médias sociaux et de l'«analyse» effectuée par le fournisseur de médias sociaux en vue de proposer le critère de ciblage [«intéressé(e) par l'impressionnisme»] au cibleur dans le but d'afficher finalement la publicité[85].

[85] Concernant les pages de médias sociaux, les conditions d'un contrôle conjoint peuvent également être réunies pour ce qui est des informations statistiques fournies par le fournisseur de médias sociaux à l'administrateur de la page: voir l'arrêt de la CJUE C-210/16, Wirtschaftsakademie.

82. Dans l'exemple 8, un contrôle conjoint existe entre la société bestpaydayloans et le fournisseur de médias sociaux en ce qui concerne les opérations de traitement déterminées conjointement. Dans ce cas, il s'agit de la sélection des critères de ciblage et de l'affichage subséquent de publicités, ainsi que la création de tout rapport en lien avec la campagne de ciblage.

5.4.2 Base juridique

83. Le ciblage des utilisateurs des médias sociaux à partir de données déduites à des fins publicitaires requiert généralement de réaliser un profilage[86]. Le GT29 a précédemment clarifié que, selon le RGPD, le profilage se définit comme le traitement automatisé de données à caractère personnel consistant à évaluer certains aspects personnels, notamment pour analyser ou prédire des éléments concernant des personnes physiques, ajoutant que «[l]'utilisation du mot "évaluer" suggère que le profilage implique une certaine forme d'appréciation ou de jugement à l'égard d'une personne»[87]. Le profilage peut être légal au regard de l'un quelconque des fondements juridiques de l'article 6, paragraphe 1, du RGPD, 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» s'applique dans la mesure où l'affichage de publicités sur la page de M[me] Delucca en lien avec le peintre Pataolito requiert une opération de lecture/écriture pour établir une correspondance de cette mention «j'aime» avec les informations précédemment détenues à son sujet par le fournisseur de médias sociaux. Le consentement sera donc exigé pour ces opérations.

85. En ce qui concerne l'exemple 8, le CEPD rappelle que dans le cas des décisions automatisées produisant des effets juridiques pour la personne concernée ou l'affectant de manière significative de façon similaire, conformément à l'article 22 du RGPD, les responsables du traitement peuvent s'appuyer sur les exceptions suivantes:

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

86. Le GT29 a déjà déclaré que «*Dans de nombreux cas typiques, la décision de présenter une publicité ciblée fondée sur le profilage [...] n'affectera pas les personnes concernées de manière significative de façon similaire [...]. Toutefois, il se peut que ce soit le cas, selon les caractéristiques particulières de la situation, y compris en ce qui concerne:*

- *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 façon dont l'annonce est diffusée; ou*
- *le recours aux vulnérabilités connues des personnes concernées visées.*»[88]

[86] Le CEPD note que le profilage peut également avoir eu lieu dans les exemples précédents.
[87] Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251 rév. 01, p. 7.
[88] Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251 rév. 01, p. 22.

87. Lorsque le profilage entrepris par le fournisseur de médias sociaux est susceptible d'«[affecter] de manière significative de façon similaire» une personne concernée, l'article 22 s'applique. Une évaluation visant à savoir si le ciblage «[affectera] de manière significative de façon similaire» une personne concernée devra être menée par le responsable du traitement (ou les responsables conjoints du traitement, selon le cas) dans chaque cas, en référence 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 RGPD (ciblant des personnes financièrement vulnérables intéressées par les paris en ligne, qui risquent de nuire de manière significative à leur situation financière). Par conséquent, en accord avec l'article 22, un consentement explicite serait exigé. En outre, le recours à des techniques de suivi déclenche l'applicabilité de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», entraînant l'exigence d'un consentement préalable. Enfin, le CEPD rappelle que pour que le traitement soit légal, le responsable du traitement doit mener une évaluation au cas par cas et que l'obtention du consentement ne réduit pas les autres obligations d'observer les exigences de loyauté, de nécessité, de proportionnalité et de qualité des données, conformément à l'article 5 du RGPD.

6 TRANSPARENCE ET DROIT D'ACCÈS

89. L'article 5, paragraphe 1, point a), du RGPD prévoit que les données à caractère personnel sont traitées de manière licite, loyale et transparente au regard de la personne concernée. Il prévoit en outre que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes. Les articles 12, 13 et 14 du RGPD contiennent des dispositions spécifiques sur les obligations de transparence du responsable du traitement. Enfin, le considérant 39 prévoit que «*Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées*»[89].

90. Les informations présentées aux personnes concernées sur la façon dont leurs données à caractère personnel sont traitées devraient, dans tous les cas, être concises, transparentes, compréhensibles et aisément accessibles, et formulées en des termes clairs et simples.

91. Le CEPD rappelle que la simple utilisation du terme «publicité» ne suffirait pas à informer les utilisateurs que leur activité fait l'objet d'un suivi aux fins de l'affichage de publicités ciblées. Les personnes concernées doivent être informées en toute transparence des types d'activités de traitement réalisés et de ce que cela signifie pour elles dans la pratique. Elles devraient être informées en des termes facilement compréhensibles si un profil sera établi à partir de leur comportement en ligne sur la plateforme ou sur le site web du cibleur, respectivement, par la plateforme de médias sociaux et par le cibleur, en adressant à ces personnes des informations sur les types de données à caractère personnel collectés aux fins d'établir de tels profils et, à terme, de permettre leur ciblage et l'affichage de publicités comportementales par les cibleurs[90]. Les informations pertinentes doivent apparaître directement sur l'écran des internautes, de façon interactive et, lorsque cela est approprié ou nécessaire, au moyen d'avis à différents niveaux[91].

[89] Voir également groupe de travail «article 29», lignes directrices sur la transparence au sens du règlement (UE) 2016/679, WP260 rév. 01, du 11 avril 2018, https://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=622227.

[90] Voir lignes directrices du CEPD sur la transparence au sens du règlement (UE) 2016/679.

[91] Lignes directrices du groupe de travail «article 29» sur le consentement au titre du règlement (UE) 2016/679, WP259 rév. 01, points 24 et 35.

6.1 Grandes lignes de l'accord et informations à fournir (article 26, paragraphe 2, du RGPD)

92. En vertu de l'article 26, paragraphe 1, du RGPD, Les responsables conjoints du traitement «*définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord*».

93. Le principe de transparence est réitéré par l'obligation de mettre les grandes lignes de l'accord de contrôle conjoint du traitement à la disposition de la personne concernée en vertu de l'article 26, paragraphe 2, du RGPD. En effet, l'article 26 du RGPD exige des responsables conjoints du traitement qu'ils prennent des mesures appropriées pour garantir que les personnes concernées sont informées de la répartition des responsabilités.

94. Par principe, les informations fournies à la personne concernée doivent couvrir tous les aspects des opérations de traitement des données pour lesquelles les responsables conjoints du traitement sont conjointement responsables. De fait, la personne concernée est en droit de recevoir toutes les informations (notamment concernant le traitement ultérieur envisagé en cas de contrôle conjoint) de prime abord, de sorte que l'information soit loyale et appropriée. Plus précisément, cet accord commun doit garantir que la personne concernée recevra les informations requises au titre des articles 13 et 14 du RGPD, notamment en ce qui concerne les finalités partagées ou associées, les durées de conservation, le transfert à des tiers, etc., qui doivent être communiquées à la personne concernée lors de la collecte des données ou avant que commence le traitement. L'accord doit stipuler clairement les responsabilités à cet égard. Pour satisfaire à ces exigences, l'accord doit contenir une information claire et complète (ou y faire référence) à l'égard du traitement auquel il renvoie, accompagnée d'explications, s'il y a lieu, sur les différentes phases et différents acteurs du traitement[92].

95. Bien que les deux responsables conjoints du traitement soient soumis à l'obligation d'informer la personne concernée en cas de responsabilité conjointe, ils peuvent décider d'un commun accord que l'un d'eux assumera la tâche de fournir l'information initiale aux personnes concernées, en particulier lorsqu'un seul des responsables du traitement interagit avec l'utilisateur avant le traitement, par exemple sur son site web[93]. Cet échange d'informations à fournir à la personne concernée doit faire partie intégrante de l'accord commun (par exemple en annexe). Si l'un des responsables conjoints du traitement ne dispose pas de toutes les informations dans le détail parce qu'il ne connaît pas, par exemple, l'exécution technique exacte des activités de traitement, l'autre responsable conjoint du traitement lui transmet toutes les informations nécessaires pour lui permettre de fournir à la personne concernée toutes les informations demandées en vertu des articles 13 et 14 du RGPD.

96. Le CEPD observe que les responsables du traitement ne sont pas directement responsables de la fourniture de l'information requise au titre des articles 13 et 14 du RGPD en lien avec les opérations de traitement ultérieures ne relevant pas du champ d'application du contrôle conjoint. Par

[92] Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP169, p. 28.
[93] CJUE *Fashion ID*, points 102 et 105.

conséquent, le cibleur n'est pas directement responsable de fournir l'information requise dans le cadre de tout traitement ultérieur effectué par la plateforme de médias sociaux[94].

97. Néanmoins, le CEPD souligne que le responsable du traitement qui a l'intention d'utiliser ultérieurement les données à caractère personnel assume des obligations spécifiques d'information pour ce traitement ultérieur en l'absence de responsabilité conjointe, conformément à l'article 14, paragraphe 4, du RGPD, ainsi que des obligations de compatibilité du traitement ultérieur au titre de l'article 6, paragraphe 4. À titre d'exemple, le cibleur et le fournisseur de médias sociaux pourraient convenir que le cibleur fournit certaines informations au nom du fournisseur de médias sociaux. Le fournisseur de médias sociaux, en revanche, demeure responsable en dernier ressort de garantir que la personne concernée a reçu les informations pertinentes en ce qui concerne toutes les activités de traitement sous son contrôle.

Dans l'exemple 3 (où M. Lopez est ciblé par des publicités pour la banque X sur sa page de médias sociaux suite au transfert par la banque de son adresse électronique au fournisseur de médias sociaux), la banque doit informer M. Lopez que son adresse électronique sera utilisée à des fins publicitaires, par l'intermédiaire du fournisseur de médias sociaux, ou en vue de l'envoi d'offres en lien avec des services bancaires. 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.

De plus, dans la mesure où le fournisseur de médias sociaux a l'intention de traiter ultérieurement l'adresse électronique de M. Lopez pour d'autres finalités, il doit s'assurer que M. Lopez a reçu les informations requises au titre de l'article 14, paragraphe 4, du RGPD avant de procéder.

Le fournisseur de médias sociaux et la banque peuvent convenir que la banque fournira à M. Lopez les informations pertinentes au nom du fournisseur de médias sociaux. Même si c'est le cas, cependant, le fournisseur de médias sociaux demeure responsable en dernier ressort de garantir que la personne concernée a reçu les informations pertinentes à l'égard de toutes les activités de traitement pour lesquelles il est (seul) responsable. Cette obligation ne s'appliquerait pas si M. Lopez avait déjà été informé par la banque de ce traitement, conformément à l'article 14, paragraphe 5, point a), du RGPD.

Ces obligations de transparence doivent être prises en compte sans préjudice des obligations spécifiques applicables aux considérations en matière de base juridique.

98. Chaque responsable conjoint du traitement est tenu de garantir que les grandes lignes de l'accord sont mises à la disposition de la personne concernée. En pratique, les grandes lignes de l'accord devraient être directement disponibles sur la plateforme, mentionnées par renvoi dans la politique de confidentialité de cette dernière, et être également directement accessibles au moyen d'un lien, par

[94] Comme le précisent les lignes directrices 7/2020 du CEPD sur les notions de responsable du traitement et de sous-traitant dans le cadre du RGPD, chaque responsable du traitement est tenu de s'assurer que les données ne subissent pas un traitement ultérieur pour une finalité incompatible avec celle de leur collecte initiale par le responsable du traitement partageant les données. Il serait une bonne pratique que le responsable du traitement qui prévoit de traiter des données à caractère personnel pour une autre finalité fournisse des moyens suffisants à l'autre responsable du traitement qui transmet les données à caractère personnel afin de s'assurer de l'existence d'une base juridique, qui serait très certainement le consentement, et que les personnes concernées ont été dûment informées, car cela permettrait au cibleur de garantir que le transfert au fournisseur de médias sociaux est licite.

exemple, dans la page du cibleur sur la plateforme de médias sociaux ou dans un lien intitulé, par exemple, «Pourquoi cette annonce est-elle apparue sur mon navigateur?».

6.2 Droit d'accès (article 15)

99. Les responsables du traitement doivent permettre aux utilisateurs d'exercer pleinement et facilement leurs droits en tant que personnes concernées. Un outil efficace et facile d'utilisation devrait être mis à la disposition de la personne concernée pour lui garantir de pouvoir exercer facilement tous ses droits, à tout moment, en particulier le droit à l'effacement, le droit de s'opposer et le droit d'accès, conformément à l'article 15 du RGPD[95]. Les paragraphes suivants se concentrent sur la façon dont le droit d'accès devrait être pris en compte, et par qui, dans le contexte du ciblage des utilisateurs de médias sociaux[96].

100. De façon générale, pour satisfaire aux exigences de l'article 15, paragraphe 1, du RGPD et garantir une transparence totale, les responsables du traitement pourraient songer à appliquer un mécanisme de vérification du profil des personnes concernées, comprenant le détail des informations et les sources utilisées pour développer celles-ci. La personne concernée devrait pouvoir connaître l'identité du cibleur et les responsables du traitement devraient faciliter l'accès aux informations concernant le ciblage, notamment les critères de ciblage utilisés, ainsi qu'aux autres informations requises au titre de l'article 15 du RGPD[97].

101. S'agissant du type d'accès à accorder aux personnes concernées, le considérant 63 dispose que «*[l]orsque c'est possible, le responsable du traitement devrait pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant*». Les caractéristiques spécifiques des fournisseurs de médias sociaux, à savoir, l'environnement en ligne et 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, paragraphes 1 et 2, du RGPD. L'accès à distance dans ce cas peut être considéré comme la mesure la plus «appropriée» au sens de l'article 12, paragraphe 1, du RGPD, prenant également en compte le fait qu'il s'agit d'une situation typique «où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin» (voir considérant 58, qui ajoute explicitement «la publicité en ligne» comme exemple concret). En outre, s'ils en font la demande, les utilisateurs des médias sociaux ayant été ciblés devraient également recevoir une copie des données à caractère personnel les concernant, conformément à l'article 15, paragraphe 3, du RGPD.

---

[95] L'article 15, paragraphes 1 et 2, du RGPD précise les informations à fournir à la personne concernée demandant à accéder à ses données. L'article 15, paragraphes 3 et 4, du RGPD réglemente le droit d'obtenir une copie.

[96] Voir lignes directrices du CEPD sur la transparence au sens du règlement (UE) 2016/679, p. 35.

[97] Pour de plus amples précisions sur les informations requises au titre de l'article 15 du RGPD dans le contexte du profilage, voir les lignes directrices du groupe de travail «article 29» sur la protection des données, WP251 rév. 01, p. 17 («*L'article 15 donne à la personne concernée le droit d'obtenir des précisions sur toutes les données à caractère personnel utilisées pour le profilage, y compris les catégories de données utilisées pour l'élaboration d'un profil. Outre les informations générales sur le traitement, le responsable du traitement est tenu, conformément à l'article 15, paragraphe 3, de mettre à disposition les données utilisées pour créer le profil, et de donner accès aux informations sur le profil et les segments dans lesquels la personne concernée a été placée.*») Il est important que ces informations soient adaptées sur mesure à la situation particulière de la personne concernée, en complétant toute information déjà fournie au titre des articles 1er et 14.

102. En vertu de l'article 15, paragraphe 1, point c), du RGPD, l'utilisateur a accès en particulier aux informations sur «*les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales*». En vertu de l'article 4, paragraphe 9, le terme «destinataire» désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Un cibleur n'est pas nécessairement le «destinataire» des données à caractère personnel (voir exemple 1), car les données à caractère personnel peuvent ne pas lui être communiquées, mais il recevra des statistiques des clients cibles sous forme agrégée ou anonymisée, par exemple dans le cadre de sa campagne ou de l'évaluation des performances de cette dernière. Néanmoins, dans la mesure où le cibleur agit en tant que responsable conjoint du traitement, il doit être présenté en tant que tel auprès de l'utilisateur du média social.

103. Bien que l'article 15 du RGPD ne soit pas explicitement mentionné dans l'article 26, paragraphe 1, du RGPD, les termes de cet article renvoient à toutes les «obligations [...] aux fins d'assurer le respect des exigences» au titre du RGPD, qui incluent l'article 15 dudit règlement.

104. Pour permettre aux personnes concernées d'exercer leurs droits d'une 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 devrait répondre aux demandes de la personne concernée et s'y conformer, mais ils ne peuvent exclure la possibilité pour la personne concernée d'exercer ses droits à l'égard de et contre chacun d'entre eux (article 26, paragraphe 3, du RGPD). Dès lors, les cibleurs et fournisseurs de médias sociaux doivent garantir qu'un mécanisme approprié est en place pour permettre aux personnes concernées d'obtenir facilement l'accès à leurs données à caractère personnel (y compris les critères de ciblage utilisés) ainsi qu'à toutes les informations requises par l'article 15 du RGPD.

7 ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

105. En principe, avant d'entamer les opérations de ciblage envisagées, les deux responsables conjoints du traitement devraient vérifier la liste des opérations de traitement «susceptible[s] d'engendrer un risque élevé» adoptée au niveau national en vertu de l'article 35, paragraphe 4, et des considérants 71, 75 et 91 du RGPD pour déterminer si le ciblage désigné correspond à l'un quelconque des types d'opérations de traitement soumis à l'exigence de réaliser une AIPD. Pour apprécier si les opérations de ciblage envisagées sont «susceptible[s] d'engendrer un risque élevé» et si une AIPD est nécessaire, les critères relevés dans les lignes directrices concernant l'AIPD devraient également être pris en compte[98], ainsi que les listes que les autorités de contrôle ont dressées sur le type d'opérations de traitement soumises à l'exigence d'une analyse d'impact relative à la protection des données (conformément à l'article 35, paragraphe 4).

106. Dans certains cas, la nature du produit ou service annoncé, le contenu du message ou la façon dont l'annonce est diffusée peut produire des effets sur la personne, qui doivent être examinés plus en détail. Cela peut être le cas, par exemple, des produits qui ciblent des personnes vulnérables. Des risques supplémentaires peuvent émerger, selon les finalités de la campagne publicitaire et son

[98] Voir lignes directrices du CEPD concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP248 rév. 0.

caractère intrusif, ou si le ciblage porte sur le traitement de données à caractère personnel observées, déduites ou dérivées.

107. Outre les obligations spécifiquement désignées à l'article 26, paragraphe 1, du RGPD, les responsables conjoints du traitement devraient également tenir compte des autres exigences au moment de déterminer leurs obligations respectives. Comme indiqué dans les lignes directrices du CEPD concernant l'analyse d'impact relative à la protection des données (AIPD), «[l]orsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives».

108. Dès lors, les responsables conjoints du traitement doivent évaluer si une AIPD est nécessaire. Si une AIPD est nécessaire, ils sont tous deux responsables de satisfaire cette obligation. Le CEPD rappelle que l'AIPD devrait englober l'intégralité du traitement des données à caractère personnel, ce qui signifie, en principe, que les deux responsables conjoints du traitement doivent participer à la réalisation de l'AIPD. Dans ce contexte, les deux responsables conjoints du traitement doivent garantir qu'ils disposent de suffisamment d'informations sur le traitement pour effectuer l'AIPD requise[99]. Cela requiert donc que «chaque responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par ex.) et à ne pas divulguer de vulnérabilités»[100].

109. En pratique, il est possible que les responsables conjoints du traitement décident que l'un d'eux assume la tâche de réaliser l'AIPD en tant que tel. Ce choix devrait alors être précisé dans l'accord commun, sans préjudice de l'existence d'une responsabilité conjointe en tant que telle. La raison étant que l'un des responsables du traitement peut s'avérer mieux placé pour apprécier certaines opérations de traitement. Par exemple, ce responsable du traitement peut, selon le contexte, avoir un niveau supérieur de contrôle et de connaissances du processus de ciblage, en particulier de la partie dorsale du système déployé, ou des moyens du traitement.

110. Chaque AIPD doit inclure les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. S'il n'est pas possible de répondre de façon suffisante aux risques recensés (c'est-à-dire si les risques résiduels demeurent élevés), les responsables conjoints du traitement sont chacun responsables de garantir une consultation préalable avec les autorités de contrôle compétentes. Si le ciblage constituait une violation du RGPD, en particulier du fait d'une identification ou d'une atténuation insuffisante des risques, il ne devrait pas avoir lieu.

Exemple 9:
Le parti politique «Letschangetheworld» souhaite encourager les utilisateurs des médias sociaux à voter pour un candidat politique en particulier lors des prochaines élections. Il souhaite cibler les personnes âgées vivant en zone rurale, qui se rendent régulièrement à l'église et qui ne sont pas allées à l'étranger depuis au moins 2 ans.

[99] Le CEPD réitère qu'une AIPD n'est pas nécessaire lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'une AIPD. Dans un tel cas, les résultats de l'AIPD réalisée pour le traitement similaire peuvent être utilisés. Voir lignes directrices du groupe de travail «article 29» concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, p. 12.

[100] *Idem*, p. 8.

111. Il existe un contrôle conjoint entre la plateforme de médias sociaux et le parti politique, aux fins d'établir une correspondance avec le profil et de l'affichage de la publicité ciblée. Le parti politique Letschangetheworld et la plateforme de médias sociaux doivent déterminer ensemble si une AIPD est nécessaire. De fait, dans cet exemple, ils ont tous deux suffisamment de connaissances sur les critères employés aux fins du ciblage des personnes pour déterminer si le traitement est susceptible d'engendrer un risque élevé.

112. Dans l'éventualité où une AIPD serait nécessaire, l'accord commun devrait chercher à établir la façon dont les responsables du traitement devraient la réaliser et garantir qu'un échange pertinent de connaissances a lieu. Dans cet exemple, la raison peut être que la plateforme de médias sociaux est mieux placée pour apprécier certaines opérations de traitement, dans la mesure où le parti politique ne fait que sélectionner des critères de ciblage généraux.

8 CATÉGORIES PARTICULIÈRES DE DONNÉES

8.1 Ce qui constitue une catégorie particulière de données

113. Le RGPD assure une protection spécifique en ce qui concerne les données à caractère personnel qui sont particulièrement sensibles du point de vue des libertés et des droits fondamentaux des personnes. Ces données sont définies à l'article 9 du RGPD comme des catégories particulières de données à caractère personnel et incluent les données concernant la santé, l'origine raciale ou ethnique, les données biométriques, 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 qu'à condition de remplir l'une des conditions énoncées à l'article 9, paragraphe 2, du RGPD, comme avoir obtenu le consentement explicite de la personne concernée ou que le traitement porte sur des données ayant été manifestement rendues publiques par la personne concernée. Outre les conditions prévues par l'article 9 du RGPD, le traitement portant sur des catégories particulières de données doit s'appuyer sur une base juridique établie à l'article 6 du RGPD et être réalisé conformément aux principes fondamentaux énoncés à l'article 5 du RGPD.

115. De plus, le traitement portant sur des catégories particulières de données à caractère personnel est pertinent lors de l'évaluation des mesures appropriées conformément aux articles 24, 25, 28 et 32 du RGPD, mais aussi pour déterminer si une AIPD doit être effectuée en vertu de l'article 35 du RGPD, et si un délégué à la protection des données doit être nommé au titre de l'article 37 du RGPD.

116. Dans le contexte des médias sociaux et du ciblage, il est nécessaire de déterminer si le traitement des données à caractère personnel porte sur des «catégories particulières de données» et si ces données sont traitées par le fournisseur de médias sociaux, le cibleur ou les deux. Si des catégories particulières de données à caractère personnel sont traitées, il convient de déterminer si et dans quelles conditions le fournisseur de médias sociaux et le cibleur peuvent traiter de manière licite ces données.

117. Si le fournisseur de médias sociaux traite la catégorie particulière de données à des fins de ciblage, il doit trouver une base juridique justifiant ce traitement dans l'article 6 du RGPD et s'appuyer sur une exception au titre de l'article 9, paragraphe 2, du RGPD, comme le consentement de la personne concernée, conformément à l'article 9, paragraphe 2, point a), du RGPD. Si un cibleur engage un fournisseur de médias sociaux et lui demande de cibler les utilisateurs à partir de cette catégorie particulière de données, le cibleur et le fournisseur de médias sociaux seront conjointement responsables du traitement de cette catégorie particulière de données.

118. L'analyse juridique suivante porte sur différentes situations dans lesquelles un tel traitement peut avoir lieu et sur leurs conséquences juridiques.

8.1.1 Catégories particulières explicites de données

119. Il arrive que des données à caractère personnel traitées relèvent clairement de la définition de catégorie particulière de données, par exemple en cas de déclaration directe concernant un membre d'un parti politique ou d'une association religieuse en particulier.

> Exemple 10:
>
> M[me] Flora déclare explicitement sur son profil de médias sociaux qu'elle est membre du parti politique GreenestPlanet. L'organisation de protection de l'environnement «Long live the Earth» souhaite cibler les utilisateurs des médias sociaux membres du parti politique GreenestPlanet afin de leur envoyer des messages ciblés.

120. Dans l'exemple 10, le fournisseur de médias sociaux et l'organisation de protection de l'environnement agissent en tant que responsables conjoints du traitement[101]. Dans la mesure où l'organisation de protection de l'environnement 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 au titre de l'article 9 du RGPD. Le traitement de ces données est, en principe, interdit par l'article 9, paragraphe 1. Le fournisseur de médias sociaux et l'organisation de protection de l'environnement doivent dès lors s'appuyer sur l'une des exceptions de l'article 9, paragraphe 2, pour effectuer ce traitement. En outre, ils doivent tous deux justifier ce traitement par une base juridique en vertu de l'article 6. Parmi les exceptions prévues à l'article 9, paragraphe 2, il semble que la seule exception applicable dans cette situation serait d'obtenir le consentement explicite de la personne concernée, en vertu de l'article 9, paragraphe 2, point a), du RGPD, ou l'exception selon laquelle M[me] Flora a manifestement rendu lesdites données publiques, en vertu de l'article 9, paragraphe 2, point e), du RGPD.

8.1.2 Catégories particulières de données déduites et combinées

121. Les suppositions ou déductions portant sur des catégories particulières de données, par exemple supposer qu'une personne est susceptible de voter pour un parti en particulier parce qu'elle a consulté la page d'un site web en faveur d'opinions libérales, constitueraient également une catégorie particulière de données à caractère personnel. De même, comme indiqué précédemment par le CEPD, «*[l]e profilage peut engendrer des données d'une catégorie particulière par inférence à partir de données qui n'appartiennent pas à une catégorie particulière en soi, mais qui le deviennent lorsqu'elles sont combinées avec d'autres données*. *Par exemple, il peut être possible de déduire l'état de santé d'une personne à partir des historiques de ses achats d'aliments combinés à des données sur la qualité et la teneur énergétique des aliments».* [102]

122. À titre d'exemple, le traitement d'une simple déclaration ou d'un simple élément de données de localisation ou similaire révélant qu'un utilisateur s'est rendu (une fois ou à plusieurs reprises) à un endroit généralement fréquenté par des personnes ayant certaines convictions religieuses ne sera généralement pas considéré en soi comme un traitement portant sur des catégories particulières de données. Cependant, ce traitement peut être considéré comme portant sur des catégories

[101] Voir l'analyse au chapitre 5.2.1.
[102] Lignes directrices du groupe de travail «article 29» relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251 rév. 01, p. 15.

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 finalités de leur utilisation.

Exemple 11:

Le profil de M. Novak sur son compte de médias sociaux ne révèle que des informations d'ordre général, telles que son nom et son lieu de résidence, mais une mise à jour de statut révèle qu'il s'est fréquemment rendu à l'église de sa ville, où il a suivi une messe. Par la suite, l'église en question souhaite cibler ses visiteurs en leur adressant des messages religieux afin d'encourager les chrétiens à rejoindre la congrégation. Dans ce cas, l'utilisation de données à caractère personnel tirées de la mise à jour du statut de M. Novak à de telles finalités de ciblage revient à procéder à un traitement portant sur des catégories particulières de données à caractère personnel.

123. Si un fournisseur de médias sociaux ou un cibleur utilise les données observées pour catégoriser l'utilisateur comme ayant certaines convictions religieuses ou philosophiques ou certaines opinions politiques, que la catégorisation soit correcte/vraie ou non, dans ce contexte, cette catégorisation de l'utilisateur doit manifestement être considérée comme un traitement portant sur des catégories particulières de données à caractère personnel. À partir du moment où la catégorisation permet un ciblage basé sur une catégorie particulière de donnée, le nom attribué à la catégorie n'a pas d'importance.

Exemple 12:

M. Sifuentes fournit des informations sur son profil de médias sociaux en mettant régulièrement à jour son statut, en indiquant sa présence à des endroits précis, etc., et ces informations révèlent qu'il participe régulièrement à des activités organisées par le mouvement «Mind, Body and Spirit». Bien qu'il ne fasse pas de déclaration explicite quant à ses convictions philosophiques, toutes les mises à jour, mentions «j'aime», indications de localisation et données similaires fournies par l'utilisateur révèlent sans équivoque que M. Sifuentes a certaines opinions philosophiques.

Exemple 13:

Un fournisseur de médias sociaux utilise les informations fournies volontairement par M^{me} Allgrove sur son profil, notamment son âge, ses centres d'intérêt et son adresse, et les combine avec des données observées sur les sites web qu'elle a consultés ainsi que les mentions «j'aime» qu'elle a attribuées sur la plateforme de médias sociaux. Le fournisseur de médias sociaux utilise les données collectées pour déduire que M^{me} Allgrove fait partie des partisans politiques libéraux de gauche et la place dans la catégorie «intéressé(e) par la politique libérale de gauche», puis met cette catégorie de ciblage à la disposition des cibleurs à des fins de publicité ciblée.

124. Dans l'exemple 12, la quantité importante d'informations et l'absence de mesures visant à empêcher un ciblage fondé sur une catégorie particulière de données signifient qu'un traitement portant sur des catégories particulières de données a lieu. Toutefois, le simple fait qu'un fournisseur de médias sociaux traite de grandes quantités de données qui pourraient potentiellement être utilisées pour déduire des catégories particulières de données ne signifie pas automatiquement que le traitement relève de l'article 9 du RGPD. L'article 9 ne pourra être invoqué si le traitement du fournisseur de médias sociaux n'entraîne pas l'inférence de catégories particulières de données et que le fournisseur de médias sociaux a pris des mesures pour empêcher que ces données puissent être déduites ou utilisées à des fins de ciblage. Dans tous les cas, le traitement d'une grande quantité de données à caractère personnel d'un utilisateur peut comporter des risques spécifiques pour les droits et libertés d'une

personne physique, qui doivent être éliminés en mettant en place des mesures de sécurité appropriées, telles que prévues par l'article 32 du RGPD, et également en tenant compte des conclusions de l'AIPD, réalisée en vertu de l'article 35 du RGPD.

125. Dans l'exemple 13, la proposition et l'utilisation de la catégorie de ciblage «intéressé(e) par la politique libérale de gauche» reviennent à effectuer un traitement portant sur des catégories particulières de données, car cette catégorie pourrait facilement être utilisée pour cibler les personnes ayant des opinions politiques libérales de gauche. En attribuant une opinion politique à un utilisateur par inférence, le fournisseur de médias sociaux procède au traitement de catégories particulières de données. Aux fins de l'article 9 du RGPD, le fait que l'utilisateur soit ou non partisan d'un parti politique libéral de gauche n'a pas d'importance. Le fait que la catégorie de ciblage soit intitulée «intéressé(e) par...» et non «partisan de...» n'a pas non plus d'importance, puisque l'utilisateur est placé dans la catégorie de ciblage à partir d'une déduction de ses centres d'intérêt politique.

Exemple 14:

M. Svenson se soumet à un test d'aptitude professionnelle comprenant une évaluation psychologique, qui a été élaboré par la société «YourPerfectJob». Le test est accessible sur une plateforme de médias sociaux et utilise l'interface de programmation (API) fournie par le fournisseur de médias sociaux. YourPerfectJob collecte des données sur l'éducation, la situation d'emploi, l'âge, les centres d'intérêt, les publications, l'adresse électronique et les connexions de M. Svenson. La société obtient les données par l'API, en accord avec les «autorisations» accordées par M. Svenson via son compte de médias sociaux. L'objectif déclaré de l'application est de prédire la meilleure orientation professionnelle d'un utilisateur en particulier.

Sans que le fournisseur de médias sociaux le sache ou l'approuve, YourPerfectJob utilise ces informations pour déduire plusieurs aspects personnels, notamment ses traits de personnalité, son profil psychologique et ses opinions politiques. YourPerfectJob décide ensuite d'utiliser ces informations pour cibler M. Svenson au nom d'un parti politique, en se servant de la fonction de ciblage par courrier électronique 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 particulières de données à caractère personnel, mais pas le fournisseur de médias sociaux. De fait, les opinions politiques de M. Svenson sont évaluées et établies sans la participation du fournisseur de médias sociaux[103]. En plus de déclencher l'interdiction générale prévue par l'article 9 du RGPD, le ciblage mentionné dans l'exemple 14 constitue également une infraction des exigences de loyauté, de transparence et de limitation de la finalité. En effet, M. Svenson n'est pas correctement informé du fait que les données à caractère personnel le concernant seront traitées aux fins d'un ciblage politique qui, par ailleurs, ne semble pas être compatible avec un test d'aptitude professionnelle.

[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 de données à caractère personnel, car ils ne déterminent pas conjointement les finalités de la collecte et le traitement ultérieur ou complémentaire des données à caractère personnel pour les finalités de YourPerfectJob à ce stade du traitement. Le CEPD aimerait rappeler que l'analyse des rôles et responsabilités doit être effectuée au cas par cas et que la conclusion dans cet exemple précis est sans préjudice de tout autre travail pouvant être réalisé par le CEPD sur les API. La situation serait bien évidemment différente si le fournisseur de médias sociaux, en plus de rendre accessibles les données à caractère personnel, participait également à la détermination de la finalité poursuivie par YourPerfectJob. Quoi qu'il en soit, le contrôle conjoint continue d'exister entre le cibleur et le fournisseur de médias sociaux en ce qui concerne le recours à un ciblage à partir d'une liste.

126. Tandis que les activités de traitement du fournisseur de médias sociaux dans l'exemple 14 ne relèvent pas du traitement portant sur des catégories particulières de données au sens de l'article 9 du RGPD, le fournisseur de médias sociaux est responsable d'intégrer les garanties nécessaires dans le traitement pour satisfaire les exigences du RGPD et protéger les droits des personnes concernées en accord avec les articles 24 et 25 du RGPD.

8.2 Exception au titre de l'article 9, paragraphe 2, des catégories particulières de données manifestement rendues publiques

127. L'article 9, paragraphe 2, point e), du RGPD autorise les traitements portant sur des catégories particulières de données lorsque les données ont été manifestement rendues publiques par la personne concernée. Le terme «manifestement» suppose que cette exception ne peut être invoquée que de façon très restrictive. Le CEPD fait remarquer que la présence d'un unique élément ne suffit pas toujours pour établir que les données ont été «manifestement» rendues publiques par la personne concernée. En pratique, il se peut qu'une combinaison des éléments suivants ou d'autres éléments doive 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 s'avérer pertinents pour la réalisation de cette évaluation:

i) les paramètres par défaut de la plateforme de médias sociaux (afin de savoir si la personne concernée a effectué une action spécifique pour changer ces paramètres de confidentialité par défaut en faveur de paramètres publics); ou

ii) la nature de la plateforme de médias sociaux [afin de savoir si la plateforme est intrinsèquement liée à l'idée de mettre la personne concernée en relation avec des connaissances proches ou de créer des relations intimes (comme c'est le cas des plateformes de rencontre en ligne), ou si elle cherche à offrir un champ plus large de relations interpersonnelles, par exemple des relations professionnelles, ou encore s'il s'agit d'une plateforme de microblogging ou de partage de médias, d'une plateforme sociale pour partager des avis en ligne, etc.]; ou

iii) l'accessibilité de la page où les données sensibles sont publiées (afin de savoir si les informations sont publiquement accessibles ou si, par exemple, la création d'un compte est nécessaire pour pouvoir accéder aux informations); ou

iv) la visibilité de l'avertissement signalant à la personne concernée la nature publique des informations qu'elle publie (afin de savoir si, par exemple, un bandeau continu apparaît sur la page ou si le bouton de validation d'une publication informe la personne concernée que les informations en question seront rendues publiques, etc.); ou

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

128. Le CEPD fait remarquer que la présence d'un unique élément ne suffit pas toujours pour établir que les données ont été «manifestement» rendues publiques par la personne concernée. En pratique, il se peut qu'une combinaison de ces éléments ou d'autres doive 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 15:

M. Jansen a ouvert un compte sur une plateforme sociale de microblogging. En complétant son profil, il a indiqué qu'il était homosexuel. Conservateur, il a choisi de rejoindre des groupes conservateurs, étant pleinement informé que les messages échangés sur la plateforme relèvent du domaine public (la plateforme l'en a informé lors de son inscription). Un parti politique conservateur souhaite cibler des personnes partageant les mêmes affiliations politiques et la même orientation sexuelle que M. Jansen en utilisant les outils de ciblage du média social.

129. L'orientation sexuelle des membres étant par défaut «privée» et compte tenu du fait que M. Jansen n'a pas choisi de rendre cette information publique, elle ne peut être considérée comme ayant été manifestement rendue publique. De plus, les données concernant son affiliation politique n'ont pas été rendues manifestement publiques, malgré i) la nature de la plateforme sociale de microblogging, qui a pour fonction de partager des informations au grand public, et ii) le fait qu'il a été informé de la nature publique des messages qu'il publie sur les forums. En outre, bien qu'il ait rejoint des forums publics en rapport avec le conservatisme, il ne peut être ciblé sur la base de ces données sensibles, car c'est la plateforme de médias sociaux qui déduit l'affiliation politique de M. Jansen alors que ce dernier n'avait pas l'intention spécifique de rendre cette information manifestement publique, d'autant plus que cette déduction peut s'avérer erronée. Il ne peut donc pas être ciblé sur la base de données sur son affiliation politique. En d'autres termes, les circonstances de chaque cas spécifique doivent être prises en compte au moment d'évaluer si les données ont été manifestement rendues publiques par la personne concernée[104].

9 CONTRÔLE CONJOINT ET RESPONSABILITÉ

9.1 Accord des responsables conjoints du traitement et détermination des responsabilités (article 26 du RGPD)

130. L'article 26, paragraphe 1, du RGPD exige des responsables conjoints du traitement qu'ils définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, notamment en ce qui concerne, comme expliqué précédemment, les obligations de transparence.

131. En termes de champ d'application, le CEPD considère que l'accord 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 accord uniquement superficiel et incomplet, les cibleurs et fournisseurs de médias sociaux manqueraient à leurs obligations au titre de l'article 26 du RGPD.

Dans l'exemple 4, par exemple, l'accord devrait couvrir le traitement total des données à caractère personnel en cas de contrôle conjoint, c'est-à-dire de la collecte des données à caractère personnel dans le contexte de la consultation par M. Schmidt du site web BestBags.com à l'aide de pixels espions, jusqu'à l'affichage de la publicité sur sa page de médias sociaux ainsi qu'un signalement ultérieur en rapport avec la campagne de ciblage.

[104] Le GT29 a clarifié dans son avis sur certains aspects clés de la directive en matière de protection des données dans le domaine répressif (WP 258, 29/11/2017, p. 10) que l'expression «manifestement rendues publiques par la personne concernée» doit être interprétée comme laissant entendre que la personne concernée a conscience que les données respectives seront rendues publiques, donc accessibles à tout le monde, y compris aux autorités; par conséquent, «en cas de doute, une interprétation étroite devrait être appliquée...».

132. Afin d'élaborer un accord complet, le fournisseur de médias sociaux et le cibleur doivent avoir connaissance des opérations particulières de traitement des données qui ont lieu et disposer d'informations suffisamment détaillées à ce sujet. L'accord entre le cibleur et le fournisseur de médias sociaux devrait dès lors contenir (ou faire référence à) toutes les informations nécessaires pour permettre aux deux parties de satisfaire leurs obligations au titre du RGPD, y compris leur obligation de respecter les principes de l'article 5, paragraphe 1, du RGPD ainsi que leur obligation de démontrer leur conformité en vertu de l'article 5, paragraphe 2, du RGPD.

133. Si, par exemple, le responsable du traitement envisage de s'appuyer sur l'article 6, paragraphe 1, point f), du RGPD comme base juridique, il est notamment nécessaire de connaître l'étendue du traitement de données pour pouvoir apprécier si les intérêts poursuivis par le ou les responsables du traitement prévalent ou non sur les intérêts ou les libertés et droits fondamentaux de la personne concernée En l'absence d'information suffisante sur le traitement, une telle appréciation ne peut être réalisée. L'importance d'inclure ou de référencer les informations nécessaires dans le contexte d'un accord commun ne peut être surestimée, en particulier lorsque l'une des parties possède de façon quasi exclusive les connaissances et l'accès aux informations nécessaires au respect du RGPD par les deux parties.

> À titre d'exemple, dans l'exemple 1, lorsque l'entreprise X évalue si elle peut s'appuyer ou non sur l'intérêt légitime comme base juridique pour cibler les hommes âgés de 30 à 45 ans ayant indiqué être célibataires, elle doit avoir accès à suffisamment d'informations concernant le traitement exécuté par la plateforme de médias sociaux, y compris par exemple en ce qui concerne les mesures supplémentaires (comme le droit d'exprimer une objection préalable) mises en place par cette dernière, pour garantir que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent pas sur les intérêts légitimes.

134. Pour garantir que les droits de la personne concernée peuvent être pris en compte de manière effective, le CEPD part du principe que l'objet du traitement et la base juridique correspondante devraient également apparaître dans l'accord commun entre les cibleurs et les fournisseurs de médias sociaux qui sont responsables conjoints du traitement. Bien que le RGPD n'empêche pas les responsables conjoints du traitement d'utiliser différentes bases juridiques pour les différentes opérations de traitement 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. De fait, si chaque étape du traitement relève d'une base juridique différente, il sera impossible pour la personne concernée d'exercer ses droits (par exemple, une étape relèverait du droit à la portabilité des données tandis qu'une autre étape relèverait du droit d'opposition).

135. En tant que responsables du traitement, le cibleur et le fournisseur de médias sociaux sont tous deux responsables de garantir le respect du principe de limitation de la finalité et devraient par conséquent intégrer des dispositions adéquates à cette fin dans l'accord commun.

Par exemple, si le cibleur souhaite exploiter les données à caractère personnel que la personne concernée lui a fournies en vue d'un ciblage sur les médias sociaux, il doit prendre des mesures appropriées pour s'assurer 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 la personne concernée ait accordé son consentement valable en vertu de l'article 6, paragraphe 4, du RGPD.

Dans l'exemple 3, la banque X devrait s'assurer que l'accord commun conclu avec la plateforme de médias sociaux comprend des dispositions appropriées pour garantir que l'adresse électronique de M. Lopez ne sera pas utilisée sans le consentement de ce dernier à d'autres fins que l'envoi d'offres en rapport avec les services bancaires dont il bénéficie déjà.

De même, le fournisseur de médias sociaux doit garantir que l'utilisation de données à des fins de ciblage par les cibleurs respecte les principes de limitation de la finalité, de transparence et de licéité.

136. Le cibleur et le fournisseur de médias sociaux devraient tenir compte d'autres obligations dans le contexte de leur accord commun, notamment les suivantes: les autres principes généraux en matière de protection des données prévus par l'article 5 du RGPD, la sécurité du traitement, la protection des données dès la conception et la protection des données par défaut, les notifications et communications des violations de données à caractère personnel, les analyses d'impact relatives à la protection des données, le recours à des sous-traitants et les transferts vers des pays tiers.

Dans l'exemple 13, par exemple, l'accord commun devrait chercher à établir la façon dont les responsables du traitement devraient réaliser une AIPD et garantir qu'un échange pertinent de connaissances a lieu. En d'autres termes, le parti politique Letschangetheworld devrait s'assurer de disposer de suffisamment d'informations, notamment sur les mesures de sécurité mises en place par la plateforme de médias sociaux, quand une AIPD est effectuée.

137. Enfin, l'accord commun entre le fournisseur de médias sociaux et le cibleur doit contenir des informations spécifiques sur la façon dont leurs obligations au titre du RGPD doivent être satisfaites. En l'absence de clarté quant à la manière dont leurs obligations doivent être satisfaites, en particulier en ce qui concerne les droits de la personne concernée, le cibleur et le fournisseur des médias sociaux seront réputés agir en violation de l'article 26, paragraphe 1, du RGPD. En outre, dans un tel cas, les deux responsables (conjoints) du traitement n'auront pas mis en place les mesures techniques et organisationnelles nécessaires afin de garantir et de pouvoir démontrer que le traitement est réalisé conformément au RGPD et auront partant manqué à leurs obligations au titre de l'article 5, paragraphe 2, et de l'article 24.

9.2 Niveaux de responsabilité

138. Le CEPD observe que les cibleurs souhaitant utiliser les outils de ciblage fournis par un fournisseur de médias sociaux peuvent être confrontés à la nécessité d'adhérer à des accords prédéfinis, sans possibilité de les négocier ou d'y apporter des modifications (conditions de type «à prendre ou à laisser»). Le CEPD estime qu'une telle situation n'annule 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 envers ses obligations au titre du RGPD. Les parties à l'accord commun sont également tenues de garantir que la

répartition des responsabilités reflète dûment leurs rôles respectifs et leurs relations vis-à-vis des personnes concernées, de manière pratique, sincère et transparente.

139. Il est important de souligner qu'un accord en vertu de l'article 26 du RGPD ne peut prévaloir sur les obligations légales qui incombent à un responsable (conjoint) du traitement. Tandis que les responsables conjoints du traitement, en accord avec l'article 26 du RGPD, «*définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences*» du RGPD, chaque responsable du traitement demeure, en 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 RGPD, notamment le principe de licéité énoncé à l'article 5, paragraphe 1, point a), du RGPD.

140. Cependant, le degré de responsabilité du cibleur et du fournisseur de médias sociaux à l'égard de certaines obligations spécifiques peut varier. Dans l'arrêt Wirtschaftsakademie, la CJUE a noté que «*l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. [...] ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.*» [105]

141. Autrement dit, bien que les responsables conjoints du traitement soient tous deux responsables du respect de leurs obligations au titre du RGPD et même si la personne concernée peut exercer ses droits contre chacun des responsables du traitement, leur niveau de responsabilité doit être évalué au regard de leur rôle réel dans le traitement. Dans l'arrêt Google Spain, la CJUE a clarifié qu'un responsable du traitement doit assurer, «*dans le cadre de ses responsabilités, de ses compétences et de ses possibilités*», que le traitement des données à caractère personnel satisfait aux exigences du droit européen de la protection des données.[106]

142. En ce qui concerne l'évaluation du niveau de responsabilité des cibleurs et des fournisseurs de médias sociaux, plusieurs facteurs peuvent s'avérer pertinents, notamment leur capacité à influencer le traitement d'un point de vue pratique, mais aussi les connaissances réelles ou constructives de chacun des responsables conjoints du traitement. Il est également important d'indiquer clairement le stade du traitement auquel le cibleur et le fournisseur de médias sociaux sont responsables du traitement, dans quelle mesure et selon quel degré[107].

Dans l'exemple 1, l'entreprise X met au point une campagne publicitaire afin que ses annonces apparaissent sur la plateforme de médias sociaux à destination des utilisateurs correspondant aux critères de ciblage spécifiques définis. Toutefois, bien qu'elle définisse les paramètres de la campagne publicitaire, elle ne collecte pas de données à caractère personnel ni n'y a accès et elle n'est pas en contact direct avec les personnes concernées. Chacun de ces éléments peut s'avérer pertinent au moment d'évaluer le niveau (ou «degré») ou la responsabilité du cibleur et du fournisseur de médias sociaux en cas d'infraction avérée du RGPD (par exemple, en cas de manque de transparence à l'égard de la personne concernée ou d'incapacité à assurer la licéité du traitement). Comme indiqué précédemment, cependant, les deux parties sont tenues de mettre en

[105] Arrêt de la CJUE du 5 juin 2018, Wirtschaftsakademie, C-210/16, point 43.
[106] Voir également l'arrêt de la CJUE, C-131/12, Google Spain («responsabilités, compétences et possibilités»).
[107] Le CEPD considère que dans une pluralité de cas, une évaluation basée sur les critères susmentionnés (par exemple, les données utilisées pour établir les critères de ciblage, la correspondance de la personne concernée, le recueil du consentement) conduira probablement à la conclusion que le fournisseur de médias sociaux a la plus forte influence factuelle sur le traitement et donc un plus haut degré de responsabilité, selon le mécanisme de ciblage spécifique utilisé.

œuvre des mesures appropriées pour satisfaire aux exigences du RGPD et protéger les droits des personnes concernées contre toute forme illicite de traitement.

Dans l'exemple 3, dans lequel un ciblage est effectué à partir d'une liste, la situation diffère légèrement de l'exemple 1. En effet, dans l'exemple 3, la banque avait initialement collecté les données à caractère personnel et les avait 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 processus de traitement des données. Chacun de ces éléments devrait être pris en compte au moment d'évaluer le niveau de responsabilité de chaque acteur et devrait être dûment reflété dans les conditions de l'accord commun.

De façon similaire, dans l'exemple 4, en cas de ciblage à partir de pixels, il convient de tenir compte du fait que le gestionnaire du site web permet la transmission des données à caractère personnel au fournisseur de médias sociaux. C'est effectivement le site web «BestBags.com» qui intègre des pixels espions sur son site, de manière à pouvoir cibler M. Schmidt, bien que ce dernier ait décidé de ne pas faire d'achat[108]. Le site web participe donc activement à la collecte et à la transmission des données. En tant que responsable conjoint du traitement, néanmoins, le fournisseur de médias sociaux assume également l'obligation de mettre en œuvre des mesures appropriées pour satisfaire aux exigences du RGPD et protéger les droits des personnes concernées contre toute forme illicite de traitement. Dans ce cas, si le consentement de la personne concernée est demandé, les responsables conjoints du traitement doivent convenir de la manière dont le consentement est recueilli dans la pratique.

143. Lorsqu'il s'agit d'évaluer le niveau de responsabilité du fournisseur de médias sociaux, le CEPD observe que plusieurs mécanismes de ciblage s'appuient sur le profilage et/ou d'autres activités de traitement entreprises précédemment par le fournisseur de médias sociaux. C'est le fournisseur de médias sociaux qui décide de traiter les données à caractère personnel 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 certaines décisions indépendamment concernant le traitement, tels que les catégories de données à traiter, les critères de ciblage à proposer et les personnes qui auront accès aux données à caractère personnel (et les types de données) traitées dans le cadre d'une campagne de ciblage particulière. De telles activités de traitement doivent également être conformes au RGPD, avant l'offre de tout service de ciblage.

144. Les exemples mentionnés aux paragraphes précédents témoignent de l'importance de répartir clairement les responsabilités dans l'accord des responsables conjoints du traitement, entre les fournisseurs de médias sociaux et les cibleurs. Bien que les conditions de l'accord devraient quoi qu'il en soit refléter le niveau de responsabilité de chaque acteur, un accord complet reflétant dûment le rôle et les capacités de chaque partie est nécessaire, non seulement pour satisfaire à l'article 26 du RGPD, mais aussi pour satisfaire aux autres règles et principes du RGPD.

145. Enfin, le CEPD remarque que, dans la mesure où les conditions de l'accord commun entre le fournisseur de médias sociaux et le cibleur ne sont pas contraignantes pour les autorités de contrôle, ces dernières peuvent exercer leurs compétences et pouvoirs vis-à-vis de chaque responsable conjoint du

[108] En outre, BestBags.com ayant intégré les pixels espions de médias sociaux sur son site web, il est également responsable de satisfaire aux exigences de la directive «vie privée et communications électroniques» à l'égard de cet outil qui, compte tenu du fait que les pixels facilitent également le traitement de données à caractère personnel, joue aussi un rôle important dans la détermination du niveau de responsabilité.

traitement, à condition que le responsable conjoint du traitement en question soit soumis à la compétence de cette autorité de contrôle.