ARRÊT DE LA COUR (grande chambre)
4 juillet 2023 (*)
Table des matières

Le cadre juridique
Le droit de l'Union
Le règlement (CE) n o 1/2003
Le RGPD
Le droit allemand
Le litige au principal et les questions préjudicielles
Sur les questions préjudicielles
Sur les première et septième questions
Sur la deuxième question
Sur la deuxième question, sous a)
Sur la deuxième question, sous b)
Sur les troisième à cinquième questions
Observations liminaires
Sur les troisième et quatrième questions
Sur la cinquième question
Sur la sixième question
Sur les dépens

« Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement de données à caractère personnel – Règlement (UE) 2016/679 – Réseaux sociaux en ligne – Abus de position dominante par l'opérateur d'un tel réseau – Abus consistant dans le traitement de données à caractère personnel des utilisateurs de ce réseau prévu par les conditions générales d'utilisation de celui-ci – Compétences d'une autorité de la concurrence d'un État membre pour constater la non-conformité de ce traitement à ce règlement – Articulation avec les compétences des autorités nationales chargées du contrôle de la protection des données personnelles – Article 4, paragraphe 3, TUE – Principe de coopération loyale – Article 6, paragraphe 1, premier alinéa, sous a) à f), du règlement 2016/679 – Licéité du traitement – Article 9, paragraphes 1 et 2 – Traitement portant sur des catégories particulières de données à caractère personnel – Article 4, point 11 – Notion de "consentement" »

Dans l'affaire C-252/21,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne), par décision du 24 mars 2021, parvenue à la Cour le 22 avril 2021, dans la procédure

Meta Platforms Inc., anciennement Facebook Inc.,
Meta Platforms Ireland Ltd, anciennement Facebook Ireland Ltd,
Facebook Deutschland GmbH

contre

Bundeskartellamt,

en présence de :

Verbraucherzentrale Bundesverband eV,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. L. Bay Larsen, vice-président, M^mes^ A. Prechal, K. Jürimäe, MM. C. Lycourgos, M. Safjan, M^me^ L. S. Rossi (rapporteure), M. D. Gratsias et M^me^ M. L. Arastey Sahún, présidents de chambre, MM. J.-C. Bonichot, S. Rodin, F. Biltgen, M. Gavalec, Z. Csehi et M^me^ O. Spineanu-Matei, juges,

avocat général : M. A. Rantos,

greffier : M. D. Dittert, chef d'unité,

vu la procédure écrite et à la suite de l'audience du 10 mai 2022,

considérant les observations présentées :

pour Meta Platforms Inc., anciennement Facebook Inc., Meta Platforms Ireland Ltd, anciennement Facebook Ireland Ltd, et Facebook Deutschland GmbH, par M^es^ M. Braun, M. Esser, L. Hesse, J. Höft et H.-G. Kamann,

Rechtsanwälte,

pour le Bundeskartellamt, par MM. J. Nothdurft, K. Ost, M^mes^ I. Sewczyk et J. Topel, en qualité d'agents,

pour Verbraucherzentrale Bundesverband eV, par M^e^ S. Louven, Rechtsanwalt,
pour le gouvernement allemand, par MM. J. Möller et P.-L. Krüger, en qualité d'agents,
pour le gouvernement tchèque, par MM. M. Smolek et J. Vláčil, en qualité d'agents,

pour le gouvernement italien, par M^me^ G. Palmieri, en qualité d'agent, assistée de MM. E. De Bonis et P. Gentili, avvocati dello Stato,

pour le gouvernement autrichien, par M. A. Posch, M^me^ J. Schmoll et M. G. Kunnert, , en qualité d'agents,
pour la Commission européenne, par MM. F. Erlbacher, H. Kranenborg et G. Meessen, en qualité d'agents,
ayant entendu l'avocat général en ses conclusions à l'audience du 20 septembre 2022,
rend le présent

Arrêt

La demande de décision préjudicielle porte sur l'interprétation de l'article 4, paragraphe 3, TUE ainsi que de l'article 6, paragraphe 1, l'article 9, paragraphes 1 et 2, l'article 51, paragraphe 1, et l'article 56, paragraphe 1, du règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1, et rectificatif JO 2018, L 127, p. 2, ci-après le « RGPD »).

Cette demande a été présentée dans le cadre d'un litige opposant Meta Platforms Inc., anciennement Facebook Inc., Meta Platforms Ireland Ltd, anciennement Facebook Ireland Ltd, et Facebook Deutschland GmbH au Bundeskartellamt (autorité fédérale de la concurrence, Allemagne) au sujet de la décision de ce dernier d'interdire à ces sociétés de procéder au traitement de certaines données à caractère personnel prévu par les conditions générales d'utilisation du réseau social Facebook (ci-après les « conditions générales »).

Le cadre juridique

Le droit de l'Union

Le règlement (CE) n^o^ 1/2003

L'article 5 du règlement (CE) n^o^ 1/2003 du Conseil, du 16 décembre 2002, relatif à la mise en œuvre des règles de concurrence prévues aux articles [101 et 102 TFUE] (JO 2003, L 1, p. 1), intitulé « Compétence des autorités de concurrence des États membres », prévoit :

« Les autorités de concurrence des États membres sont compétentes pour appliquer les articles [101 et 102 TFUE] dans des cas individuels. À cette fin, elles peuvent, agissant d'office ou saisies d'une plainte, adopter les décisions suivantes :

ordonner la cessation d'une infraction,
ordonner des mesures provisoires,
accepter des engagements,
infliger des amendes, astreintes ou toute autre sanction prévue par leur droit national.

Lorsqu'elles considèrent, sur la base des informations dont elles disposent, que les conditions d'une interdiction ne sont pas réunies, elles peuvent également décider qu'il n'y a pas lieu pour elles d'intervenir. »

Le RGPD

Les considérants 1, 4, 38, 42, 43, 46, 47, 49 et 51 du RGPD énoncent :

La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la [c]harte des droits fondamentaux de l'Union européenne (ci-après la "Charte") et l'article 16, paragraphe 1, [TFUE] disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

[...]

Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

[...]

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, 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. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

[...]

Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement. [...] Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. Le consentement

ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

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

[...]

Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique. Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine.

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

[...]

Le traitement de données à caractère personnel dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations, c'est-à-dire la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données à caractère personnel conservées ou transmises, ainsi que la sécurité des services connexes offerts ou rendus accessibles via ces réseaux et systèmes, [...] constitue un intérêt légitime du responsable du traitement concerné.

Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits. Ces données à caractère personnel devraient comprendre les données à caractère personnel qui révèlent l'origine raciale ou ethnique, étant entendu que l'utilisation de l'expression "origine raciale" dans le présent règlement n'implique pas que l'Union [européenne] adhère à des théories tendant à établir l'existence de races humaines distinctes. Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. De telles données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans des cas spécifiques prévus par le présent règlement, compte tenu du fait que le droit d'un État membre peut prévoir des dispositions spécifiques relatives à la protection des données visant à adapter l'application des règles du présent règlement en vue de respecter une obligation légale ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Outre les exigences spécifiques applicables à ce traitement, les principes généraux et les autres règles du présent règlement devraient s'appliquer, en particulier en ce qui concerne les conditions de licéité du traitement. Des dérogations à l'interdiction générale de traiter ces catégories particulières de données à caractère personnel devraient être explicitement prévues, entre autres lorsque la personne concernée donne son consentement explicite ou pour répondre à des besoins spécifiques, en particulier lorsque le traitement est effectué dans le cadre d'activités légitimes de certaines associations ou fondations ayant pour objet de permettre l'exercice des libertés fondamentales. »

L'article 4 de ce règlement prévoit :

« Aux fins du présent règlement, on entend par :

"données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; [...]

"traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la

consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;
[...]
"responsable du traitement", la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
[...]
"consentement" de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ;

"traitement transfrontalier",
un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou
un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ;

L'article 5 dudit règlement, intitulé « Principes relatifs au traitement des données à caractère personnel », dispose, à ses paragraphes 1 et 2 :
« 1. Les données à caractère personnel doivent être :
traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; [...]
adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité). »
L'article 6 du même règlement, intitulé « Licéité du traitement », est libellé comme suit :
« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :
la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.
[...]
3. Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :
le droit de l'Union, ou
le droit de l'État membre auquel le responsable du traitement est soumis.
[...]
[...] Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. »
L'article 7 du RGPD, intitulé « Conditions applicables au consentement », prévoit :
« 1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
[...]
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat. »
L'article 9 de ce règlement, intitulé « Traitement portant sur des catégories particulières de données à caractère personnel », dispose :

« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ;

le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

[...] »

L'article 13 dudit règlement, relatif aux « [i]nformations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée », prévoit, à son paragraphe 1, ce qui suit :

« Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

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

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

Le chapitre VI du RGPD, relatif aux « [a]utorités de contrôle indépendantes », comprend les articles 51 à 59 de ce règlement.

L'article 51 dudit règlement, intitulé « Autorité de contrôle », prévoit, à ses paragraphes 1 et 2 :

« 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union [...]

2. Chaque autorité de contrôle contribue à l'application cohérente du présent règlement dans l'ensemble de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission [européenne] conformément au chapitre VII. »

Aux termes de l'article 55 du même règlement, intitulé « Compétence » :

« 1. Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève.

2. Lorsque le traitement est effectué par des autorités publiques ou des organismes privés agissant sur la base de l'article 6, paragraphe 1, point c) ou e), l'autorité de contrôle de l'État membre concerné est compétente. Dans ce cas, l'article 56 n'est pas applicable. »

L'article 56 du RGPD, intitulé « Compétence de l'autorité de contrôle chef de file », énonce, à son paragraphe 1 :

« Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60. »

L'article 57 de ce règlement, intitulé « Missions », dispose, à son paragraphe 1 :

« Sans préjudice des autres missions prévues au titre du présent règlement, chaque autorité de contrôle, sur son territoire :

contrôle l'application du présent règlement et veille au respect de celui-ci ;

[...]

coopère avec d'autres autorités de contrôle, y compris en partageant des informations, et fournit une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente du présent règlement et des mesures prises pour en assurer le respect ;

[...] »

L'article 58 dudit règlement fixe, à son paragraphe 1, la liste des pouvoirs d'enquête dont dispose chaque autorité de contrôle et précise, à son paragraphe 5, que « [c]haque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement ».

La section 1, intitulée « Coopération », du chapitre VII du RGPD, lui-même intitulé « Coopération et cohérence », comprend les articles 60 à 62 de ce règlement. L'article 60, relatif à la « [c]oopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées », prévoit, à son paragraphe 1 :

« L'autorité de contrôle chef de file coopère avec les autres autorités de contrôle concernées conformément au présent article en s'efforçant de parvenir à un consensus. L'autorité de contrôle chef de file et les autorités de contrôle concernées échangent toute information utile. »

L'article 61 du RGPD, intitulé « Assistance mutuelle », énonce, à son paragraphe 1 :

« Les autorités de contrôle se communiquent les informations utiles et se prêtent mutuellement assistance en vue de mettre en œuvre et d'appliquer le présent règlement de façon cohérente, et mettent en place des mesures pour coopérer efficacement. L'assistance mutuelle concerne notamment les demandes d'informations et les mesures de contrôle, telles que les demandes d'autorisation et de consultation préalables, les inspections et les enquêtes. »

L'article 62 de ce règlement, intitulé « Opérations conjointes des autorités de contrôle », prévoit, à ses paragraphes 1 et 2 :

« 1. Les autorités de contrôle mènent, le cas échéant, des opérations conjointes, y compris en effectuant des enquêtes conjointes et en prenant des mesures répressives conjointes, auxquelles participent des membres ou des agents des autorités de contrôle d'autres États membres.

2. Lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ou si un nombre important de personnes concernées dans plusieurs États membres sont susceptibles d'être sensiblement affectées par des opérations de traitement, une autorité de contrôle de chacun de ces États membres a le droit de participer aux opérations conjointes. [...] »

La section 2, intitulée « Cohérence », du chapitre VII du RGPD comprend les articles 63 à 67 de ce règlement. L'article 63, intitulé « Mécanisme de contrôle de la cohérence », est libellé comme suit :

« Afin de contribuer à l'application cohérente du présent règlement dans l'ensemble de l'Union, les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section. »

Aux termes de l'article 64, paragraphe 2, de ce règlement :

« Toute autorité de contrôle, le président du comité [européen de la protection des données] ou la Commission peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité [européen de la protection des données] en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle conformément à l'article 61 ou les obligations relatives aux opérations conjointes conformément à l'article 62. »

L'article 65 dudit règlement, intitulé « Règlement des litiges par le comité », prévoit, à son paragraphe 1 :

« En vue d'assurer l'application correcte et cohérente du présent règlement dans les cas d'espèce, le comité [européen de la protection des données] adopte une décision contraignante dans les cas suivants :

lorsque, dans le cas visé à l'article 60, paragraphe 4, une autorité de contrôle concernée a formulé une objection pertinente et motivée à l'égard d'un projet de décision de l'autorité de contrôle chef de file et que l'autorité de contrôle chef de file n'a pas donné suite à l'objection ou a rejeté cette objection au motif qu'elle n'est pas pertinente ou motivée. La décision contraignante concerne toutes les questions qui font l'objet de l'objection pertinente et motivée, notamment celle de savoir s'il y a violation du présent règlement ;

lorsqu'il existe des points de vue divergents quant à l'autorité de contrôle concernée qui est compétente pour l'établissement principal ;

Le droit allemand

L'article 19, paragraphe 1, du Gesetz gegen Wettbewerbsbeschränkungen (loi contre les restrictions à la concurrence), dans sa version publiée le 26 juin 2013 (BGBl. 2013 I, p. 1750, 3245), modifiée en dernier lieu par l'article 2 de la loi du 16 juillet 2021 (BGBl. 2021 I, p. 2959) (ci-après le « GWB »), dispose :

« L'abus d'une position dominante sur le marché par une ou plusieurs entreprises est interdite. »

Aux termes de l'article 32, paragraphe 1, du GWB :

« L'autorité de la concurrence peut imposer aux entreprises ou associations d'entreprises de mettre fin à une infraction à une disposition de la présente partie ou aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. »

L'article 50f du GWB prévoit, à son paragraphe 1 :

« Les autorités de concurrence, les autorités de régulation, le responsable fédéral de la protection des données et de la liberté de l'information, les responsables régionaux de la protection des données ainsi que les autorités compétentes au sens de l'article 2 de l'EU-Verbraucherschutzdurchführungsgesetz [(loi sur la mise en œuvre du droit de la protection des consommateurs de l'Union européenne)] peuvent, indépendamment de la procédure choisie, échanger entre eux des informations, y compris des données à caractère personnel et des secrets commerciaux et d'affaires, dans la mesure où cela est nécessaire à l'accomplissement de leurs missions respectives ainsi qu'utiliser ces informations dans le cadre de leurs procédures. [...] »

Le litige au principal et les questions préjudicielles

Meta Platforms Ireland gère l'offre du réseau social en ligne Facebook dans l'Union et promeut, notamment à l'adresse www.facebook.com, des services qui sont gratuits pour les utilisateurs privés. D'autres entreprises du groupe Meta proposent, dans l'Union, d'autres services en ligne dont Instagram, WhatsApp, Oculus et – jusqu'au 13 mars 2020 – Masquerade.

Le modèle économique du réseau social en ligne Facebook se fonde sur le financement par la publicité en ligne, qui est faite sur mesure pour les utilisateurs individuels du réseau social en fonction notamment de leurs attitudes de consommation, de leurs intérêts, de leur pouvoir d'achat et de leur situation personnelle. Une telle publicité est techniquement rendue possible par l'établissement automatisé de profils détaillés des utilisateurs du réseau et des services en ligne proposés au niveau du groupe Meta. À cette fin, outre les données que ces utilisateurs fournissent directement lors de leur inscription aux services en ligne concernés, d'autres données relatives auxdits utilisateurs et à leurs appareils sont également collectées, à l'intérieur et à l'extérieur de ce réseau social et des services en ligne fournis par le groupe Meta, et reliées à leurs différents comptes d'utilisateur. L'aperçu global de ces données permet de tirer des conclusions détaillées sur les préférences et les intérêts de ces mêmes utilisateurs.

Pour le traitement desdites données, Meta Platforms Ireland se fonde sur le contrat d'utilisation auquel adhèrent les utilisateurs du réseau social Facebook par l'activation du bouton « s'inscrire » et par lequel ceux-ci acceptent les

conditions générales établies par cette société. L'acceptation de ces conditions est nécessaire pour pouvoir utiliser le réseau social Facebook. S'agissant du traitement des données à caractère personnel, les conditions générales renvoient aux politiques d'utilisation des données et des *cookies* fixées par ladite société. En vertu de ces dernières, Meta Platforms Ireland collecte des données relatives aux utilisateurs et aux appareils, portant sur les activités des utilisateurs à l'intérieur et à l'extérieur du réseau social, et met ces données en relation avec les comptes Facebook des utilisateurs concernés. Quant à ces dernières données, relatives aux activités en dehors du réseau social (ci-après également les « données *off* Facebook »), il s'agit, d'une part, des données concernant la consultation de pages Internet et d'applications tierces, qui sont reliées à Facebook à travers des interfaces de programmation – les « Outils Facebook Business » – et, d'autre part, des données relatives à l'utilisation des autres services en ligne appartenant au groupe Meta, dont Instagram, WhatsApp, Oculus et – jusqu'au 13 mars 2020 – Masquerade.

L'autorité fédérale de la concurrence a engagé une procédure contre Meta Platforms, Meta Platforms Ireland et Facebook Deutschland, à l'issue de laquelle, par décision du 6 février 2019, fondée sur l'article 19, paragraphe 1, et l'article 32 du GWB, il leur a fait, en substance, interdiction de subordonner, dans les conditions générales, l'utilisation du réseau social Facebook par des utilisateurs privés résidant en Allemagne au traitement de leurs données *off* Facebook et de procéder, sans leur consentement, au traitement de ces données sur la base des conditions générales alors en vigueur. En outre, il leur a imposé d'adapter ces conditions générales de sorte qu'il en ressorte clairement que lesdites données ne seront ni collectées, ni mises en relation avec les comptes d'utilisateurs Facebook, ni utilisées sans le consentement de l'utilisateur concerné, et a clarifié le fait qu'un tel consentement n'est pas valide lorsque celui-ci constitue une condition pour l'utilisation du réseau social.

L'autorité fédérale de la concurrence a motivé sa décision par le fait que le traitement des données des utilisateurs concernés, tel que prévu par les conditions générales et mis en œuvre par Meta Platforms Ireland, constituait une exploitation abusive de la position dominante de cette société sur le marché des réseaux sociaux en ligne pour les utilisateurs privés en Allemagne, au sens de l'article 19, paragraphe 1, du GWB. En particulier, selon l'autorité fédérale de la concurrence, ces conditions générales, en tant qu'émanation de cette position dominante, seraient abusives dès lors que le traitement des données *off* Facebook qu'elles prévoient ne serait pas conforme aux valeurs sous-tendant le RGPD et, notamment, ne pourrait être justifié au regard de l'article 6, paragraphe 1, et de l'article 9, paragraphe 2, de ce règlement.

Le 11 février 2019, Meta Platforms, Meta Platforms Ireland et Facebook Deutschland ont introduit un recours contre la décision de l'autorité fédérale de la concurrence devant l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf, Allemagne).

Le 31 juillet 2019, Meta Platforms Ireland a introduit des nouvelles conditions générales indiquant expressément que l'utilisateur, au lieu de payer pour l'utilisation des produits Facebook, déclare consentir aux annonces publicitaires.

En outre, depuis le 28 janvier 2020, Meta Platforms propose, au niveau mondial, l'« *Off-Facebook-Activity* », laquelle permet aux utilisateurs du réseau social Facebook de recevoir un résumé des informations les concernant, que les sociétés du groupe Meta obtiennent en relation avec leurs activités sur d'autres pages Internet et applications, et de dissocier, s'ils le souhaitent, ces données de leur compte Facebook.com, tant pour le passé que pour le futur.

L'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf) nourrit des doutes, en premier lieu, quant à la possibilité pour des autorités nationales de la concurrence de contrôler, dans le cadre de l'exercice de leurs compétences, la conformité d'un traitement de données à caractère personnel aux exigences formulées dans le RGPD ; en deuxième lieu, quant à la possibilité pour un opérateur d'un réseau social en ligne de traiter les données à caractère personnel sensibles de la personne concernée, au sens de l'article 9, paragraphes 1 et 2, de ce règlement ; en troisième lieu, quant à la licéité du traitement des données à caractère personnel de l'utilisateur concerné de la part d'un tel opérateur, conformément à l'article 6, paragraphe 1, dudit règlement et, en quatrième lieu, quant à la validité, au regard de l'article 6, paragraphe 1, premier alinéa, sous a), et de l'article 9, paragraphe 2, sous a), du même règlement, du consentement donné à une entreprise ayant une position dominante sur le marché national des réseaux sociaux en ligne, aux fins d'un tel traitement.

Dans ce contexte, estimant que la solution du litige au principal dépend de la réponse à donner à ces questions, l'Oberlandesgericht Düsseldorf (tribunal régional supérieur de Düsseldorf) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

Est-il compatible avec les articles 51 et suivants du RGPD qu'une autorité de la concurrence nationale d'un État membre, telle que l'autorité fédérale de la concurrence, qui n'est pas une autorité de contrôle au sens des articles 51 et suivants du RGPD, dans une situation où une entreprise établie en dehors de l'Union européenne possède, dans ledit État membre, une succursale qui assiste, dans le domaine de la publicité, de la communication et des relations publiques, l'établissement principal de cette entreprise qui se trouve dans un autre État membre et qui est le responsable à titre exclusif pour le traitement des données à caractère personnel pour l'ensemble du territoire de l'Union européenne, constate, dans le cadre du contrôle des pratiques abusives au regard du droit de la concurrence, une violation du RGPD par des conditions contractuelles de l'établissement principal concernant le traitement des données, ainsi que par la mise en œuvre de ces conditions, et ordonne la cessation de cette infraction ?

Dans l'affirmative, est-ce que cela est compatible avec l'article 4, paragraphe 3, TUE, lorsque, en même temps, l'autorité de contrôle chef de file dans l'État membre de l'établissement principal, au sens de l'article 56, paragraphe 1, du RGPD, soumet les conditions contractuelles de ce dernier concernant le traitement des données à une procédure d'examen ?

En cas de réponse affirmative à la première question :

Lorsqu'un utilisateur d'Internet soit consulte simplement des sites Internet ou des applications en rapport avec les critères de l'article 9, paragraphe 1, du RGPD, tels que des applications de flirt, des applications de rencontres pour

homosexuels, des sites Internet de partis politiques, des sites Internet ayant trait à la santé, soit y insère des données, par exemple en s'inscrivant ou en effectuant des commandes, et qu'une [...] entreprise, telle que [Meta Platforms Ireland], collecte, à travers des interfaces intégrées telles que les "Outils Facebook Business", ou bien à travers des *cookies* enregistrés dans l'ordinateur ou le terminal mobile de l'utilisateur d'Internet, ou à travers des technologies d'enregistrement similaires, les données concernant la consultation de ces sites Internet et applications par l'utilisateur et les données insérées par ce dernier, les met en relation avec les données du compte Facebook.com de l'utilisateur et les utilise, cette collecte et/ou cette mise en relation et/ou cette utilisation constituent-elles un traitement de données sensibles au sens de cette disposition ?

Dans l'affirmative, en consultant ces pages Internet et applications et/ou en insérant des données et/ou en activant des boutons de sélection d'un opérateur comme [Meta Platforms Ireland], intégrés dans ces sites Internet ou applications ("*plugins* sociaux" tels que "j'aime", "partager" ou "*login* Facebook" ou "*account kit*"), l'utilisateur rend-il manifestement publiques les données concernant la consultation en tant que telle et/ou les données qu'il a insérées, au sens de l'article 9, paragraphe 2, sous e), du RGPD ?

Une entreprise comme [Meta Platforms Ireland], qui exploite un réseau social financé par la publicité et qui propose, dans ses conditions de service, la personnalisation des contenus et de la publicité, la sécurité du réseau, l'amélioration du produit ainsi que l'utilisation homogène et fluide de tous les produits propres au groupe, peut-elle se prévaloir de la justification tirée du caractère nécessaire à l'exécution du contrat, conformément à l'article 6, paragraphe 1, sous b), du RGPD, ou de la prise en compte d'intérêts légitimes, conformément à l'article 6, paragraphe 1, sous f), du RGPD, lorsqu'elle collecte, met en relation avec le compte Facebook.com de l'utilisateur et utilise, à ces fins, des données issues d'autres services propres au groupe et de sites Internet et d'applications tiers, à travers des interfaces intégrées à ces derniers, telles que les "Outils Facebook Business", ou bien à travers des *cookies* enregistrés dans l'ordinateur ou le terminal mobile de l'utilisateur d'Internet, ou à travers des technologies d'enregistrement similaires ?

En pareil cas[,]

le fait que l'utilisateur soit mineur, aux fins de la personnalisation des contenus et de la publicité, de l'amélioration du produit, de la sécurité du réseau et de la communication non commerciale à destination de l'utilisateur,

la mise à la disposition des annonceurs, des développeurs et d'autres partenaires de mesures, d'analyses et d'autres services professionnels, afin qu'ils puissent évaluer leurs prestations et les améliorer,

la mise à disposition d'une communication commerciale à destination de l'utilisateur, afin que l'entreprise puisse améliorer ses produits et effectuer une promotion commerciale directe,

la recherche et l'innovation pour des finalités sociales, en vue de promouvoir l'état de la technique et la compréhension scientifique à l'égard de thématiques sociales importantes et en vue d'influencer positivement la société et le monde,

l'information des autorités compétentes pour l'exercice de poursuites pénales et pour l'exécution de peines, et la réponse à des demandes légales visant à éviter, à découvrir et à poursuivre des infractions, des violations des conditions de service et des politiques ainsi que d'autres comportements nuisibles,

peuvent-ils également constituer un intérêt légitime au sens de l'article 6, paragraphe 1, [sous f)], du RGPD, lorsque l'entreprise, à cet effet, collecte, met en relation avec le compte Facebook.com de l'utilisateur et utilise des données issues d'autres services propres au groupe et de sites Internet et d'applications tiers, à travers des interfaces intégrées à ces derniers, telles que les "Outils Facebook Business", ou bien à travers des *cookies* enregistrés dans l'ordinateur ou le terminal mobile de l'utilisateur d'Internet, ou à travers des technologies d'enregistrement similaires ?

En pareil cas, la collecte de données issues d'autres services propres au groupe et de sites Internet et d'applications tiers, à travers des interfaces intégrées à ces derniers, telles que les "Outils Facebook Business", ou bien à travers des *cookies* enregistrés dans l'ordinateur ou le terminal mobile de l'utilisateur d'Internet, la mise en relation avec le compte Facebook.com de l'utilisateur et l'utilisation de ces données ou bien l'utilisation de données déjà autrement et légalement collectées et mises en relation peuvent-elles, le cas échéant, également être justifiées au titre de l'article 6, paragraphe 1, sous c), d) et e), du RGPD, par exemple en vue de répondre à une demande juridiquement valable de fournir certaines données [sous c)], en vue de lutter contre des comportements nuisibles et de promouvoir la sécurité [sous d)], aux fins de la recherche pour le bien de la société et en vue de promouvoir la protection, l'intégrité et la sécurité [sous e)] ?

Un consentement valable et libre, notamment au sens de l'article 4, point 11, du RGPD, peut-il être donné à une entreprise ayant une position dominante sur le marché, telle que [Meta Platforms Ireland], conformément à l'article 6, paragraphe 1, sous a), et à l'article 9, paragraphe 2, sous a), du RGPD ?

En cas de réponse négative à la première question :

Une autorité de la concurrence nationale d'un État membre, telle que l'autorité fédérale de la concurrence, qui n'est pas une autorité de contrôle au sens des articles 51 et suivants du RGPD et qui examine une violation de l'interdiction des pratiques abusives en matière de droit de la concurrence commise par une entreprise ayant une position dominante sur le marché et ne consistant pas en une violation du RGPD par ses conditions de traitement des données et par la mise en œuvre de celles-ci, peut-elle effectuer des constatations, par exemple dans le cadre de la mise en balance des intérêts, sur le point de savoir si les conditions de traitement des données de l'entreprise en question et leur mise en œuvre sont conformes au RGPD ?

Si oui : cela s'applique-t-il, eu égard à l'article 4, paragraphe 3, TUE, également lorsque, en même temps, les conditions de traitement des données de cette même entreprise sont soumises à une procédure d'examen par l'autorité de contrôle chef de file compétente en vertu de l'article 56, paragraphe 1, du RGPD ?

En cas de réponse affirmative à la septième question, il est nécessaire de répondre aux troisième à cinquième questions en ce qui concerne les données issues de l'utilisation du service Instagram propre à l'entreprise. »

Sur les questions préjudicielles

Sur les première et septième questions

Par ses première et septième questions, qu'il convient de traiter ensemble, la juridiction de renvoi demande, en substance, si les articles 51 et suivants du RGPD doivent être interprétés en ce sens qu'une autorité de la concurrence d'un État membre peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise, au sens de l'article 102 TFUE, que les conditions générales d'utilisation de cette entreprise relatives au traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes au RGPD et, dans l'affirmative, si l'article 4, paragraphe 3, TUE doit être interprété en ce sens qu'une telle constatation, de nature incidente, par l'autorité de la concurrence est également possible lorsque ces conditions sont soumises, en même temps, à une procédure d'examen par l'autorité de contrôle chef de file compétente, en vertu de l'article 56, paragraphe 1, du RGPD.

Afin de répondre à cette question, il importe d'emblée de rappeler que l'article 55, paragraphe 1, du RGPD établit la compétence de principe de chaque autorité de contrôle pour exercer les missions et les pouvoirs dont elle est investie, conformément à ce règlement, sur le territoire de l'État membre dont elle relève (arrêt du 15 juin 2021, Facebook Ireland e.a., C-645/19, EU:C:2021:483, point 47 ainsi que jurisprudence citée).

Au nombre des missions dont ces autorités de contrôle sont investies figure celle de contrôler l'application du RGPD et de veiller au respect de celui-ci, prévue à l'article 51, paragraphe 1, et à l'article 57, paragraphe 1, sous a), de ce règlement, dans le but de protéger les libertés et les droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel et de faciliter le libre flux de telles données au sein de l'Union. En outre, conformément à l'article 51, paragraphe 2, et à l'article 57, paragraphe 1, sous g), dudit règlement, lesdites autorités de contrôle coopèrent entre elles, y compris en partageant des informations, et fournissent une assistance mutuelle dans ce cadre en vue d'assurer une application cohérente de ce même règlement et des mesures prises pour en assurer le respect.

En vue d'accomplir ces missions, l'article 58 du RGPD confère auxdites autorités de contrôle, à son paragraphe 1, des pouvoirs d'enquête, à son paragraphe 2, le pouvoir d'adopter des mesures correctrices et, à son paragraphe 5, le pouvoir de porter toute violation de ce règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice en vue de faire appliquer les dispositions de ce règlement.

Sans préjudice de la règle de compétence énoncée à l'article 55, paragraphe 1, du RGPD, l'article 56, paragraphe 1, de ce règlement prévoit, pour les traitements transfrontaliers, au sens de l'article 4, point 23, de celui-ci, un mécanisme de « guichet unique », fondé sur une répartition des compétences entre une « autorité de contrôle chef de file » et les autres autorités de contrôle concernées ainsi que sur une coopération entre l'ensemble de ces autorités conformément à la procédure de coopération prévue à l'article 60 dudit règlement.

Par ailleurs, l'article 61, paragraphe 1, du RGPD fait obligation aux autorités de contrôle notamment de se communiquer les informations utiles ainsi que de se prêter mutuellement assistance en vue de mettre en œuvre et d'appliquer ce règlement de façon cohérente dans l'ensemble de l'Union. L'article 63 dudit règlement précise que c'est dans ce but qu'est prévu le mécanisme de contrôle de la cohérence, établi aux articles 64 et 65 de celui-ci (arrêt du 15 juin 2021, Facebook Ireland e.a., C-645/19, EU:C:2021:483, point 52 ainsi que jurisprudence citée).

Cela étant, il importe de relever que les règles de coopération prévues dans le RGPD ne s'adressent pas aux autorités de la concurrence nationales mais régissent la coopération entre les autorités de contrôle nationales concernées et l'autorité de contrôle chef de file ainsi que, le cas échéant, la coopération de ces autorités avec le comité européen de la protection des données et la Commission.

En effet, ni le RGPD ni aucun autre instrument du droit de l'Union ne prévoient de règles spécifiques quant à la coopération entre une autorité de la concurrence nationale et les autorités de contrôle nationales concernées ou l'autorité de contrôle chef de file. En outre, aucune disposition de ce règlement n'interdit aux autorités de la concurrence nationales de constater, dans le cadre de l'exercice de leurs fonctions, la non-conformité audit règlement d'un traitement de données, effectué par une entreprise en position dominante et susceptible de constituer un abus de cette position.

À cet égard, il y a lieu de préciser, en premier lieu, que les autorités de contrôle, d'une part, et les autorités de la concurrence nationales, d'autre part, exercent des fonctions différentes et poursuivent des objectifs ainsi que des missions qui leur sont propres.

En effet, d'une part, ainsi qu'il a été indiqué au point 38 du présent arrêt, en vertu de l'article 51, paragraphes 1 et 2, ainsi que de l'article 57, paragraphe 1, sous a) et g), du RGPD, l'autorité de contrôle a pour mission principale de contrôler l'application de ce règlement et de veiller à son respect, tout en contribuant à son application cohérente dans l'Union, et ce afin de protéger les libertés et les droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel et de faciliter le libre flux de telles données au sein de l'Union. À cette fin, ainsi qu'il a été rappelé au point 39 du présent arrêt, l'autorité de contrôle dispose des différents pouvoirs qui lui sont conférés en vertu de l'article 58 du RGPD.

D'autre part, conformément à l'article 5 du règlement n° 1/2003, les autorités de la concurrence nationales sont compétentes pour adopter notamment des décisions constatant un abus de position dominante de la part d'une entreprise, au sens de l'article 102 TFUE, dont l'objectif consiste à établir un régime assurant que la concurrence ne soit pas faussée dans le marché intérieur, eu égard, également, aux conséquences d'un tel abus pour les consommateurs dans ce marché.

Ainsi que l'a en substance relevé M. l'avocat général au point 23 de ses conclusions, dans le cadre de l'adoption d'une telle décision, une autorité de la concurrence doit apprécier, sur la base de toutes les circonstances spécifiques de l'affaire, si le comportement de l'entreprise en position dominante a pour effet de faire obstacle, par le recours à des moyens différents de ceux qui gouvernent une compétition normale des produits ou des services, au maintien du degré de concurrence existant sur le marché ou au développement de cette concurrence (voir, en ce sens, arrêt du 25 mars 2021, Deutsche Telekom/Commission, C-152/19 P, EU:C:2021:238, points 41 et 42). À cet égard, la conformité ou la non-conformité d'un tel comportement aux dispositions du RGPD peut constituer, le cas échéant, un indice important parmi les circonstances pertinentes de l'espèce pour établir si ce comportement

constitue un recours à des moyens qui gouvernent une compétition normale ainsi que pour évaluer les conséquences d'une certaine pratique sur le marché ou pour les consommateurs.

Il s'ensuit que, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise sur un marché déterminé, il peut s'avérer nécessaire pour l'autorité de la concurrence de l'État membre concerné d'examiner également la conformité du comportement de cette entreprise à des normes autres que celles relevant du droit de la concurrence, telles que les règles en matière de protection des données à caractère personnel prévues par le RGPD.

Or, compte tenu des objectifs différents poursuivis par les règles établies en matière de concurrence, en particulier l'article 102 TFUE, d'une part, et par celles prévues en matière de protection des données à caractère personnel en vertu du RGPD, d'autre part, il y a lieu de constater que, lorsqu'une autorité de la concurrence nationale relève une violation de ce règlement dans le cadre du constat d'un abus de position dominante, elle ne se substitue pas aux autorités de contrôle. En particulier, une telle autorité de la concurrence nationale ne contrôle pas l'application ni ne veille au respect de ce règlement dans le but visé à l'article 51, paragraphe 1, de celui-ci, à savoir afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union. En outre, en se limitant à relever la non-conformité d'un traitement de données au RGPD aux seules fins de constater un abus de position dominante et en imposant des mesures visant à la cessation de cet abus sur le fondement d'une base juridique issue du droit de la concurrence, une telle autorité n'exerce aucune des missions figurant à l'article 57 de ce règlement, pas plus qu'elle ne fait usage des pouvoirs réservés à l'autorité de contrôle en vertu de l'article 58 dudit règlement.

Par ailleurs, il importe de constater que l'accès aux données à caractère personnel ainsi que leur exploitation revêtent une importance majeure dans le cadre de l'économie numérique. Cette importance est illustrée, dans le cadre du litige au principal, par le modèle économique sur lequel se fonde le réseau social Facebook, lequel prévoit, comme il a été rappelé au point 27 du présent arrêt, le financement par la commercialisation de messages publicitaires personnalisés en fonction de profils d'utilisateur établis sur la base de données à caractère personnel collectées par Meta Platforms Ireland.

Ainsi que l'a souligné notamment la Commission, l'accès aux données à caractère personnel et la possibilité de traitement de ces données sont devenus un paramètre significatif de la concurrence entre entreprises de l'économie numérique. Partant, exclure les règles en matière de protection des données à caractère personnel du cadre juridique à prendre en considération par les autorités de la concurrence lors de l'examen d'un abus de position dominante méconnaîtrait la réalité de cette évolution économique et serait susceptible de porter atteinte à l'effectivité du droit de la concurrence au sein de l'Union.

Toutefois, en second lieu, il importe de relever que, dans l'hypothèse où une autorité de la concurrence nationale considère nécessaire de se prononcer, dans le cadre d'une décision relative à un abus de position dominante, sur la conformité ou la non-conformité au RGPD d'un traitement de données à caractère personnel effectué par l'entreprise en question, cette autorité et l'autorité de contrôle concernée ou, le cas échéant, l'autorité de contrôle chef de file compétente au sens de ce règlement doivent coopérer entre elles afin d'assurer une application cohérente de ce règlement.

En effet, si, comme il a été relevé aux points 42 et 43 du présent arrêt, ni le RGPD ni aucun autre instrument du droit de l'Union ne prévoient de règles spécifiques à cet égard, il n'en reste pas moins que, ainsi que l'a relevé en substance M. l'avocat général au point 28 de ses conclusions, lorsqu'elles appliquent le RGPD, les différentes autorités nationales impliquées sont toutes tenues par le principe de coopération loyale consacré à l'article 4, paragraphe 3, TUE. En vertu de ce principe, conformément à une jurisprudence constante, dans les domaines relevant du droit de l'Union, les États membres, y compris leurs autorités administratives, doivent se respecter et s'assister mutuellement dans l'accomplissement des missions découlant des traités, prendre toute mesure propre à assurer l'exécution des obligations résultant notamment des actes des institutions de l'Union ainsi que s'abstenir de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union (voir, en ce sens, arrêts du 7 novembre 2013, UPC Nederland, C-518/11, EU:C:2013:709, point 59, ainsi que du 1er août 2022, Sea Watch, C-14/21 et C-15/21, EU:C:2022:604, point 156).

Ainsi, compte tenu de ce principe, lorsque les autorités de la concurrence nationales sont amenées, dans l'exercice de leurs compétences, à examiner la conformité d'un comportement d'une entreprise aux dispositions du RGPD, elles doivent se concerter et coopérer loyalement avec les autorités de contrôle nationales concernées ou avec l'autorité de contrôle chef de file, l'ensemble de ces autorités étant alors tenues, dans ce contexte, de respecter leurs pouvoirs et compétences respectifs, de manière à ce que les obligations découlant du RGPD ainsi que les objectifs de ce règlement soient respectés et que leur effet utile soit préservé.

En effet, l'examen par une autorité de la concurrence d'un comportement d'une entreprise à la lumière des normes du RGPD peut comporter le risque de divergences entre celle-ci et les autorités de contrôle quant à l'interprétation de ce règlement.

Il s'ensuit que, lorsque, dans le cadre de l'examen visant à constater un abus de position dominante au sens de l'article 102 TFUE de la part d'une entreprise, une autorité de la concurrence nationale considère qu'il est nécessaire d'examiner la conformité d'un comportement de cette entreprise à l'égard des dispositions du RGPD, ladite autorité doit vérifier si ce comportement ou un comportement similaire a déjà fait l'objet d'une décision par l'autorité de contrôle nationale compétente ou par l'autorité de contrôle chef de file ou bien encore par la Cour. Si tel est le cas, l'autorité de la concurrence nationale ne peut s'en écarter, tout en restant libre d'en tirer ses propres conclusions sous l'angle de l'application du droit de la concurrence.

Lorsqu'elle nourrit des doutes sur la portée de l'appréciation effectuée par l'autorité de contrôle nationale compétente ou l'autorité de contrôle chef de file, lorsque le comportement en cause ou un comportement similaire fait, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête desdites autorités, elle considère qu'un comportement d'une entreprise n'est pas conforme aux dispositions du RGPD, l'autorité de la concurrence nationale doit consulter ces autorités et solliciter leur coopération, afin de lever

ses doutes ou de déterminer s'il y a lieu d'attendre l'adoption d'une décision de la part de l'autorité de contrôle concernée avant d'entamer sa propre appréciation.

Pour sa part, lorsque l'autorité de contrôle est sollicitée par une autorité de la concurrence nationale, elle doit répondre à cette demande de renseignement ou de coopération dans un délai raisonnable, en communiquant à cette dernière les informations dont elle dispose pouvant permettre de lever les doutes de cette autorité sur la portée de l'appréciation effectuée par l'autorité de contrôle ou, le cas échéant, en informant l'autorité de la concurrence nationale si elle envisage d'activer la procédure de coopération avec les autres autorités de contrôle concernées ou avec l'autorité de contrôle chef de file, conformément aux articles 60 et suivants du RGPD, afin de parvenir à une décision visant à constater la conformité ou la non-conformité du comportement en question à ce règlement.

En l'absence de réponse de la part de l'autorité de contrôle sollicitée dans un délai raisonnable, l'autorité de la concurrence nationale peut poursuivre sa propre enquête. Il en va de même lorsque l'autorité de contrôle nationale compétente et l'autorité de contrôle chef de file n'émettent pas d'objection à ce qu'une telle enquête soit poursuivie sans attendre l'adoption d'une décision de leur part.

En l'occurrence, il ressort du dossier dont dispose la Cour que, au cours des mois d'octobre et de novembre 2018, soit avant l'adoption de la décision du 6 février 2019, l'autorité fédérale de la concurrence a pris contact avec le Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (commissaire fédéral à la protection des données et à la liberté de l'information, Allemagne), le Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (commissaire à la protection des données et à la liberté de l'information de Hambourg, Allemagne), compétent à l'égard de Facebook Deutschland, et la Data Protection Commission (DPC) (autorité de protection des données, Irlande), pour informer ces autorités de son intervention. En outre, il apparaît que l'autorité fédérale de la concurrence a obtenu la confirmation qu'aucune enquête n'était alors conduite par lesdites autorités concernant des faits similaires à ceux en cause au principal, et celles-ci n'ont soulevé aucune objection à l'égard de son intervention. Enfin, aux points 555 et 556 de sa décision du 6 février 2019, l'autorité fédérale de la concurrence a expressément fait référence à cette coopération.

Dans ces conditions, et sous réserve des vérifications qu'il appartient à la juridiction de renvoi d'effectuer, l'autorité fédérale de la concurrence paraît avoir rempli ses obligations de coopération loyale avec les autorités de contrôle nationales concernées ainsi qu'avec l'autorité de contrôle chef de file.

Compte tenu de ce qui précède, il y a lieu de répondre aux première et septième questions que les articles 51 et suivants du RGPD ainsi que l'article 4, paragraphe 3, TUE doivent être interprétés en ce sens que, sous réserve du respect de son obligation de coopération loyale avec les autorités de contrôle, une autorité de la concurrence d'un État membre peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise, au sens de l'article 102 TFUE, que les conditions générales d'utilisation de cette entreprise relatives au traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes à ce règlement, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus.

Au vu de cette obligation de coopération loyale, l'autorité de la concurrence nationale ne peut s'écarter d'une décision de l'autorité de contrôle nationale compétente ou de l'autorité de contrôle chef de file compétente relative à ces conditions générales ou à des conditions générales similaires. Lorsqu'elle nourrit des doutes à l'égard de la portée d'une telle décision, lorsque lesdites conditions ou des conditions similaires font, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête ou de décision desdites autorités, l'autorité de la concurrence considère que les conditions en cause ne sont pas conformes au RGPD, elle doit consulter ces mêmes autorités de contrôle et solliciter leur coopération, afin de lever ses doutes ou de déterminer s'il y a lieu d'attendre l'adoption d'une décision de leur part avant d'entamer sa propre appréciation. En l'absence d'objection de leur part ou de réponse dans un délai raisonnable, l'autorité de la concurrence nationale peut poursuivre sa propre enquête.

Sur la deuxième question

Par sa deuxième question, sous a), la juridiction de renvoi demande, en substance, si l'article 9, paragraphe 1, du RGPD doit être interprété en ce sens que, dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à cette disposition et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne, consistant en la collecte, au moyen d'interfaces intégrées, de *cookies* ou de technologies d'enregistrement similaires, des données issues de la consultation de ces sites et de ces applications ainsi que des données insérées par l'utilisateur, en la mise en relation de l'ensemble de ces données avec le compte du réseau social de celui-ci et en l'utilisation desdites données par cet opérateur, doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de ladite disposition, qui est en principe interdit, sous réserve des dérogations prévues à cet article 9, paragraphe 2.

Dans l'affirmative, la juridiction de renvoi demande, en substance, par sa deuxième question, sous b), si l'article 9, paragraphe 2, sous e), du RGPD doit être interprété en ce sens que, lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications ayant des liens avec les catégories énoncées à l'article 9, paragraphe 1, du RGPD, saisit des données sur ces sites ou applications ou active des boutons de sélection intégrés sur ceux-ci, tels que les boutons « j'aime » ou « partager » ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou ces applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social en ligne, son numéro de téléphone ou son adresse électronique, il est réputé avoir manifestement rendu publiques, au sens de la première de ces dispositions, les données collectées à cette occasion par l'opérateur de ce réseau social en ligne à travers des *cookies* ou des technologies d'enregistrement similaires.

Sur la deuxième question, sous a)

Le considérant 51 du RGPD énonce que les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et ces droits. Ce considérant précise que de telles données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans les cas spécifiques prévus par ledit règlement.

Dans ce contexte, l'article 9, paragraphe 1, du RGPD pose le principe de l'interdiction du traitement portant sur des catégories particulières de données à caractère personnel qu'il mentionne. Il s'agit, notamment, des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ainsi que des données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Aux fins de l'application de l'article 9, paragraphe 1, du RGPD, il importe de vérifier, dans le cas d'un traitement de données à caractère personnel effectué par l'opérateur d'un réseau social en ligne, si ces données permettent de révéler des informations relevant d'une des catégories visées à cette disposition, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique. Dans l'affirmative, un tel traitement de données à caractère personnel est alors interdit, sous réserve des dérogations prévues à l'article 9, paragraphe 2, du RGPD.

Ainsi que l'a, en substance, relevé M. l'avocat général aux points 40 et 41 de ses conclusions, cette interdiction de principe, prévue à l'article 9, paragraphe 1, du RGPD, est indépendante du point de savoir si l'information révélée par le traitement en cause est exacte ou non et si le responsable du traitement agit dans le but d'obtenir des informations relevant d'une des catégories particulières visées à cette disposition.

En effet, compte tenu des risques importants pour les libertés fondamentales et les droits fondamentaux des personnes concernées, engendrés par tout traitement de données à caractère personnel relevant des catégories visées à l'article 9, paragraphe 1, du RGPD, celui-ci a pour objectif d'interdire ces traitements, indépendamment de leur but affiché.

En l'occurrence, le traitement en cause au principal effectué par Meta Platforms Ireland consiste, tout d'abord, en la collecte des données à caractère personnel des utilisateurs du réseau social Facebook lorsque ceux-ci consultent des sites Internet ou des applications – y compris ceux susceptibles de révéler des informations relevant d'une ou de plusieurs des catégories visées à l'article 9, paragraphe 1, du RGPD – et, le cas échéant, y insèrent des informations en s'inscrivant ou en effectuant des commandes en ligne, ensuite en la mise en relation de ces données avec le compte du réseau social de ces utilisateurs et, enfin, en l'utilisation desdites données.

À cet égard, il appartiendra à la juridiction de renvoi de déterminer si les données ainsi collectées, à elles seules ou par leur mise en relation avec les comptes Facebook des utilisateurs concernés, permettent effectivement de révéler de telles informations, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique. Toutefois, compte tenu des interrogations de cette juridiction, il convient de préciser qu'il apparaît, sous réserve des vérifications à effectuer par celle-ci, que le traitement des données relatives à la consultation des sites Internet ou des applications en question peut, dans certains cas, révéler de telles informations, sans qu'il soit nécessaire que lesdits utilisateurs y insèrent des informations en s'inscrivant ou en effectuant des commandes en ligne.

Compte tenu de ce qui précède, il y a lieu de répondre à la deuxième question, sous a), que l'article 9, paragraphe 1, du RGPD doit être interprété en ce sens que, dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à cette disposition et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne, consistant en la collecte, au moyen d'interfaces intégrées, de *cookies* ou de technologies d'enregistrement similaires, des données issues de la consultation de ces sites et de ces applications ainsi que des données insérées par l'utilisateur, en la mise en relation de l'ensemble de ces données avec le compte du réseau social de celui-ci et en l'utilisation desdites données par cet opérateur, doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de ladite disposition, qui est en principe interdit, sous réserve des dérogations prévues à cet article 9, paragraphe 2, lorsque ce traitement de données permet de révéler des informations relevant d'une de ces catégories, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique.

Sur la deuxième question, sous b)

S'agissant de la deuxième question, sous b), telle qu'elle a été reformulée au point 65 du présent arrêt et relative à la dérogation prévue à l'article 9, paragraphe 2, sous e), du RGPD, il y a lieu de rappeler que, en vertu de cette disposition, l'interdiction de principe de tout traitement portant sur des catégories particulières de données à caractère personnel, posée par cet article 9, paragraphe 1, ne s'applique pas dans l'hypothèse où le traitement porte sur des données à caractère personnel qui sont « manifestement rendues publiques par la personne concernée ».

À titre liminaire, il y a lieu de relever que, d'une part, cette dérogation s'applique aux seules données manifestement rendues publiques « par la personne concernée ». Partant, elle n'est pas applicable aux données concernant d'autres personnes que celle ayant rendu ces données publiques.

D'autre part, dans la mesure où il prévoit une exception au principe de l'interdiction du traitement des catégories particulières de données à caractère personnel, l'article 9, paragraphe 2, du RGPD doit être interprété de manière restrictive (voir, en ce sens, arrêts du 17 septembre 2014, Baltic Agro, C-3/13, EU:C:2014:2227, point 24 et jurisprudence citée, ainsi que du 6 juin 2019, Weil, C-361/18, EU:C:2019:473, point 43 et jurisprudence citée).

Il s'ensuit que, aux fins de l'application de l'exception prévue à l'article 9, paragraphe 2, sous e), du RGPD, il importe de vérifier si la personne concernée a entendu, de manière explicite et par un acte positif clair, rendre accessibles au grand public les données à caractère personnel en question.

À cet égard, s'agissant, d'une part, de la consultation des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à l'article 9, paragraphe 1, du RGPD, il importe de constater que, par celle-ci, l'utilisateur concerné n'entend nullement rendre public le fait qu'il a consulté ces sites ou ces applications et les

données relatives à cette consultation qui peuvent être rattachées à sa personne. En effet, ce dernier peut tout au plus s'attendre à ce que le gestionnaire du site ou de l'application ait accès à ces données et qu'il les partage, le cas échéant et sous réserve du consentement explicite donné par cet utilisateur, avec certains tiers et non pas avec le grand public.

Ainsi, il ne saurait être déduit de la seule consultation de tels sites Internet ou de telles applications par un utilisateur que lesdites données à caractère personnel auraient été manifestement rendues publiques par cet utilisateur, au sens de l'article 9, paragraphe 2, sous e), du RGPD.

D'autre part, en ce qui concerne les activités consistant à insérer des données sur lesdits sites Internet ou lesdites applications ainsi qu'à activer des boutons de sélection intégrés à ceux-ci, tels que les boutons « j'aime » ou « partager » ou les boutons permettant à l'utilisateur de s'identifier sur un site Internet ou sur une application en utilisant les identifiants de connexion liés à son compte d'utilisateur Facebook, son numéro de téléphone ou son adresse électronique, il y a lieu de relever que ces activités comportent une interaction entre cet utilisateur et le site Internet ou l'application en question, et, le cas échéant, le site Internet du réseau social en ligne, interaction dont les formes de publicité peuvent varier en ce qu'elles peuvent faire l'objet d'un paramétrage individuel de la part dudit utilisateur.

Dans ces conditions, il incombe à la juridiction de renvoi de vérifier si les utilisateurs concernés ont la possibilité de décider, sur la base d'un paramétrage effectué en connaissance de cause, de rendre les données insérées dans les sites Internet ou dans les applications en question ainsi que les données résultant de l'activation des boutons de sélection intégrés à ceux-ci accessibles au grand public ou, au contraire, à un nombre plus ou moins limité de personnes sélectionnées.

Lorsque les utilisateurs concernés ont effectivement un tel choix, ceux-ci ne peuvent être regardés, lorsqu'ils insèrent volontairement des données dans un site Internet ou dans une application ou qu'ils activent des boutons de sélection intégrés à ceux-ci, comme rendant manifestement publiques des données les concernant, au sens de l'article 9, paragraphe 2, sous e), du RGPD, que, dans le cas où, sur la base d'un paramétrage individuel effectué en toute connaissance de cause, ces utilisateurs ont clairement exprimé leur choix que ces données soient rendues accessibles à un nombre illimité de personnes, ce qu'il incombe à la juridiction de renvoi de vérifier.

En revanche, si un tel paramétrage individuel n'est pas proposé, il convient de considérer, compte tenu de ce qui a été exposé au point 77 du présent arrêt, que, lorsque des utilisateurs insèrent volontairement des données dans un site Internet ou dans une application ou activent des boutons de sélection intégrés à ceux-ci, ils doivent, pour être réputés avoir manifestement rendu publiques ces données, avoir explicitement consenti, sur la base d'une information expresse fournie par ce site ou par cette application avant une telle insertion ou activation, à ce que lesdites données puissent être visualisées par toute personne ayant accès audit site ou à ladite application.

Compte tenu de ce qui précède, il y a lieu de répondre à la deuxième question, sous b), que l'article 9, paragraphe 2, sous e), du RGPD doit être interprété en ce sens que, lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à l'article 9, paragraphe 1, du RGPD, il ne rend pas manifestement publiques, au sens de la première de ces dispositions, les données relatives à cette consultation, collectées par l'opérateur de ce réseau social en ligne à travers des *cookies* ou des technologies d'enregistrement similaires.

Lorsqu'il insère des données dans de tels sites Internet ou dans de telles applications ou lorsqu'il active des boutons de sélection intégrés à ces sites et à ces applications, tels que les boutons « j'aime » ou « partager » ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou ces applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social, son numéro de téléphone ou son adresse électronique, un tel utilisateur ne rend manifestement publiques, au sens de cet article 9, paragraphe 2, sous e), les données ainsi insérées ou résultant de l'activation de ces boutons que dans le cas où il a explicitement exprimé son choix au préalable, le cas échéant sur la base d'un paramétrage individuel effectué en toute connaissance de cause, de rendre les données le concernant publiquement accessibles à un nombre illimité de personnes.

Sur les troisième à cinquième questions

Par ses troisième et quatrième questions, qu'il convient d'examiner conjointement, la juridiction de renvoi souhaite savoir, en substance, si et dans quelles conditions l'article 6, paragraphe 1, premier alinéa, sous b) et f), du RGPD doit être interprété en ce sens que le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, peut être considéré comme étant nécessaire à l'exécution d'un contrat auquel les personnes concernées sont parties, au sens du point b), ou aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, au sens du point f). Cette juridiction se demande notamment si, à cette fin, certains intérêts qu'elle cite explicitement constituent un « intérêt légitime », au sens de cette dernière disposition.

Par sa cinquième question, la juridiction de renvoi demande, en substance, si l'article 6, paragraphe 1, premier alinéa, sous c) à e), du RGPD doit être interprété en ce sens qu'un tel traitement de données à caractère personnel peut être considéré comme étant nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, au sens du point c), à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, au sens du point d), ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, au sens du point e), dans le cas où ledit traitement est effectué respectivement en vue de répondre à une demande juridiquement valable de fournir certaines données, afin de lutter contre des comportements nuisibles et de promouvoir la sécurité, et aux fins de la recherche pour le bien de la société et en vue de promouvoir la protection, l'intégrité et la sécurité.

Observations liminaires

À titre liminaire, il y a lieu de faire observer, premièrement, que les troisième à cinquième questions sont posées en raison du fait que, d'après les constatations de l'autorité fédérale de la concurrence dans sa décision du 6 février 2019, il ne saurait être considéré que les utilisateurs du réseau social Facebook ont donné leur consentement au traitement de leurs données en cause au principal, au sens de l'article 6, paragraphe 1, premier alinéa, sous a), et de l'article 9, paragraphe 2, sous a), du RGPD. C'est donc dans ce contexte que la juridiction de renvoi, tout en interrogeant la Cour par sa sixième question par rapport à cette prémisse, estime devoir vérifier si ce traitement correspond à l'une des autres conditions de licéité, visées à cet article 6, paragraphe 1, premier alinéa, sous b) à f), de ce règlement.

Dans ce cadre, il convient de relever que les opérations de collecte, de mise en relation et d'utilisation des données, visées dans les troisième à cinquième questions, sont susceptibles d'englober à la fois des données sensibles au sens de l'article 9, paragraphe 1, du RGPD et des données non sensibles. Or, il y a lieu de préciser que, dans le cas où un ensemble de données comportant à la fois des données sensibles et des données non sensibles fait l'objet de telles opérations et est notamment collecté en bloc sans que les données puissent être dissociées les unes des autres au moment de cette collecte, le traitement de cet ensemble de données doit être considéré comme étant interdit, au sens de l'article 9, paragraphe 1, du RGPD dès lors qu'il comporte au moins une donnée sensible et qu'aucune des dérogations visées à l'article 9, paragraphe 2, de ce règlement n'est applicable.

Deuxièmement, afin de répondre aux troisième à cinquième questions, il convient de rappeler que l'article 6, paragraphe 1, premier alinéa, du RGPD prévoit une liste exhaustive et limitative des cas dans lesquels un traitement de données à caractère personnel peut être considéré comme licite. Ainsi, pour qu'il puisse être considéré comme légitime, un traitement doit relever de l'un des cas prévus à cette disposition [arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 99 et jurisprudence citée].

Aux termes de l'article 6, paragraphe 1, premier alinéa, sous a), de ce règlement, le traitement de données à caractère personnel est licite si, et dans la mesure où, la personne concernée y a consenti pour une ou plusieurs finalités spécifiques.

En l'absence d'un tel consentement, ou lorsque ce consentement n'a pas été donné de manière libre, spécifique, éclairée et univoque, au sens de l'article 4, point 11, du RGPD, un tel traitement est néanmoins justifié lorsqu'il répond à l'une des exigences de nécessité mentionnées à l'article 6, paragraphe 1, premier alinéa, sous b) à f), de ce règlement.

Dans ce contexte, les justifications prévues à cette dernière disposition, en ce qu'elles permettent de rendre licite un traitement de données à caractère personnel effectué en l'absence du consentement de la personne concernée, doivent faire l'objet d'une interprétation restrictive [voir, en ce sens, arrêt du 24 février 2022, Valsts ieņēmumu dienests (Traitement des données personnelles à des fins fiscales), C-175/20, EU:C:2022:124, point 73 et jurisprudence citée].

En outre, ainsi que la Cour l'a jugé, lorsqu'il est possible de constater qu'un traitement de données à caractère personnel est nécessaire au regard d'une des justifications prévues à l'article 6, paragraphe 1, premier alinéa, sous b) à f), du RGPD, il n'y a pas lieu de déterminer si ce traitement relève également d'une autre de ces justifications (voir, en ce sens, arrêt du 1er août 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, point 71).

Il convient enfin de préciser que, conformément à l'article 5 du RGPD, c'est sur le responsable du traitement que repose la charge de prouver que ces données sont notamment collectées pour des finalités déterminées, explicites et légitimes et qu'elles sont traitées de manière licite, loyale et transparente au regard de la personne concernée. En outre, conformément à l'article 13, paragraphe 1, sous c), de ce règlement, lorsque des données à caractère personnel sont collectées auprès de la personne concernée, il incombe au responsable du traitement d'informer celle-ci des finalités du traitement auquel sont destinées ces données ainsi que de la base juridique de ce traitement.

S'il appartient à la juridiction de renvoi de déterminer si les différents éléments du traitement en cause au principal sont justifiés par l'une ou l'autre des nécessités visées à l'article 6, paragraphe 1, premier alinéa, sous b) à f), du RGPD, la Cour peut néanmoins lui fournir des indications utiles afin de lui permettre de trancher le litige dont elle est saisie.

Sur les troisième et quatrième questions

En ce qui concerne, en premier lieu, l'article 6, paragraphe 1, premier alinéa, sous b), du RGPD, celui-ci prévoit qu'un traitement de données à caractère personnel est licite s'il est « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».

À cet égard, pour qu'un traitement de données à caractère personnel soit regardé comme étant nécessaire à l'exécution d'un contrat, au sens de cette disposition, il doit être objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à la personne concernée. Le responsable du traitement doit ainsi être en mesure de démontrer en quoi l'objet principal du contrat ne pourrait être atteint en l'absence du traitement en cause.

Le fait qu'un tel traitement soit mentionné dans le contrat ou qu'il soit seulement utile à l'exécution de celui-ci est, en soi, dépourvu de pertinence à cet égard. En effet, l'élément déterminant aux fins de l'application de la justification visée à l'article 6, paragraphe 1, premier alinéa, sous b), du RGPD est que le traitement de données à caractère personnel effectué par le responsable du traitement soit essentiel afin de permettre l'exécution correcte du contrat conclu entre celui-ci et la personne concernée et, partant, qu'il n'existe pas d'autres solutions praticables et moins intrusives.

À cet égard, ainsi que l'a relevé M. l'avocat général au point 54 de ses conclusions, lorsque le contrat consiste en plusieurs services ou en plusieurs éléments distincts d'un même service qui peuvent être exécutés indépendamment les uns des autres, l'applicabilité de l'article 6, paragraphe 1, premier alinéa, sous b), du RGPD doit être évaluée séparément dans le contexte de chacun de ces services.

En l'occurrence, dans le cadre des justifications susceptibles de relever du champ d'application de cette disposition, la juridiction de renvoi fait référence, en tant qu'éléments visant à assurer l'exécution adéquate du contrat conclu entre Meta Platforms Ireland et ses utilisateurs, à la personnalisation des contenus ainsi qu'à l'utilisation homogène et fluide des services propres au groupe Meta.

S'agissant, premièrement, de la justification tirée de la personnalisation des contenus, il importe de relever que, si une telle personnalisation est utile pour l'utilisateur, dans la mesure où elle lui permet notamment de visualiser un contenu correspondant dans une large mesure à ses intérêts, il n'en reste pas moins que, sous réserve de vérification à effectuer par la juridiction de renvoi, la personnalisation des contenus n'apparaît pas nécessaire pour offrir à cet utilisateur les services du réseau social en ligne. Ces services peuvent, le cas échéant, lui être fournis sous la forme d'une alternative équivalente n'impliquant pas une telle personnalisation, de sorte que cette dernière n'est pas objectivement indispensable à une finalité faisant partie intégrante des mêmes services.

Pour ce qui est, secondement, de la justification tirée de l'utilisation homogène et fluide des services propres au groupe Meta, il ressort du dossier dont dispose la Cour qu'une personne n'est pas tenue de souscrire aux différents services proposés par le groupe Meta afin de pouvoir créer un compte d'utilisateur dans le réseau social Facebook. En effet, les différents produits et services proposés par ce groupe peuvent être utilisés indépendamment les uns des autres et l'utilisation de chaque produit ou service se fonde sur la souscription d'un contrat d'utilisation distinct.

Partant et sous réserve de vérification par la juridiction de renvoi, un traitement de données à caractère personnel issues de services autres que le service du réseau social en ligne proposés par le groupe Meta ne paraît pas être nécessaire pour permettre la fourniture de ce dernier service.

En ce qui concerne, en second lieu, l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, celui-ci prévoit qu'un traitement de données à caractère personnel est licite s'il est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et les droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».

Ainsi que la Cour l'a déjà jugé, cette disposition prévoit trois conditions cumulatives pour que les traitements de données à caractère personnel qu'elle vise soient licites, à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par un tiers, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition que les intérêts ou les libertés et les droits fondamentaux de la personne concernée par la protection des données ne prévalent pas sur l'intérêt légitime du responsable du traitement ou d'un tiers (arrêt du 17 juin 2021, M.I.C.M., C-597/19, EU:C:2021:492, point 106 et jurisprudence citée).

S'agissant, premièrement, de la condition relative à la poursuite d'un intérêt légitime, il y a lieu de préciser que, conformément à l'article 13, paragraphe 1, sous d), du RGPD, il incombe au responsable du traitement, au moment où des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, de lui indiquer les intérêts légitimes poursuivis lorsque ce traitement est fondé sur l'article 6, paragraphe 1, premier alinéa, sous f), de ce règlement.

En ce qui concerne, deuxièmement, la condition relative à la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi, celle-ci impose à la juridiction de renvoi de vérifier que l'intérêt légitime du traitement des données poursuivi ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte [voir, en ce sens, arrêt du 22 juin 2021, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, point 110 et jurisprudence citée].

Dans ce contexte, il y a également lieu de rappeler que la condition tenant à la nécessité du traitement doit être examinée conjointement avec le principe dit de la « minimisation des données » consacré à l'article 5, paragraphe 1, sous c), du RGPD, selon lequel les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » (voir, en ce sens, arrêt du 11 décembre 2019, Asociaţia de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, point 48).

Pour ce qui est, troisièmement, de la condition que les intérêts ou les libertés et les droits fondamentaux de la personne concernée par la protection des données ne prévalent pas sur l'intérêt légitime du responsable du traitement ou d'un tiers, la Cour a déjà jugé que celle-ci implique une pondération des droits et des intérêts opposés en cause qui dépend, en principe, des circonstances concrètes du cas particulier et que, par conséquent, il revient à la juridiction de renvoi d'effectuer cette pondération en tenant compte de ces circonstances spécifiques (arrêt du 17 juin 2021, M.I.C.M., C-597/19, EU:C:2021:492, point 111 et jurisprudence citée).

À cet égard, il ressort du texte même de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD qu'il est nécessaire, dans le cadre d'une telle pondération, de prêter une attention particulière à la situation où la personne concernée est un enfant. En effet, conformément au considérant 38 de ce règlement, les enfants méritent une protection spécifique en ce qui concerne le traitement de leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées ainsi que de leurs droits liés à un tel traitement des données à caractère personnel. Ainsi, une telle protection particulière doit, notamment, s'appliquer au traitement de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur ou encore de proposition de services visant directement des enfants.

En outre, ainsi qu'il ressort du considérant 47 du RGPD, les intérêts et les droits fondamentaux de la personne concernée peuvent, en particulier, prévaloir sur l'intérêt du responsable du traitement lorsque des données à caractère personnel sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un tel traitement.

En l'occurrence, dans le cadre des justifications susceptibles de relever du champ d'application de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, la juridiction de renvoi fait référence à la personnalisation de la publicité, à la sécurité du réseau, à l'amélioration du produit, à l'information des autorités compétentes pour l'exercice de poursuites pénales ainsi que pour l'exécution de peines, au fait que l'utilisateur soit un mineur d'âge, à la recherche et à l'innovation à des fins sociales ainsi qu'à l'offre, destinée aux annonceurs et aux autres partenaires professionnels, de services de communication commerciale à destination de l'utilisateur et d'outils d'analyse leur permettant d'évaluer leurs performances.

À cet égard, il y a lieu de relever, d'emblée, que la demande de décision préjudicielle ne comporte pas d'éléments d'explication permettant de comprendre en quoi la recherche et l'innovation pour des finalités sociales ou le fait que l'utilisateur soit un mineur d'âge pourraient justifier, en tant qu'intérêts légitimes au sens de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD, la collecte et l'exploitation des données en question. Par conséquent, la Cour n'est pas en mesure de se prononcer à cet égard.

S'agissant, premièrement, de la personnalisation de la publicité, il y a lieu de relever que, selon le considérant 47 de ce règlement, le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime du responsable du traitement.

Cependant, encore faut-il qu'un tel traitement soit nécessaire à la réalisation de cet intérêt et que les intérêts ou les libertés et les droits fondamentaux de la personne concernée ne prévalent pas sur celui-ci. Dans le cadre de cette pondération des droits et des intérêts opposés en cause, à savoir ceux du responsable du traitement, d'une part, et ceux de la personne concernée, d'autre part, il importe de tenir compte, ainsi qu'il a été relevé au point 112 du présent arrêt, notamment des attentes raisonnables de la personne concernée ainsi que de l'étendue du traitement en cause et de l'impact de celui-ci sur cette personne.

À cet égard, il importe de relever que, malgré la gratuité des services d'un réseau social en ligne tel que Facebook, l'utilisateur de celui-ci ne saurait raisonnablement s'attendre à ce que, sans son consentement, l'opérateur de ce réseau social traite les données à caractère personnel de cet utilisateur à des fins de personnalisation de la publicité. Dans ces conditions, il doit être considéré que les intérêts et les droits fondamentaux d'un tel utilisateur prévalent sur l'intérêt de cet opérateur à une telle personnalisation de la publicité par laquelle il finance son activité, de sorte que le traitement effectué par celui-ci à de telles fins ne saurait relever de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD.

Par ailleurs, le traitement en cause au principal est particulièrement étendu dès lors qu'il porte sur des données potentiellement illimitées et qu'il a un impact important sur l'utilisateur, dont une grande partie, voire la quasi-totalité, des activités en ligne sont monitorées par Meta Platforms Ireland, ce qui peut susciter auprès de celui-ci la sensation d'une surveillance continue de sa vie privée.

Deuxièmement, en ce qui concerne l'objectif visant à garantir la sécurité du réseau, celui-ci constitue, ainsi que l'énonce le considérant 49 du RGPD, un intérêt légitime de Meta Platforms Ireland, susceptible de justifier le traitement en cause au principal.

Toutefois, s'agissant de la nécessité de ce traitement à la réalisation de cet intérêt légitime, la juridiction de renvoi devra vérifier si et dans quelle mesure le traitement de données à caractère personnel collectées à partir de sources extérieures au réseau social Facebook s'avère effectivement nécessaire pour assurer que la sécurité interne de ce réseau n'est pas compromise.

Dans ce contexte, ainsi qu'il a été relevé aux points 108 et 109 du présent arrêt, elle devra également vérifier, d'une part, si l'intérêt légitime du traitement des données poursuivi ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte et, d'autre part, si le principe dit de la « minimisation des données », consacré à l'article 5, paragraphe 1, sous c), du RGPD, est respecté.

Troisièmement, s'agissant de l'objectif visant l'amélioration du produit, il ne saurait être exclu a priori que l'intérêt du responsable du traitement d'améliorer son produit ou son service en vue de le rendre plus performant et ainsi plus attrayant puisse constituer un intérêt légitime permettant de justifier un traitement de données à caractère personnel et qu'un tel traitement puisse être nécessaire à la poursuite de cet intérêt.

Cependant, sous réserve de l'appréciation finale à effectuer à cet égard par la juridiction de renvoi, il apparaît douteux que, s'agissant du traitement de données en cause au principal, l'objectif visant l'amélioration du produit puisse, compte tenu de l'ampleur de ce traitement et de l'impact important de celui-ci sur l'utilisateur, ainsi que de la circonstance que ce dernier ne saurait raisonnablement s'attendre à ce que ces données soient traitées par Meta Platforms Ireland, prévaloir sur les intérêts et les droits fondamentaux d'un tel utilisateur, d'autant plus dans l'hypothèse où celui-ci est un enfant.

Quatrièmement, en ce qui concerne l'objectif évoqué par la juridiction de renvoi, relatif à l'information des autorités compétentes pour l'exercice de poursuites pénales et pour l'exécution de peines visant à éviter, à découvrir et à poursuivre des infractions, il y a lieu de constater que cet objectif n'est pas susceptible, en principe, de constituer un intérêt légitime poursuivi par le responsable du traitement, au sens de l'article 6, paragraphe 1, premier alinéa, sous f), du RGPD. En effet, un opérateur privé tel que Meta Platforms Ireland ne saurait exciper d'un tel intérêt légitime, étranger à son activité économique et commerciale. En revanche, ledit objectif peut justifier le traitement effectué par un tel opérateur lorsqu'il est objectivement nécessaire au respect d'une obligation légale à laquelle cet opérateur est soumis.

Au vu de tout ce qui précède, il convient de répondre aux troisième et quatrième questions que l'article 6, paragraphe 1, premier alinéa, sous b), du RGPD doit être interprété en ce sens que le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut être considéré comme

étant nécessaire à l'exécution d'un contrat auquel les personnes concernées sont parties, au sens de cette disposition, qu'à la condition que ce traitement soit objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à ces mêmes utilisateurs, de telle sorte que l'objet principal du contrat ne pourrait être atteint en l'absence de ce traitement.

L'article 6, paragraphe 1, premier alinéa, sous f), du RGPD doit être interprété en ce sens qu'un tel traitement ne peut être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, au sens de cette disposition, qu'à la condition que ledit opérateur ait indiqué aux utilisateurs auprès desquels les données ont été collectées un intérêt légitime poursuivi par leur traitement, que ce traitement est opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime et qu'il ressort d'une pondération des intérêts opposés, au regard de l'ensemble des circonstances pertinentes, que les intérêts ou les libertés et les droits fondamentaux de ces utilisateurs ne prévalent pas sur ledit intérêt légitime du responsable du traitement ou d'un tiers.

Sur la cinquième question

En premier lieu, pour autant que cette question vise l'article 6, paragraphe 1, premier alinéa, sous c) et e), du RGPD, il y a lieu de rappeler que, en vertu de ce point c), un traitement de données à caractère personnel est licite s'il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. En outre, selon ce point e), est également licite le traitement qui est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

L'article 6, paragraphe 3, du RGPD précise notamment, à l'égard de ces deux hypothèses de licéité, que le traitement doit être fondé sur le droit de l'Union ou sur le droit de l'État membre auquel le responsable du traitement est soumis, et que cette base juridique doit répondre à un objectif d'intérêt public et être proportionnée à l'objectif légitime poursuivi.

En l'occurrence, la juridiction de renvoi cherche à savoir si un traitement de données à caractère personnel, tel que celui en cause au principal, peut être considéré comme étant justifié au regard de l'article 6, paragraphe 1, premier alinéa, sous c), du RGPD, lorsqu'il vise à « répondre à une demande juridiquement valable de fournir certaines données », et, au regard de l'article 6, paragraphe 1, premier alinéa, sous e), de ce règlement, lorsqu'il a pour objet la « recherche pour le bien de la société » et cherche à « promouvoir la protection, l'intégrité et la sécurité ».

Toutefois, il importe de constater que cette juridiction n'a pas fourni à la Cour les éléments lui permettant de se prononcer concrètement à cet égard.

Il incombera donc à ladite juridiction de vérifier, au regard des conditions énoncées au point 128 du présent arrêt, si ledit traitement peut être considéré comme étant justifié par les finalités avancées.

En particulier, compte tenu de ce qui a été relevé au point 124 du présent arrêt, il lui appartiendra de rechercher, aux fins de l'application de l'article 6, paragraphe 1, premier alinéa, sous c), du RGPD, si Meta Platforms Ireland est soumise à une obligation légale de collecte et de conservation des données à caractère personnel de manière préventive en vue de pouvoir répondre à toute demande d'une autorité nationale visant à obtenir certaines données relatives à ses utilisateurs.

De même, il appartiendra à ladite juridiction d'apprécier, au regard de l'article 6, paragraphe 1, premier alinéa, sous e), du RGPD, si Meta Platforms Ireland est investie d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, notamment en vue d'assurer la recherche pour le bien de la société ainsi que de promouvoir la protection, l'intégrité et la sécurité, étant précisé que, au vu de la nature et du caractère essentiellement économique et commercial de son activité, il apparaît peu probable que cet opérateur privé soit investi d'une telle mission.

En outre, la juridiction de renvoi devra, le cas échéant, vérifier si, compte tenu de l'ampleur du traitement de données effectué par Meta Platforms Ireland et de son incidence importante pour les utilisateurs du réseau social Facebook, ce traitement est opéré dans les limites du strict nécessaire.

En ce qui concerne, en second lieu, l'article 6, paragraphe 1, premier alinéa, sous d), du RGPD, cette disposition prévoit que le traitement de données à caractère personnel est licite lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Ainsi qu'il ressort du considérant 46 de ce règlement, cette disposition vise la situation particulière dans laquelle le traitement de données à caractère personnel est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. À cet égard, ce considérant cite notamment à titre d'exemples les fins humanitaires, telles que le suivi des épidémies et de leur propagation, ainsi que les cas d'urgence humanitaire, tels que les situations de catastrophe naturelle et d'origine humaine.

Il ressort de ces exemples ainsi que de l'interprétation stricte qu'il convient de retenir de l'article 6, paragraphe 1, premier alinéa, sous d), du RGPD que, au vu de la nature des services fournis par l'opérateur d'un réseau social en ligne, un tel opérateur, dont l'activité revêt un caractère essentiellement économique et commercial, ne saurait invoquer la protection d'un intérêt essentiel à la vie de ses utilisateurs ou d'une autre personne pour justifier, dans l'absolu et de manière purement abstraite et préventive, la licéité d'un traitement de données tel que celui en cause au principal.

Au vu de ce qui précède, il convient de répondre à la cinquième question que l'article 6, paragraphe 1, premier alinéa, sous c), du RGPD doit être interprété en ce sens que le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, est justifié, au titre de cette disposition, lorsqu'il est effectivement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, en vertu d'une disposition du droit de l'Union ou du droit de l'État membre concerné, que cette base

juridique répond à un objectif d'intérêt public et est proportionnée à l'objectif légitime poursuivi et que ce traitement est opéré dans les limites du strict nécessaire.

L'article 6, paragraphe 1, premier alinéa, sous d) et sous e), du RGPD doit être interprété en ce sens qu'un tel traitement de données à caractère personnel ne peut, en principe et sous réserve d'une vérification à effectuer par la juridiction de renvoi, être considéré comme étant nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, au sens du point d), ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, au sens du point e).

Sur la sixième question

Par sa sixième question, la juridiction de renvoi demande, en substance, si l'article 6, paragraphe 1, premier alinéa, sous a), et l'article 9, paragraphe 2, sous a), du RGPD doivent être interprétés en ce sens qu'un consentement donné par l'utilisateur d'un réseau social en ligne à l'opérateur d'un tel réseau peut être considéré comme satisfaisant aux conditions de validité prévues à l'article 4, point 11, de ce règlement, en particulier à celle selon laquelle ce consentement doit être donné librement, lorsque cet opérateur occupe une position dominante sur le marché des réseaux sociaux en ligne.

L'article 6, paragraphe 1, premier alinéa, sous a), et l'article 9, paragraphe 2, sous a), du RGPD exigent le consentement de la personne concernée aux fins, respectivement, du traitement, pour une ou plusieurs finalités spécifiques, de ses données à caractère personnel ainsi que du traitement de catégories particulières de données visées à cet article 9, paragraphe 1.

De son côté, l'article 4, point 11, du RGPD définit la notion de « consentement » comme étant « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Au regard des interrogations de la juridiction de renvoi, il importe de rappeler, en premier lieu, que, conformément au considérant 42 du RGPD, le consentement ne peut être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

En deuxième lieu, le considérant 43 de ce règlement énonce que, pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement. Ce considérant précise également que le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel, bien que cela soit approprié dans le cas d'espèce.

En troisième lieu, l'article 7, paragraphe 4, du RGPD prévoit que, au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution de ce contrat.

C'est sur la base de ces considérations qu'il convient de répondre à la sixième question.

À cet égard, il importe de constater que, certes, la circonstance que l'opérateur d'un réseau social en ligne, en tant que responsable du traitement, occupe une position dominante sur le marché des réseaux sociaux ne fait pas obstacle en tant que telle à ce que les utilisateurs de ce réseau social puissent valablement consentir, au sens de l'article 4, point 11, du RGPD, au traitement de leurs données à caractère personnel, effectué par cet opérateur.

Il n'en reste pas moins que, ainsi que l'a relevé, en substance, M. l'avocat général au point 75 de ses conclusions, une telle circonstance doit être prise en considération dans l'appréciation du caractère valable et, notamment, libre du consentement donné par l'utilisateur dudit réseau, dès lors qu'elle est susceptible d'affecter la liberté de choix de cet utilisateur qui pourrait ne pas être en mesure de refuser ou de retirer son consentement sans subir un préjudice, ainsi que l'indique le considérant 42 du RGPD.

En outre, l'existence d'une telle position dominante est susceptible de créer un déséquilibre manifeste, au sens du considérant 43 du RGPD, entre la personne concernée et le responsable du traitement, ce déséquilibre favorisant notamment l'imposition de conditions qui ne sont pas strictement nécessaires à l'exécution du contrat, ce qui doit être pris en compte conformément à l'article 7, paragraphe 4, de ce règlement. Dans ce contexte, il y a lieu de rappeler que, ainsi qu'il a été relevé aux points 102 à 104 du présent arrêt, il n'apparaît pas, sous réserve des vérifications à effectuer par la juridiction de renvoi, que le traitement en cause au principal soit strictement nécessaire à l'exécution du contrat entre Meta Platforms Ireland et les utilisateurs du réseau social Facebook.

Ainsi, ces utilisateurs doivent disposer de la liberté de refuser individuellement, dans le cadre du processus contractuel, de donner leur consentement à des opérations particulières de traitement de données non nécessaires à l'exécution du contrat sans qu'ils soient pour autant tenus de renoncer intégralement à l'utilisation du service offert par l'opérateur du réseau social en ligne, ce qui implique que lesdits utilisateurs se voient proposer, le cas échéant contre une rémunération appropriée, une alternative équivalente non accompagnée de telles opérations de traitement de données.

De plus, compte tenu de l'ampleur du traitement des données en question et de l'impact important de celui-ci sur les utilisateurs de ce réseau ainsi que de la circonstance que ces utilisateurs ne sauraient raisonnablement s'attendre à ce que des données autres que celles relatives à leur comportement à l'intérieur du réseau social soient traitées par l'opérateur de celui-ci, il est approprié, au sens de ce considérant 43, qu'un consentement distinct puisse être donné pour le traitement de ces dernières données, d'une part, et des données *off* Facebook, d'autre part. Il appartient à la juridiction de renvoi de vérifier l'existence d'une telle possibilité, en l'absence de laquelle le consentement desdits utilisateurs au traitement des données *off* Facebook doit être présumé ne pas avoir été donné librement.

Enfin, il importe de rappeler que, en vertu de l'article 7, paragraphe 1, du RGPD, dans les cas où le traitement repose sur le consentement, la charge de démontrer que la personne concernée a donné son consentement au

traitement de données à caractère personnel la concernant pèse sur le responsable du traitement.

C'est à la lumière de ces critères et d'un examen détaillé de toutes les circonstances de l'espèce qu'il appartiendra à la juridiction de renvoi de déterminer si les utilisateurs du réseau social Facebook ont valablement et, notamment, librement donné leur consentement au traitement en cause au principal.

Compte tenu de ce qui précède, il y a lieu de répondre à la sixième question que l'article 6, paragraphe 1, premier alinéa, sous a), et l'article 9, paragraphe 2, sous a), du RGPD doivent être interprétés en ce sens que la circonstance que l'opérateur d'un réseau social en ligne occupe une position dominante sur le marché des réseaux sociaux en ligne ne fait pas obstacle en tant que telle à ce que les utilisateurs d'un tel réseau puissent valablement consentir, au sens de l'article 4, point 11, de ce règlement, au traitement de leurs données à caractère personnel, effectué par cet opérateur. Cette circonstance constitue néanmoins un élément important pour déterminer si le consentement a effectivement été donné valablement et, notamment, librement, ce qu'il incombe audit opérateur de prouver.

Sur les dépens

La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

Les articles 51 et suivants 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 (règlement général sur la protection des données), ainsi que l'article 4, paragraphe 3, TUE

doivent être interprétés en ce sens que :

sous réserve du respect de son obligation de coopération loyale avec les autorités de contrôle, une autorité de la concurrence d'un État membre peut constater, dans le cadre de l'examen d'un abus de position dominante de la part d'une entreprise, au sens de l'article 102 TFUE, que les conditions générales d'utilisation de cette entreprise relatives au traitement des données à caractère personnel et leur mise en œuvre ne sont pas conformes à ce règlement, lorsque ce constat est nécessaire pour établir l'existence d'un tel abus.

Au vu de cette obligation de coopération loyale, l'autorité de la concurrence nationale ne peut s'écarter d'une décision de l'autorité de contrôle nationale compétente ou de l'autorité de contrôle chef de file compétente relative à ces conditions générales ou à des conditions générales similaires. Lorsqu'elle nourrit des doutes à l'égard de la portée d'une telle décision, lorsque lesdites conditions ou des conditions similaires font, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête ou de décision desdites autorités, l'autorité de la concurrence considère que les conditions en cause ne sont pas conformes au règlement 2016/679, elle doit consulter ces mêmes autorités de contrôle et solliciter leur coopération, afin de lever ses doutes ou de déterminer s'il y a lieu d'attendre l'adoption d'une décision de leur part avant d'entamer sa propre appréciation. En l'absence d'objection de leur part ou de réponse dans un délai raisonnable, l'autorité de la concurrence nationale peut poursuivre sa propre enquête.

L'article 9, paragraphe 1, du règlement 2016/679

doit être interprété en ce sens que :

dans le cas où un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à cette disposition et, le cas échéant, y insère des données en s'inscrivant ou en effectuant des commandes en ligne, le traitement de données à caractère personnel par l'opérateur de ce réseau social en ligne, consistant en la collecte, au moyen d'interfaces intégrées, de *cookies* ou de technologies d'enregistrement similaires, des données issues de la consultation de ces sites et de ces applications ainsi que des données insérées par l'utilisateur, en la mise en relation de l'ensemble de ces données avec le compte du réseau social de celui-ci et en l'utilisation desdites données par cet opérateur, doit être considéré comme un « traitement portant sur des catégories particulières de données à caractère personnel », au sens de ladite disposition, qui est en principe interdit, sous réserve des dérogations prévues à cet article 9, paragraphe 2, lorsque ce traitement de données permet de révéler des informations relevant d'une de ces catégories, que ces informations concernent un utilisateur de ce réseau ou toute autre personne physique.

L'article 9, paragraphe 2, sous e), du règlement 2016/679

doit être interprété en ce sens que :

lorsqu'un utilisateur d'un réseau social en ligne consulte des sites Internet ou des applications en rapport avec une ou plusieurs des catégories visées à l'article 9, paragraphe 1, de ce règlement, il ne rend pas manifestement publiques, au sens de la première de ces dispositions, les données relatives à cette consultation, collectées par l'opérateur de ce réseau social en ligne à travers des *cookies* ou des technologies d'enregistrement similaires.

Lorsqu'il insère des données dans de tels sites Internet ou dans de telles applications ou lorsqu'il active des boutons de sélection intégrés à ces sites et à ces applications, tels que les boutons « j'aime » ou « partager » ou les boutons permettant à l'utilisateur de s'identifier sur ces sites ou ces applications en utilisant les identifiants de connexion liés à son compte d'utilisateur du réseau social, son numéro de téléphone ou son adresse électronique, un tel utilisateur ne rend manifestement publiques, au sens de cet article 9, paragraphe 2, sous e), les données ainsi insérées ou résultant de l'activation de ces boutons que dans le cas où il a explicitement exprimé son choix au préalable, le cas échéant sur la base d'un paramétrage individuel effectué en toute connaissance de cause, de rendre les données le concernant publiquement accessibles à un nombre illimité de personnes.

L'article 6, paragraphe 1, premier alinéa, sous b), du règlement 2016/679
doit être interprété en ce sens que :
le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut être considéré comme étant nécessaire à l'exécution d'un contrat auquel les personnes concernées sont parties, au sens de cette disposition, qu'à la condition que ce traitement soit objectivement indispensable pour réaliser une finalité faisant partie intégrante de la prestation contractuelle destinée à ces mêmes utilisateurs, de telle sorte que l'objet principal du contrat ne pourrait être atteint en l'absence de ce traitement.

L'article 6, paragraphe 1, premier alinéa, sous f), du règlement 2016/679
doit être interprété en ce sens que :
le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut être considéré comme étant nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, au sens de cette disposition, qu'à la condition que ledit opérateur ait indiqué aux utilisateurs auprès desquels les données ont été collectées un intérêt légitime poursuivi par leur traitement, que ce traitement est opéré dans les limites du strict nécessaire pour la réalisation de cet intérêt légitime et qu'il ressort d'une pondération des intérêts opposés, au regard de l'ensemble des circonstances pertinentes, que les intérêts ou les libertés et les droits fondamentaux de ces utilisateurs ne prévalent pas sur ledit intérêt légitime du responsable du traitement ou d'un tiers.

L'article 6, paragraphe 1, premier alinéa, sous c), du règlement 2016/679
doit être interprété en ce sens que :
le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, est justifié, au titre de cette disposition, lorsqu'il est effectivement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, en vertu d'une disposition du droit de l'Union ou du droit de l'État membre concerné, que cette base juridique répond à un objectif d'intérêt public et est proportionnée à l'objectif légitime poursuivi et que ce traitement est opéré dans les limites du strict nécessaire.

L'article 6, paragraphe 1, premier alinéa, sous d) et sous e), du règlement 2016/679
doit être interprété en ce sens que :
le traitement de données à caractère personnel effectué par un opérateur d'un réseau social en ligne, consistant en la collecte de données des utilisateurs d'un tel réseau issues d'autres services du groupe auquel appartient cet opérateur ou issues de la consultation par ces utilisateurs de sites Internet ou d'applications tiers, en la mise en relation de ces données avec le compte du réseau social desdits utilisateurs et en l'utilisation desdites données, ne peut, en principe et sous réserve d'une vérification à effectuer par la juridiction de renvoi, être considéré comme étant nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, au sens du point d), ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, au sens du point e).

L'article 6, paragraphe 1, premier alinéa, sous a), et l'article 9, paragraphe 2, sous a), du règlement 2016/679
doivent être interprétés en ce sens que :
la circonstance que l'opérateur d'un réseau social en ligne occupe une position dominante sur le marché des réseaux sociaux en ligne ne fait pas obstacle en tant que telle à ce que les utilisateurs d'un tel réseau puissent valablement consentir, au sens de l'article 4, point 11, de ce règlement, au traitement de leurs données à caractère personnel, effectué par cet opérateur. Cette circonstance constitue néanmoins un élément important pour déterminer si le consentement a effectivement été donné valablement et, notamment, librement, ce qu'il incombe audit opérateur de prouver.

Signatures

---

* Langue de procédure : l'allemand.