



Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

4 octobre 2024*

« Renvoi préjudiciel – Protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière – Directive (UE) 2016/680 – Article 3, point 2 – Notion de “traitement” – Article 4 – Principes relatifs au traitement des données à caractère personnel – Article 4, paragraphe 1, sous c) – Principe de la “minimisation des données” – Articles 7, 8 et 47 ainsi que article 52, paragraphe 1, de la charte des droits fondamentaux de l’Union européenne – Exigence selon laquelle une limitation de l’exercice d’un droit fondamental doit être « prévue par la loi » – Proportionnalité – Appréciation de la proportionnalité au regard de l’ensemble des éléments pertinents – Contrôle préalable par une juridiction ou une autorité administrative indépendante – Article 13 – Informations à mettre à la disposition de la personne concernée ou à lui fournir – Limites – Article 54 – Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant – Enquête policière en matière de trafic de stupéfiants – Tentative de déverrouillage d’un téléphone portable par les autorités de police, en vue d’accéder, aux fins de cette enquête, aux données contenues dans ce téléphone »

Dans l’affaire C-548/21,

ayant pour objet une demande de décision préjudicielle au titre de l’article 267 TFUE, introduite par le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol, Autriche), par décision du 1^{er} septembre 2021, parvenue à la Cour le 6 septembre 2021, dans la procédure

CG

contre

Bezirkshauptmannschaft Landeck,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. L. Bay Larsen, vice-président, M^{me} K. Jürimäe, MM. C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi et M^{me} O. Spineanu-Matei, présidents de chambre, MM. P. G. Xuereb (rapporteur), I. Jarukaitis, A. Kumin, N. Jääskinen et M. Gavalec, juges,

avocat général : M. M. Campos Sánchez-Bordona,

greffier : M. C. Di Bella, administrateur,

* Langue de procédure : l’allemand

vu la procédure écrite et à la suite de l'audience du 16 janvier 2023,

considérant les observations présentées :

- pour le gouvernement autrichien, par M. A. Posch, M^{me} J. Schmoll, MM. K. Ibili et E. Riedl, en qualité d'agents,
- pour le gouvernement danois, par M. M. P. B. Jespersen, M^{mes} V. Pasternak Jørgensen, M. Søndahl Wolff et Y. T. Thyregod Kollberg, en qualité d'agents,
- pour le gouvernement allemand, par MM. J. Möller et M. Hellmann, en qualité d'agents,
- pour le gouvernement estonien, par M^{me} M. Kriisa, en qualité d'agent,
- pour l'Irlande, par M^{me} M. Browne, Chief State Solicitor, M. A. Joyce et M^{me} M. Lane, en qualité d'agents, assistés de M. R. Farrell, SC, M. D. Fennelly, BL, et M. D. O'Reilly, solicitor,
- pour le gouvernement français, par M. R. Bénard, M^{mes} A. Daniel, A.-L. Desjonquères et M. J. Illouz, en qualité d'agents,
- pour le gouvernement chypriote, par M^{me} I. Neophytou, en qualité d'agent,
- pour le gouvernement hongrois, par M^{me} Zs. Biró-Tóth et M. M. Z. Fehér, en qualité d'agents,
- pour le gouvernement néerlandais, par M^{mes} M. K. Bulterman, A. Hanje et M. J. Langer, en qualité d'agents,
- pour le gouvernement polonais, par M. B. Majczyna, en qualité d'agent,
- pour le gouvernement finlandais, par M^{me} A. Laine, en qualité d'agent,
- pour le gouvernement suédois, par M. J. Lundberg, M^{mes} H. Eklinder, C. Meyer-Seitz, A. M. Runeskjöld, M. Salborn Hodgson, R. Shahsavan Eriksson, H. Shev et M. O. Simonsson, en qualité d'agents,
- pour le gouvernement norvégien, par M. F. Bergsjø, M^{mes} H. Busch, K. Moe Winther et M. P. Wennerås, en qualité d'agents,
- pour la Commission européenne, par MM. G. Braun, S. L. Kaléda, H. Kranenborg et F. Wilman, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 20 avril 2023,

rend le présent

Arrêt

- 1 La demande de décision préjudicielle porte sur l'interprétation de l'article 5 et de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »), lu à la lumière des articles 7, 8, 11, 41 et 47 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).
- 2 Cette demande a été présentée dans le cadre d'un litige opposant CG à la Bezirkshauptmannschaft Landeck (autorité administrative du district de Landeck, Autriche) au sujet de la saisie du téléphone portable de CG par les autorités de police et des tentatives de celles-ci, dans le cadre d'une enquête en matière de trafic de stupéfiants, de déverrouiller ce téléphone pour accéder aux données contenues dans celui-ci.

Le cadre juridique

Le droit de l'Union

La directive 2002/58

- 3 L'article 1^{er} de la directive 2002/58, intitulé « Champ d'application et objectif », dispose :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans la Communauté.

[...]

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité [FUE], telles que celles visées dans les titres V et VI du traité [UE], et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. »
- 4 L'article 3 de cette directive, intitulé « Services concernés », prévoit :

« La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification. »

5 L'article 5 de ladite directive, intitulé « Confidentialité des communications », dispose, à son paragraphe 1 :

« Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. »

6 L'article 15 de la même directive, intitulé « Application de certaines dispositions de la directive 95/46/CE », énonce, à son paragraphe 1 :

« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE [du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31)]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, [TUE]. »

La directive (UE) 2016/680

7 Les considérants 2, 4, 7, 10, 11, 15, 26, 37, 44, 46 et 104 de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89), sont libellés comme suit :

« (2) Les principes et les règles applicables en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. La présente directive vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice.

[...]

- (4) Il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union [européenne], et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. Ces évolutions obligent à mettre en place dans l'Union un cadre pour la protection des données à caractère personnel solide et plus cohérent, assorti d'une application rigoureuse des règles.

[...]

- (7) Il est crucial d'assurer un niveau élevé et homogène de protection des données à caractère personnel des personnes physiques et de faciliter l'échange de données à caractère personnel entre les autorités compétentes des États membres, afin de garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière. À cette fin, le niveau de protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait être équivalent dans tous les États membres. Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige non seulement de renforcer les droits des personnes concernées et les obligations de ceux qui traitent les données à caractère personnel, mais aussi de renforcer les pouvoirs équivalents de suivi et de contrôle du respect des règles relatives à la protection des données à caractère personnel dans les États membres.

[...]

- (10) Dans la déclaration n° 21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière, annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne, la conférence a reconnu que des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation des données à caractère personnel dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 [TFUE] pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines.
- (11) Il convient dès lors que ces domaines soient régis par une directive qui fixe les règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, en respectant la nature spécifique de ces activités. Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. Lorsqu'un tel organisme ou une telle entité traite des données à caractère personnel à des fins autres que celles prévues dans la présente directive, le 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)] s'applique. Par conséquent, le [règlement 2016/679] s'applique lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. [...]

[...]

- (15) Afin d'assurer le même niveau de protection pour les personnes physiques à l'aide de droits opposables dans l'ensemble de l'Union et d'éviter que des divergences n'entravent les échanges de données à caractère personnel entre les autorités compétentes, la présente directive devrait prévoir des règles harmonisées pour la protection et la libre circulation des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Le rapprochement des législations des États membres ne devrait pas conduire à un affaiblissement de la protection des données à caractère personnel qu'elles offrent mais devrait, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans l'Union. Il convient que les États membres ne soient pas empêchés de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes.

[...]

- (26) [...] Les données à caractère personnel devraient être adéquates et pertinentes au regard des finalités pour lesquelles elles sont traitées. Il convient notamment de veiller à ce que les données à caractère personnel collectées ne soient pas excessives, ni conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. [...]

[...]

- (37) Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et 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 la présente directive n'implique pas que l'Union adhère à des théories tendant à établir l'existence de races humaines distinctes. Ces données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne s'accompagne de garanties appropriées pour les droits et libertés de la personne concernée fixées par la loi et ne soit permis dans des cas autorisés par la loi ; lorsqu'il n'est pas déjà autorisé par une telle loi, qu'il ne soit nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ; ou qu'il ne porte sur des données manifestement rendues publiques par la personne concernée. Des garanties appropriées pour les droits et des libertés de la personne concernée pourraient comprendre la

possibilité de ne collecter ces données qu'en rapport avec d'autres données relatives à la personne physique concernée, la possibilité de sécuriser les données collectées de manière adéquate, des règles plus strictes pour l'accès du personnel de l'autorité compétente aux données et l'interdiction de la transmission de ces données. Il convient également que le traitement de pareilles données soit autorisé par la loi lorsque la personne concernée a expressément marqué son accord au traitement qui est particulièrement intrusif pour elle. Toutefois, l'accord de la personne concernée ne devrait pas constituer en soi une base juridique pour le traitement de ces données à caractère personnel sensibles par les autorités compétentes.

[...]

- (44) Les États membres devraient pouvoir adopter des mesures législatives visant à retarder ou à limiter l'information des personnes concernées ou à ne pas leur accorder cette information, ou à leur limiter, complètement ou partiellement, l'accès aux données à caractère personnel les concernant, dès lors qu'une telle mesure constitue une mesure nécessaire et proportionnée dans une société démocratique, compte dûment tenu des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires, pour éviter de nuire à la prévention et à la détection des infractions pénales, aux enquêtes et poursuites en la matière ou à l'exécution de sanctions pénales, pour sauvegarder la sécurité publique ou la sécurité nationale, ou pour protéger les droits et libertés d'autrui. Le responsable du traitement devrait apprécier, en examinant chaque cas de façon concrète et individuelle, s'il y a lieu de limiter le droit d'accès partiellement ou complètement.

[...]

- (46) Toute limitation des droits de la personne concernée doit respecter la Charte et la [convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950], telles qu'elles sont interprétées respectivement par la Cour de justice [de l'Union européenne] et par la Cour européenne des droits de l'homme dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés.

[...]

- (104) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la Charte, tels qu'ils sont consacrés par le [traité FUE] et notamment le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à accéder à un tribunal impartial. Les limitations apportées à ces droits sont conformes à l'article 52, paragraphe 1, de la Charte car elles sont nécessaires pour répondre à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. »

8 L'article 1^{er} de cette directive, intitulé « Objet et objectifs », dispose, à ses paragraphes 1 et 2 :

« 1. La présente directive établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière

ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

2. Conformément à la présente directive, les États membres :

- a) protègent les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ; et
- b) veillent à ce que l'échange de données à caractère personnel par les autorités compétentes au sein de l'Union, lorsque cet échange est requis par le droit de l'Union ou le droit d'un État membre, ne soit ni limité ni interdit pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. »

9 L'article 2 de ladite directive, intitulé « Champ d'application », prévoit, à ses paragraphes 1 et 3 :

« 1. La présente directive s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins énoncées à l'article 1^{er}, paragraphe 1.

[...]

3. La présente directive ne s'applique pas au traitement de données à caractère personnel effectué :

- a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;

[...] »

10 Aux termes de l'article 3 de la même directive, intitulé « Définitions » :

« Aux fins de la présente directive, on entend par :

- 1. "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- 2. "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel 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 ;

[...]

7. "autorité compétente" :

- a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; ou
- b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

[...] »

- 11 L'article 4 de la directive 2016/680, intitulé « Principes relatifs au traitement des données à caractère personnel », dispose, à son paragraphe 1 :

« Les États membres prévoient que les données à caractère personnel sont :

- a) traitées de manière licite et loyale ;
- b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ;
- c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;

[...] »

- 12 L'article 6 de cette directive, intitulé « Distinction entre différentes catégories de personnes concernées », énonce :

« Les États membres prévoient que le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

- a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;
- b) les personnes reconnues coupables d'une infraction pénale ;
- c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale ; et
- d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points a) et b). »

13 L'article 10 de ladite directive, intitulé « Traitement portant sur des catégories particulières de données à caractère personnel », est rédigé en ces termes :

« Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et 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 est autorisé uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

- a) lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre ;
- b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;
ou
- c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. »

14 L'article 13 de la directive 2016/680, intitulé « Informations à mettre à la disposition de la personne concernée ou à lui fournir », dispose :

« 1. Les États membres prévoient que le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes :

- a) l'identité et les coordonnées du responsable du traitement ;
- b) le cas échéant, les coordonnées du délégué à la protection des données ;
- c) les finalités du traitement auquel sont destinées les données à caractère personnel ;
- d) le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de ladite autorité ;
- e) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et la limitation du traitement des données à caractère personnel relatives à une personne concernée.

2. En plus des informations visées au paragraphe 1, les États membres prévoient, par la loi, que le responsable du traitement fournit à la personne concernée, dans des cas particuliers, les informations additionnelles suivantes afin de lui permettre d'exercer ses droits :

- a) la base juridique du traitement,
- b) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- c) le cas échéant, les catégories de destinataires des données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales ;

d) au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de la personne concernée.

3. Les États membres peuvent adopter des mesures législatives visant à retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée pour :

- a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ;
- b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;
- c) protéger la sécurité publique ;
- d) protéger la sécurité nationale ;
- e) protéger les droits et libertés d'autrui.

[...] »

15 L'article 54 de cette directive, intitulé « Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant », énonce :

« Les États membres prévoient que, sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, notamment le droit d'introduire une réclamation auprès d'une autorité de contrôle en vertu de l'article 52, une personne concernée a droit à un recours juridictionnel effectif lorsqu'elle considère que ses droits prévus dans les dispositions adoptées en vertu de la présente directive ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation desdites dispositions. »

Le droit autrichien

16 L'article 27, paragraphe 1, du Suchtmittelgesetz (loi sur les stupéfiants), du 5 septembre 1997 (BGBl. I, 112/1997), dans sa version applicable au litige au principal, dispose :

« Quiconque, illégalement

- 1. Acquiert, possède, produit, transporte, importe, exporte ou offre, donne ou procure des stupéfiants à une autre personne,

[...]

est passible d'une peine de prison pouvant aller jusqu'à un an ou d'une amende pouvant aller jusqu'à 360 jours-amendes.

[...] »

17 L'article 17 du Strafgesetzbuch (code pénal), du 1^{er} janvier 1975 (BGBl., 60/1974), dans sa version applicable au litige au principal (ci-après le « StGB »), énonce :

« (1) Les crimes sont des actes intentionnels passibles de la prison à vie ou d'une peine d'emprisonnement de plus de trois ans.

(2) Toutes les autres infractions sont des délits. »

18 L'article 18 de la Strafprozessordnung (code de procédure pénale), du 30 décembre 1975 (BGBl., 631/1975), dans sa version applicable au litige au principal (ci-après la « StPO »), prévoit :

« (1) La police judiciaire est chargée de missions au service de l'administration de la justice pénale (article 10, paragraphe 1, point 6, du Bundes-Verfassungsgesetz [(Loi constitutionnelle fédérale)]).

(2) Les enquêtes de police judiciaire relèvent de la responsabilité des autorités de sûreté, dont l'organisation et la compétence territoriale sont régies par les dispositions du Sicherheitspolizeigesetz [(loi sur la police de sûreté)] relatives à l'organisation de l'administration de la sûreté publique.

(3) Les organes du service de sûreté publique (article 5, deuxième alinéa, du Sicherheitspolizeigesetz [(loi sur la police de sûreté)]) assurent le service exécutif de la police judiciaire, qui consiste à investiguer et à poursuivre les infractions pénales conformément aux dispositions de la présente loi.

[...] »

19 L'article 99, paragraphe 1, de la StPO dispose :

« La police judiciaire enquête d'office ou sur la base d'une plainte ; elle est tenue de se conformer aux ordres du ministère public et de la justice (article 105, paragraphe 2). »

Le litige au principal et les questions préjudicielles

20 Le 23 février 2021, à l'occasion d'un contrôle en matière de stupéfiants, des agents du bureau de douane d'Innsbruck (Autriche) ont saisi un colis adressé à CG, contenant 85 grammes de cannabis. Ce colis a été transmis, pour examen, au commissariat central de police de St. Anton am Arlberg (Autriche).

21 Le 6 mars 2021, deux agents de police de ce commissariat ont effectué une perquisition du domicile de CG, au cours de laquelle ils l'ont interrogé au sujet de l'expéditeur dudit colis et ont fouillé son logement. Au cours de cette perquisition, les fonctionnaires de police ont demandé à accéder aux données de connexion du téléphone portable de CG. À la suite du refus opposé par ce dernier, ces agents de police ont procédé à la saisie de ce téléphone portable, comportant une carte SIM et une carte SD, et ont remis à CG le procès-verbal de saisie.

22 Par la suite, ledit téléphone portable a été remis, en vue de son déverrouillage, à un expert du poste de police du district de Landeck (Autriche). Celui-ci n'étant pas parvenu à déverrouiller le téléphone portable en cause, ce dernier a été envoyé au Bundeskriminalamt (Office fédéral de la police judiciaire) de Vienne (Autriche), où une nouvelle tentative de déverrouillage a été effectuée.

- 23 La saisie du téléphone portable de CG ainsi que les tentatives d'exploitation ultérieures de ce téléphone ont été effectuées de la propre initiative des agents de police concernés, sans que ceux-ci y aient été autorisés par le ministère public ou un juge.
- 24 Le 31 mars 2021, CG a introduit un recours devant le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol, Autriche), qui est la juridiction de renvoi, visant à contester la légalité de la saisie de son téléphone portable. Ce dernier a été restitué à CG le 20 avril 2021.
- 25 CG n'a pas été immédiatement informé des tentatives d'exploitation de son téléphone portable. Il en a seulement eu connaissance lorsque l'agent de police ayant procédé à la saisie de ce téléphone portable et entamé, par la suite, les démarches visant à en exploiter les données numériques a été interrogé en tant que témoin dans le cadre de la procédure pendante devant la juridiction de renvoi. Ces tentatives n'ont pas non plus été documentées dans le dossier de la police judiciaire.
- 26 Au vu de ces éléments, la juridiction de renvoi se demande, en premier lieu, si, au regard des points 52 à 61 de l'arrêt du 2 octobre 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788), et de la jurisprudence citée à ces points, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens qu'un accès complet et non contrôlé à l'ensemble des données contenues dans un téléphone portable, à savoir les données de connexion, le contenu des communications, les photographies et les historiques de navigation, lesquelles peuvent fournir une image très détaillée et approfondie de presque tous les domaines de la vie privée de la personne concernée, constitue une ingérence tellement grave dans les droits fondamentaux consacrés à ces articles 7 et 8 que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, cet accès doit être limité à la lutte contre les infractions graves.
- 27 À cet égard, cette juridiction précise que l'infraction qui est reprochée à CG dans le cadre de la procédure d'enquête pénale en cause au principal est prévue à l'article 27, paragraphe 1, de la loi sur les stupéfiants et passible d'une peine d'emprisonnement d'un an au maximum et ne constitue, au regard de la classification de l'article 17 du StGB, qu'un délit.
- 28 En deuxième lieu, après avoir rappelé les enseignements découlant des points 48 à 54 de l'arrêt du 2 mars 2021, *Prokuratuur* (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), ainsi que de la jurisprudence citée à ces points, ladite juridiction se demande si l'article 15, paragraphe 1, de la directive 2002/58 s'oppose à une réglementation nationale telle que celle ressortant des dispositions combinées de l'article 18 et de l'article 99, paragraphe 1, de la StPO, en vertu desquelles, au cours d'une procédure d'enquête pénale, la police judiciaire peut se procurer, sans l'autorisation d'un juge ou d'une entité administrative indépendante, un accès complet et non contrôlé à l'ensemble des données numériques contenues dans un téléphone portable.
- 29 En troisième et dernier lieu, après avoir souligné que l'article 18 de la StPO, lu en combinaison avec l'article 99, paragraphe 1, de la StPO, ne prévoit aucune obligation, dans le chef des autorités de police, de documenter les mesures d'exploitation numérique d'un téléphone portable, ou encore d'informer son propriétaire de l'existence de telles mesures, de sorte que celui-ci puisse, le cas échéant, s'y opposer au moyen d'un recours juridictionnel préventif ou a posteriori, la juridiction de renvoi s'interroge sur la compatibilité de ces dispositions de la StPO avec le principe de l'égalité des armes et le droit à un recours juridictionnel effectif, au sens de l'article 47 de la Charte.

- 30 Dans ces conditions, le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :
- « 1) L'article 15, paragraphe 1, [de la directive 2002/58, lu, le cas échéant, en combinaison avec l'article 5 de celle-ci], doit-il, à la lumière des articles 7 et 8 de la [Charte], se comprendre en ce sens que l'accès des autorités publiques aux données stockées dans les téléphones portables constitue une ingérence dans les droits fondamentaux garantis à ces articles de la Charte d'une telle gravité que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, cet accès doit être limité à la lutte contre la criminalité grave ?
- 2) L'article 15, paragraphe 1, de la [directive 2002/58], doit-il, à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], se comprendre en ce sens qu'il s'oppose à une réglementation nationale, telle que les dispositions combinées de l'article 18 et de l'article 99, paragraphe 1, [de la StPO], en vertu de laquelle les autorités nationales chargées de la sécurité se procurent de leur propre initiative, au cours d'une procédure d'enquête pénale, sans l'autorisation d'une juridiction ou d'une autorité administrative indépendante, un accès complet et non contrôlé à l'ensemble des données numériques stockées dans un téléphone portable ?
- 3) L'article 47 de la [Charte] doit-il être compris, lu, le cas échéant, en combinaison avec les articles 41 et 52 de la même Charte, du point de vue de l'égalité des armes et du droit à un recours juridictionnel effectif, comme s'opposant à une réglementation d'un État membre qui, telles les dispositions combinées de l'article 18 et de l'article 99, paragraphe 1, [de la StPO], permet l'exploitation des données numériques d'un téléphone portable sans que la personne concernée soit informée au préalable de la mesure concernée ou, au moins, après qu'elle a été prise ? »

La procédure devant la Cour

- 31 Le 20 octobre 2021, la Cour a adressé une demande d'informations à la juridiction de renvoi par laquelle elle a invité cette juridiction à lui indiquer si la directive 2016/680 pourrait être pertinente dans le cadre de l'affaire au principal et, le cas échéant, de lui exposer les dispositions de droit national transposant cette directive dans le droit autrichien qui pourraient s'appliquer en l'espèce.
- 32 Le 11 novembre 2021, la juridiction de renvoi a répondu à cette demande en indiquant notamment que les prescriptions de ladite directive devaient être respectées dans cette affaire. Cette réponse a été notifiée, avec la décision de renvoi, aux parties intéressées visées à l'article 23 du statut de la Cour de justice de l'Union européenne.
- 33 Le 8 novembre 2022, en application de l'article 61 du règlement de procédure de la Cour, la Cour a demandé aux participants à la phase orale de la procédure de concentrer leurs plaidoiries sur la directive 2016/680 et de répondre, lors de l'audience de plaidoiries, à certaines questions relatives à cette directive.

Sur la demande de réouverture de la phase orale de la procédure

- 34 À la suite de la présentation des conclusions de M. l'avocat général, par acte déposé au greffe de la Cour le 17 mai 2023, le gouvernement autrichien a présenté une demande de rectification de ces conclusions au motif qu'elles présenteraient de façon inexacte la position qu'il a exprimée dans ses observations tant écrites qu'orales et qu'elles comporteraient des erreurs d'ordre factuel.
- 35 En effet, selon ce gouvernement, d'une part, le point 50 des conclusions de M. l'avocat général, lu en combinaison avec la note en bas de page 14 de celles-ci, laisserait entendre que, selon ledit gouvernement, une tentative d'accès aux données contenues dans un téléphone portable, telle que celle en cause au principal, ne saurait constituer un traitement de données à caractère personnel, au sens de l'article 3, point 2, de la directive 2016/680. Or, le même gouvernement aurait soutenu le contraire, lors de l'audience devant la Cour, en se ralliant explicitement à la position exprimée par la Commission européenne dans ses observations écrites, selon laquelle il ressortirait d'une interprétation systémique de cette directive, lue à la lumière de ses objectifs, que celle-ci régit non seulement les traitements proprement dits, mais également des opérations intervenant en amont de ceux-ci, telles qu'une tentative de traitement, sans que l'application de ladite directive soit subordonnée à la condition que cette tentative de traitement ait été couronnée de succès.
- 36 D'autre part, le gouvernement autrichien fait valoir que le point 27 des conclusions de M. l'avocat général repose sur des faits erronés, en ce qu'il laisse entendre que les tentatives de traitement mentionnées au point 22 du présent arrêt n'auraient pas été documentées dans le dossier de la police judiciaire. À cet égard, ce gouvernement précise que, contrairement à ce qui ressort de ce point 27 ainsi que de la demande de décision préjudicielle, il a exposé, dans ses observations écrites, que ces tentatives de traitement avaient été consignées dans deux rapports dressés par les agents de police en charge de l'enquête dans l'affaire au principal et que ces rapports avaient, par la suite, été versés au dossier du ministère public.
- 37 Par une décision du président de la Cour du 23 mai 2023, la demande du gouvernement autrichien visant à obtenir la rectification des conclusions de M. l'avocat général a été requalifiée en une demande de réouverture de la phase orale de la procédure, au sens de l'article 83 du règlement de procédure.
- 38 À cet égard, il convient de rappeler, d'une part, que le statut de la Cour de justice de l'Union européenne et le règlement de procédure ne prévoient pas la possibilité, pour les intéressés visés à l'article 23 de ce statut, de présenter des observations en réponse aux conclusions présentées par l'avocat général. D'autre part, en vertu de l'article 252, second alinéa, TFUE, l'avocat général présente publiquement, en toute impartialité et en toute indépendance, des conclusions motivées sur les affaires qui, conformément audit statut, requièrent son intervention. La Cour n'est liée ni par ces conclusions ni par la motivation au terme de laquelle l'avocat général parvient à celles-ci. Par conséquent, le désaccord d'une partie intéressée avec les conclusions de l'avocat général, quelles que soient les questions que ce dernier examine dans ses conclusions, ne peut constituer en soi un motif justifiant la réouverture de la procédure orale (arrêt du 14 mars 2024, f6 Cigarettenfabrik, C-336/22, EU:C:2024:226, point 25 et jurisprudence citée).
- 39 Certes, conformément à l'article 83 de son règlement de procédure, la Cour peut, à tout moment, l'avocat général entendu, ordonner la réouverture de la phase orale de la procédure, notamment si elle considère qu'elle est insuffisamment éclairée, ou lorsqu'une partie a soumis, après la clôture

de cette phase, un fait nouveau de nature à exercer une influence décisive sur la décision de la Cour, ou encore lorsque l'affaire doit être tranchée sur la base d'un argument qui n'a pas été débattu.

- 40 Toutefois, en l'occurrence, la Cour considère qu'elle dispose, au terme de la phase écrite de la procédure et de l'audience qui s'est tenue devant elle, de tous les éléments nécessaires pour statuer sur la présente demande de décision préjudicielle. En outre, les éléments invoqués par le gouvernement autrichien à l'appui de sa demande de réouverture de la phase orale de la procédure ne constituent pas des faits nouveaux de nature à exercer une influence décisive sur la décision qu'elle est appelée à rendre dans la présente affaire.
- 41 S'agissant, plus particulièrement, des éléments d'ordre factuel relevés au point 36 du présent arrêt, il convient de rappeler que, dans le cadre d'une procédure préjudicielle, il incombe à la Cour non pas de déterminer si des faits allégués sont établis, mais uniquement de procéder à l'interprétation des dispositions pertinentes du droit de l'Union (voir, en ce sens, arrêt du 31 janvier 2023, Puig Gordi e.a., C-158/21, EU:C:2023:57, point 36). En effet, selon la jurisprudence de la Cour, les questions relatives à l'interprétation du droit de l'Union sont posées par le juge national dans le cadre réglementaire et factuel qu'il définit sous sa responsabilité, et dont il n'appartient pas à la Cour de vérifier l'exactitude [voir, en ce sens, arrêt du 18 juin 2024, Bundesrepublik Deutschland (Effet d'une décision d'octroi du statut de réfugié), C-753/22, EU:C:2024:524, point 44 et jurisprudence citée].
- 42 Dans ces conditions, la Cour considère, l'avocat général entendu, qu'il n'y a pas lieu d'ordonner la réouverture de la phase orale de la procédure.

Sur la recevabilité de la demande de décision préjudicielle

- 43 Plusieurs des parties intéressées ayant déposé des observations écrites dans le cadre de la présente procédure ont contesté la recevabilité de la demande de décision préjudicielle dans son ensemble ou de certaines des questions posées par la juridiction de renvoi.
- 44 En premier lieu, les gouvernements autrichien, français et suédois font valoir que la décision de renvoi ne remplit pas les exigences prévues à l'article 94 du règlement de procédure, au motif qu'elle ne comporterait pas les éléments de fait et de droit nécessaires pour fournir une réponse utile à cette juridiction.
- 45 En second lieu, le gouvernement autrichien soutient, d'une part, que, par ses deuxième et troisième questions préjudicielles, la juridiction de renvoi souhaite, en substance, savoir si les dispositions des articles 18 et 99 de la StPO, lues ensemble, sont conformes au droit de l'Union. Or, ces dispositions ne fixant pas les conditions dans lesquelles l'exploitation de supports de données saisis doit s'effectuer, ces questions n'auraient aucun rapport avec l'objet du litige au principal. Il fait valoir, d'autre part, que, en vertu du droit autrichien, une ordonnance du ministère public est nécessaire pour procéder à la saisie d'un téléphone portable ou pour tenter d'accéder à des données contenues dans ce téléphone. Cette juridiction devrait donc constater une violation du droit autrichien, de sorte que les questions posées par ladite juridiction ne seraient pas nécessaires à la solution de ce litige et que, partant, il n'y aurait pas lieu de statuer sur la demande de décision préjudicielle.

- 46 Il convient de rappeler, à titre liminaire, que, selon une jurisprudence constante, dans le cadre de la coopération entre la Cour et les juridictions nationales instituée à l'article 267 TFUE, il appartient au seul juge national, qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir, d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, dès lors que les questions posées portent sur l'interprétation du droit de l'Union, la Cour est, en principe, tenue de statuer (arrêt du 24 juillet 2023, Lin, C-107/23 PPU, EU:C:2023:606, point 61 et jurisprudence citée).
- 47 Il s'ensuit que les questions portant sur le droit de l'Union bénéficient d'une présomption de pertinence. Le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation sollicitée du droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées (arrêt du 24 juillet 2023, Lin, C-107/23 PPU, EU:C:2023:606, point 62 et jurisprudence citée).
- 48 S'agissant, en premier lieu, de l'argument tiré du non-respect des exigences prévues à l'article 94 du règlement de procédure, il convient de relever que, selon une jurisprudence constante, désormais reflétée à cet article 94, sous a) et b), la nécessité de parvenir à une interprétation du droit de l'Union qui soit utile pour le juge national exige que celui-ci définisse le cadre factuel et réglementaire dans lequel s'insèrent les questions qu'il pose ou que, à tout le moins, il explique les hypothèses factuelles sur lesquelles ces questions sont fondées. En outre, il est indispensable, comme l'énonce ledit article 94, sous c), que la demande de décision préjudicielle contienne un exposé des raisons qui ont conduit la juridiction de renvoi à s'interroger sur l'interprétation ou la validité de certaines dispositions du droit de l'Union, ainsi que le lien qu'elle établit entre ces dispositions et la réglementation nationale applicable au litige au principal (arrêt du 21 décembre 2023, European Superleague Company, C-333/21, EU:C:2023:1011, point 59 et jurisprudence citée).
- 49 En l'occurrence, s'agissant du cadre factuel, la juridiction de renvoi a précisé, dans sa demande de décision préjudicielle, que les autorités de police autrichiennes, après avoir saisi le téléphone portable de CG dans le cadre d'une enquête policière en matière de trafic de stupéfiants, ont tenté, à deux reprises, d'avoir accès aux données contenues dans ce téléphone, de leur propre initiative, sans disposer d'une autorisation préalable du ministère public ou d'un juge à cet effet. Elle a également précisé que CG avait seulement pris connaissance des tentatives d'accès aux données contenues dans son téléphone portable au moment où il a entendu le témoignage d'un agent de police. Enfin, elle a indiqué que ces tentatives d'accès n'avaient pas non plus été documentées dans le dossier constitué par la police judiciaire.
- 50 S'agissant du cadre réglementaire, cette juridiction a précisé que les dispositions nationales qu'elle a mentionnées dans la décision de renvoi permettaient une tentative d'accès aux données contenues dans un téléphone portable à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans limiter cette possibilité aux seules fins de la lutte contre la criminalité grave, sans soumettre cette tentative d'accès à un contrôle préalable par un juge ou une entité administrative indépendante et sans prévoir que les personnes concernées soient informées de ladite tentative, en vue, notamment, de pouvoir s'y opposer par l'introduction d'un recours juridictionnel.

- 51 En outre, ladite juridiction a précisé, ainsi que cela ressort des points 26 à 29 du présent arrêt, les raisons qui l'ont amenée à présenter sa demande de décision préjudicielle à la Cour et le lien qui, selon elle, existe entre les dispositions du droit de l'Union et de la Charte visées par cette demande et celles du droit autrichien applicables, selon elle, au litige au principal.
- 52 Les éléments visés aux points 49 à 51 du présent arrêt permettent ainsi de considérer que la demande de décision préjudicielle répond aux exigences prévues à l'article 94 du règlement de procédure.
- 53 En second lieu, s'agissant des arguments tirés de ce que les dispositions du droit autrichien visées aux deuxième et troisième questions préjudicielles ne seraient pas pertinentes et de ce que la juridiction de renvoi aurait dû constater une violation de ce droit, il convient de rappeler qu'il n'appartient pas à la Cour de se prononcer sur l'interprétation des dispositions nationales et de juger si l'interprétation ou l'application qu'en donne le juge national est correcte, une telle interprétation relevant de la compétence exclusive de ce dernier [arrêt du 15 juin 2023, Getin Noble Bank (Suspension de l'exécution d'un contrat de crédit), C-287/22, EU:C:2023:491, point 32 et jurisprudence citée].
- 54 En l'occurrence, il ressort de la demande de décision préjudicielle et, en particulier, du libellé des questions préjudicielles, que la juridiction de renvoi considère, d'une part, que ces dispositions du droit autrichien sont applicables au litige au principal et, d'autre part, qu'une tentative d'accès aux données contenues dans un téléphone portable, sans autorisation préalable du ministère public ou d'un juge, telle que celle en cause au principal, est permise par le droit autrichien. Conformément à la jurisprudence citée au point précédent du présent arrêt, il n'appartient pas à la Cour de se prononcer sur une telle interprétation desdites dispositions.
- 55 Il s'ensuit que les questions posées par la juridiction de renvoi sont recevables.

Sur le fond

- 56 Le gouvernement autrichien fait valoir, dans ses observations écrites, que la Cour n'est pas compétente pour répondre aux première et deuxième questions préjudicielles étant donné que ces questions portent sur l'interprétation de l'article 5 et de l'article 15, paragraphe 1, de la directive 2002/58, alors qu'il est manifeste que cette directive ne s'applique pas au litige au principal. Lors de l'audience, plusieurs gouvernements ont soutenu qu'une reformulation des questions préjudicielles au regard de la directive 2016/680 n'était pas possible. En particulier, le gouvernement autrichien a souligné que le fait que cette dernière directive ne contenait pas de dispositions équivalentes à l'article 5 et à l'article 15, paragraphe 1, de la directive 2002/58 s'opposait à cette reformulation. Le gouvernement français a soutenu, quant à lui, que le pouvoir de reformulation des questions préjudicielles trouvait l'une de ses limites dans le droit, pour les États membres, de présenter des observations écrites. En effet, selon ce dernier gouvernement, ce droit serait privé de toute effectivité si le cadre juridique de la procédure pouvait être radicalement modifié lors de la reformulation des questions préjudicielles par la Cour.
- 57 À cet égard, il convient de rappeler que la Cour a jugé, en se fondant en particulier sur l'article 1^{er}, paragraphes 1 et 3, et l'article 3 de la directive 2002/58, que, lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications, la protection des données des personnes concernées relève non pas de la

directive 2002/58, mais du seul droit national, sous réserve de l'application de la directive 2016/680 (arrêts du 6 octobre 2020, *Privacy International*, C-623/17, EU:C:2020:790, point 48, ainsi que du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 103).

- 58 Or, il est constant que le litige au principal concerne la tentative d'accès à des données à caractère personnel contenues dans un téléphone portable directement par les autorités de police, sans qu'une quelconque intervention d'un fournisseur de services de communications électroniques ait été sollicitée.
- 59 Partant, il est manifeste que ce litige ne relève pas du champ d'application de la directive 2002/58, visée par les première et deuxième questions préjudicielles.
- 60 Il convient toutefois de rappeler que, selon une jurisprudence constante, dans le cadre de la procédure de coopération entre les juridictions nationales et la Cour instituée à l'article 267 TFUE, il appartient à celle-ci de donner au juge national une réponse utile qui lui permette de trancher le litige dont il est saisi. Dans cette optique, il incombe, le cas échéant, à la Cour de reformuler les questions qui lui sont soumises. En outre, la Cour peut être amenée à prendre en considération des normes du droit de l'Union auxquelles le juge national n'a pas fait référence dans l'énoncé de ses questions [arrêts du 15 juillet 2021, *Ministrstvo za obrambo*, C-742/19, EU:C:2021:597, point 31 et jurisprudence citée, ainsi que du 18 juin 2024, *Generalstaatsanwaltschaft Hamm* (Demande d'extradition d'un réfugié vers la Turquie), C-352/22, EU:C:2024:521, point 47].
- 61 En effet, la circonstance qu'une juridiction nationale a, sur un plan formel, formulé une question préjudicielle en se référant à certaines dispositions du droit de l'Union ne fait pas obstacle à ce que la Cour fournisse à cette juridiction tous les éléments d'interprétation qui peuvent être utiles au jugement de l'affaire dont elle est saisie, qu'elle y ait fait ou non référence dans l'énoncé de ses questions. Il appartient, à cet égard, à la Cour d'extraire de l'ensemble des éléments fournis par la juridiction nationale, et notamment de la motivation de la décision de renvoi, les éléments du droit de l'Union qui appellent une interprétation compte tenu de l'objet du litige (arrêt du 22 juin 2022, *Volvo et DAF Trucks*, C-267/20, EU:C:2022:494, point 28 ainsi que jurisprudence citée).
- 62 Certes, en vertu d'une jurisprudence constante, les informations fournies dans la décision de renvoi doivent non seulement permettre à la Cour d'apporter des réponses utiles, mais également donner aux gouvernements des États membres ainsi qu'aux autres parties intéressées la possibilité de présenter des observations conformément à l'article 23 du statut de la Cour de justice de l'Union européenne (arrêt du 21 décembre 2023, *Royal Antwerp Football Club*, C-680/21, EU:C:2023:1010, point 32 et jurisprudence citée).
- 63 Toutefois, ainsi que cela ressort des points 31 à 33 du présent arrêt, en réponse à la demande d'informations adressée par la Cour à la juridiction de renvoi, cette dernière a indiqué que la directive 2016/680 était applicable au litige au principal. Les parties intéressées ont pu, dans leurs observations écrites, prendre position sur l'interprétation de cette directive et sa pertinence pour l'affaire au principal. En outre, en vue de l'audience de plaidoiries, la Cour a demandé aux participants à la phase orale de la procédure de répondre, lors de cette audience, à certaines questions relatives à ladite directive. En particulier, elle les a invitées à prendre position sur la

pertinence de l'article 4 de cette dernière pour répondre à la première question préjudicielle ainsi que sur celle des articles 13 et 54 de la même directive pour répondre à la troisième question préjudicielle.

- 64 Par conséquent, la circonstance que les première et deuxième questions préjudicielles portent sur l'interprétation de l'article 5 et de l'article 15, paragraphe 1, de la directive 2002/58 et non sur la directive 2016/680 ne fait pas obstacle à la reformulation des questions posées par la juridiction de renvoi au regard des dispositions pertinentes, pour la présente affaire, de cette dernière directive et, partant, à la compétence de la Cour pour répondre à ces questions.
- 65 Cette conclusion n'est pas remise en cause par l'argument de l'Irlande ainsi que des gouvernements français et norvégien selon lequel une tentative d'accès à des données à caractère personnel ne relève pas du champ d'application de la directive 2016/680, dès lors que celle-ci ne s'applique qu'aux traitements réalisés effectivement.
- 66 Ces gouvernements font valoir, à cet égard, que l'interprétation des dispositions de cette directive ne serait pas utile à la solution du litige au principal, de même que celle de la Charte, dans la mesure où celle-ci ne trouve à s'appliquer que lorsque les États membres mettent en œuvre le droit de l'Union.
- 67 Toutefois, lorsqu'il n'apparaît pas de manière manifeste que l'interprétation d'un acte de droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal, comme c'est le cas de la directive 2016/680 en l'occurrence, l'objection tirée de l'inapplicabilité de cet acte à l'affaire au principal relève du fond des questions (voir, par analogie, arrêt du 24 juillet 2023, Lin, C-107/23 PPU, EU:C:2023:606, point 66 et jurisprudence citée).
- 68 Ainsi, il convient, au préalable, d'examiner si une tentative d'accès, par des autorités de police, aux données contenues dans un téléphone portable relève du champ d'application matériel de cette directive.

Sur l'application de la directive 2016/680 à une tentative d'accès aux données contenues dans un téléphone portable

- 69 L'article 2, paragraphe 1, de la directive 2016/680 définit le champ d'application matériel de celle-ci. Selon cette disposition, cette directive « s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins énoncées à [son] article 1^{er}, paragraphe 1 », à savoir, notamment, « de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ».
- 70 L'article 3, point 2, de ladite directive définit la notion de « traitement » comme comprenant « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que [...] l'extraction, la consultation » ou encore « la diffusion ou toute autre forme de mise à disposition ».
- 71 Il ressort ainsi du libellé même de l'article 3, point 2, de la directive 2016/680 et notamment de l'utilisation des expressions « toute opération », « tout ensemble d'opérations » et « toute autre forme de mise à disposition » que le législateur de l'Union a entendu donner une portée large à la notion de « traitement » et, partant, au champ d'application matériel de cette directive. Cette interprétation est corroborée par le caractère non exhaustif, exprimé par la locution « telles

que », des opérations mentionnées à cette disposition [voir, par analogie, arrêt du 24 février 2022, *Valsts ienēmumu dienests* (Traitement des données personnelles à des fins fiscales), C-175/20, EU:C:2022:124, point 35].

- 72 Ces éléments textuels militent ainsi dans le sens d'une interprétation selon laquelle, lorsque des autorités de police saisissent un téléphone et le manipulent à des fins d'extraction et de consultation des données à caractère personnel contenues dans ce téléphone, elles entament un traitement, au sens de l'article 3, point 2, de la directive 2016/680, quand bien même ces autorités ne parviendraient pas, pour des raisons techniques, à accéder à ces données.
- 73 Cette interprétation est confirmée par le contexte dans lequel s'inscrit l'article 3, point 2, de la directive 2016/680. En effet, en vertu de l'article 4, paragraphe 1, sous b), de cette directive, les États membres prévoient que les données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités. Cette dernière disposition consacre le principe de limitation des finalités [voir, en ce sens, arrêt du 26 janvier 2023, *Ministerstvo na vatreshnite raboti* (Enregistrement de données biométriques et génétiques par la police), C-205/21, EU:C:2023:49, point 122]. Or, l'effectivité de ce principe exige nécessairement que la finalité de la collecte soit déterminée dès le stade où les autorités compétentes tentent d'accéder à des données à caractère personnel puisqu'une telle tentative, si elle s'avère fructueuse, est de nature à permettre à celles-ci, notamment, de collecter, d'extraire ou de consulter immédiatement les données en cause.
- 74 S'agissant des objectifs de la directive 2016/680, celle-ci vise notamment, ainsi que cela ressort de ses considérants 4, 7 et 15, à assurer un niveau élevé de protection des données à caractère personnel des personnes physiques.
- 75 Or, cet objectif serait remis en cause si une tentative d'accès à des données à caractère personnel contenues dans un téléphone portable ne pouvait pas être qualifiée de « traitement » de ces données. En effet, une interprétation de la directive 2016/680 en ce sens exposerait les personnes concernées par une telle tentative d'accès à un risque important qu'une méconnaissance des principes établis par cette directive ne puisse plus être évitée.
- 76 Il convient encore de relever qu'une telle interprétation est conforme au principe de sécurité juridique, qui, conformément à la jurisprudence constante de la Cour, exige que l'application des règles de droit soit prévisible pour les justiciables, en particulier lorsqu'elles peuvent avoir des conséquences défavorables (arrêt du 27 juin 2024, *Gestore dei Servizi Energetici*, C-148/23, EU:C:2024:555, point 42 et jurisprudence citée). En effet, une interprétation selon laquelle l'applicabilité de la directive 2016/680 dépendrait du succès de la tentative d'accès à des données à caractère personnel contenues dans un téléphone portable créerait tant pour les autorités nationales compétentes que pour les justiciables une incertitude incompatible avec ce principe.
- 77 Il ressort de ce qui précède qu'une tentative d'accès aux données contenues dans un téléphone portable, par des autorités de police aux fins d'une enquête en matière pénale, telle que celle en cause au principal, relève, ainsi que M. l'avocat général l'a considéré au point 53 de ses conclusions, du champ d'application de la directive 2016/680.

Sur les première et deuxième questions

- 78 La juridiction de renvoi a expressément visé, à ses première et deuxième questions, d'une part, l'article 15, paragraphe 1, de la directive 2002/58, qui requiert notamment que les mesures législatives dont il permet l'adoption par les États membres, limitant la portée des droits et des obligations prévus à plusieurs dispositions de cette directive, constituent une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, et, d'autre part, l'article 52, paragraphe 1, de la Charte, qui consacre le principe de proportionnalité dans le contexte de la limitation de l'exercice des droits et des libertés reconnus par la Charte.
- 79 Or, aux termes de l'article 4, paragraphe 1, sous c), de la directive 2016/680, les États membres doivent prévoir que les données à caractère personnel sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées. Cette disposition exige ainsi le respect, par les États membres, du principe de la « minimisation des données », lequel donne expression à ce principe de proportionnalité (arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politsia » pri MVR – Sofia, C-118/22, EU:C:2024:97, point 41 et jurisprudence citée).
- 80 Il s'ensuit que, notamment, la collecte de données à caractère personnel dans le cadre d'une procédure pénale, et la conservation de celles-ci par les autorités de police, à des fins énoncées à l'article 1^{er}, paragraphe 1, de ladite directive, doivent respecter, comme tout traitement relevant du champ d'application de celle-ci, ce dernier principe (arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politsia » pri MVR – Sofia, C-118/22, EU:C:2024:97, point 42 et jurisprudence citée).
- 81 Ainsi, il y a lieu de considérer que, par ses première et deuxième questions, qu'il convient d'examiner ensemble, la juridiction de renvoi demande, en substance, si l'article 4, paragraphe 1, sous c), de la directive 2016/680, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à une réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales en général et qui ne soumet pas l'exercice de cette possibilité à un contrôle préalable par un juge ou une entité administrative indépendante.
- 82 À titre liminaire, il y a lieu de relever que, ainsi que cela ressort des considérants 2 et 4 de la directive 2016/680, tout en mettant en place un cadre pour la protection des données à caractère personnel solide et cohérent afin d'assurer le respect du droit fondamental de la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant, reconnu à l'article 8, paragraphe 1, de la Charte et à l'article 16, paragraphe 1, TFUE, cette directive vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice au sein de l'Union [voir, en ce sens, arrêt du 25 février 2021, Commission/Espagne (Directive données à caractère personnel – Domaine pénal), C-658/19, EU:C:2021:138, point 75].
- 83 À cette fin, la directive 2016/680 vise notamment, ainsi que cela a été relevé au point 74 du présent arrêt, à assurer un niveau élevé de protection des données à caractère personnel des personnes physiques.

- 84 À cet égard, il convient de rappeler que, ainsi que le considérant 104 de la directive 2016/680 le met en exergue, les limitations que cette directive permet d'apporter au droit à la protection des données à caractère personnel, prévu à l'article 8 de la Charte, ainsi qu'au droit au respect de la vie privée et familiale, protégé par l'article 7 de cette Charte, doivent être interprétées conformément aux exigences de l'article 52, paragraphe 1, de celle-ci, lesquelles incluent le respect du principe de proportionnalité (voir, en ce sens, arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politisia » pri MVR – Sofia, C-118/22, EU:C:2024:97, point 33).
- 85 En effet, ces droits fondamentaux ne sont pas des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux. Toute limitation à l'exercice desdits droits fondamentaux doit, conformément à l'article 52, paragraphe 1, de la Charte, être prévue par la loi et respecter le contenu essentiel des mêmes droits fondamentaux ainsi que le principe de proportionnalité. En vertu de ce dernier principe, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui. Elles doivent s'opérer dans les limites du strict nécessaire et la réglementation comportant les limitations en cause doit prévoir des règles claires et précises régissant la portée et l'application de ces limitations (arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politisia » pri MVR – Sofia, C-118/22, EU:C:2024:97, point 39 et jurisprudence citée).
- 86 En ce qui concerne, en premier lieu, l'objectif d'intérêt général susceptible de justifier une limitation à l'exercice des droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telle que celle qui découle de la réglementation en cause au principal, il convient de souligner qu'un traitement de données à caractère personnel dans le cadre d'une enquête policière visant la répression d'une infraction pénale, tel qu'une tentative d'accès aux données contenues dans un téléphone portable, doit être considéré, en principe, comme répondant effectivement à un objectif d'intérêt général reconnu par l'Union, au sens de l'article 52, paragraphe 1, de la Charte.
- 87 En ce qui concerne, en deuxième lieu, l'exigence du caractère nécessaire d'une telle limitation, ainsi que le souligne, en substance, le considérant 26 de la directive 2016/680, cette exigence n'est pas remplie lorsque l'objectif d'intérêt général visé peut raisonnablement être atteint de manière aussi efficace par d'autres moyens, moins attentatoires aux droits fondamentaux des personnes concernées (voir, en ce sens, arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politisia » pri MVR – Sofia, C-118/22, EU:C:2024:97, point 40 et jurisprudence citée).
- 88 En revanche, l'exigence de nécessité est remplie lorsque l'objectif poursuivi par le traitement de données en cause ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et familiale ainsi qu'à la protection des données à caractère personnel garantis aux articles 7 et 8 de la Charte [arrêt du 26 janvier 2023, Ministerstvo na vatrešnite raboti (Enregistrement de données biométriques et génétiques par la police), C-205/21, EU:C:2023:49, point 126 et jurisprudence citée].
- 89 En ce qui concerne, en troisième lieu, le caractère proportionné de la limitation à l'exercice des droits fondamentaux garantis aux articles 7 et 8 de la Charte, découlant de tels traitements, celui-ci implique une pondération de l'ensemble des éléments pertinents du cas d'espèce (voir, en ce sens, arrêt du 30 janvier 2024, Direktor na Glavna direktsia « Natsionalna politisia » pri MVR – Sofia, C-118/22, EU:C:2024:97, points 62 et 63 et jurisprudence citée).

- 90 Relèvent, notamment, de tels éléments, la gravité de la limitation ainsi apportée à l'exercice des droits fondamentaux en cause, laquelle dépend de la nature et de la sensibilité des données auxquelles les autorités de police compétentes sont susceptibles d'avoir accès, l'importance de l'objectif d'intérêt général poursuivi par cette limitation, le lien existant entre le propriétaire du téléphone portable et l'infraction pénale en cause ou encore la pertinence des données en cause pour constater les faits.
- 91 S'agissant, premièrement, de la gravité de la limitation des droits fondamentaux résultant d'une réglementation telle que celle en cause au principal, il ressort de la décision de renvoi que cette réglementation permet aux autorités de police compétentes d'accéder, sans autorisation préalable, aux données contenues dans un téléphone portable.
- 92 Un tel accès est susceptible de porter, en fonction du contenu du téléphone portable en cause et des choix opérés par ces autorités de police, non seulement sur des données relatives au trafic et à la localisation, mais aussi sur des photographies et l'historique de navigation sur Internet effectuée avec ce téléphone, voire sur une partie du contenu des communications opérées avec ledit téléphone, notamment en consultant les messages qui y sont conservés.
- 93 L'accès à un tel ensemble de données est susceptible de permettre de tirer des conclusions très précises concernant la vie privée de la personne concernée, telles que ses habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de cette personne et les milieux sociaux fréquentés par celle-ci.
- 94 Enfin, il ne saurait être exclu que les données contenues dans un téléphone portable puissent inclure des données particulièrement sensibles, telles que des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques et les convictions religieuses ou philosophiques, cette sensibilité justifiant la protection spécifique que requiert à leur égard l'article 10 de la directive 2016/680, laquelle s'étend également à des données dévoilant indirectement, au terme d'une opération intellectuelle de déduction ou de recoupement, des informations de cette nature [voir, par analogie, arrêt du 5 juin 2023, Commission/Pologne (Indépendance et vie privée des juges), C-204/21, EU:C:2023:442, point 344].
- 95 L'ingérence dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte à laquelle peut donner lieu l'application d'une réglementation telle que celle en cause au principal doit dès lors être considérée comme étant grave, voire particulièrement grave.
- 96 S'agissant, deuxièmement, de l'importance de l'objectif poursuivi, il convient de souligner que la gravité de l'infraction qui fait l'objet de l'enquête constitue l'un des paramètres centraux lors de l'examen de la proportionnalité de l'ingérence grave que constitue l'accès aux données à caractère personnel contenues dans un téléphone portable et qui permettent de tirer des conclusions précises sur la vie privée de la personne concernée.
- 97 Toutefois, considérer que seule la lutte contre la criminalité grave est susceptible de justifier l'accès à des données contenues dans un téléphone portable limiterait les pouvoirs d'enquête des autorités compétentes, au sens de la directive 2016/680, à l'égard des infractions pénales en général. Il en résulterait un accroissement du risque d'impunité pour de telles infractions, compte tenu de l'importance que peuvent avoir de telles données pour les enquêtes pénales. Ainsi, une telle limitation méconnaîtrait la nature spécifique des missions accomplies par ces

autorités aux fins énoncées à l'article 1^{er}, paragraphe 1, de cette directive, mise en exergue aux considérants 10 et 11 de celle-ci, et nuirait à l'objectif de réalisation d'un espace de liberté, de sécurité et de justice au sein de l'Union que poursuit ladite directive.

- 98 Cela étant, ces considérations sont sans préjudice de l'exigence, découlant de l'article 52, paragraphe 1, de la Charte, selon laquelle toute limitation à l'exercice d'un droit fondamental doit être « prévue par la loi », cette exigence impliquant que la base légale autorisant une telle limitation en définisse la portée de manière suffisamment claire et précise [voir, en ce sens, arrêt du 26 janvier 2023, *Ministerstvo na vatreshnite raboti* (Enregistrement de données biométriques et génétiques par la police), C-205/21, EU:C:2023:49, point 65 et jurisprudence citée].
- 99 En vue de satisfaire à cette exigence, il incombe au législateur national de définir de manière suffisamment précise les éléments, notamment la nature ou les catégories des infractions concernées, devant être pris en compte.
- 100 S'agissant, troisièmement, du lien existant entre le propriétaire du téléphone portable et l'infraction pénale en cause ainsi que de la pertinence des données en cause pour constater les faits, il ressort de l'article 6 de la directive 2016/680 que la notion de « personne concernée » couvre différentes catégories de personnes, à savoir, en substance, les personnes soupçonnées, pour des motifs sérieux, d'avoir commis ou d'être sur le point de commettre une infraction pénale, les personnes ayant été reconnues coupables d'une infraction pénale, les victimes ou victimes potentielles de telles infractions, ainsi que les tiers à une infraction pénale pouvant être appelés à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures. Selon cet article, les États membres sont tenus de prévoir que le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de ces différentes catégories de personnes concernées.
- 101 À cet égard, en ce qui concerne en particulier l'accès à des données contenues dans le téléphone portable de la personne faisant l'objet d'une enquête pénale, comme dans l'affaire au principal, il importe que l'existence de soupçons raisonnables à l'égard de celle-ci, en ce sens qu'elle a commis, commet ou projette de commettre une infraction, ou encore qu'elle est impliquée d'une manière ou d'une autre dans une telle infraction, soit étayée par des éléments objectifs et suffisants.
- 102 C'est notamment en vue de s'assurer que le principe de proportionnalité est respecté dans chaque cas concret en effectuant une pondération de l'ensemble des éléments pertinents qu'il est essentiel que, lorsque l'accès des autorités nationales compétentes aux données à caractère personnel comporte le risque d'une ingérence grave, voire particulièrement grave, dans les droits fondamentaux de la personne concernée, cet accès soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante.
- 103 Ce contrôle préalable requiert que la juridiction ou l'entité administrative indépendante chargée de l'effectuer dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts légitimes et des droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès.

- 104 Ce contrôle indépendant, dans une situation telle que celle visée au point 102 du présent arrêt, doit intervenir préalablement à toute tentative d'accès aux données concernées, sauf en cas d'urgence dûment justifié, auquel cas ledit contrôle doit intervenir dans de brefs délais. En effet, un contrôle ultérieur ne permettrait pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire.
- 105 En particulier, la juridiction ou l'entité administrative indépendante, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande d'accès motivée relevant du champ d'application de la directive 2016/680, doit être habilitée à refuser ou à restreindre cet accès lorsqu'elle constate que l'ingérence dans les droits fondamentaux que constituerait ledit accès serait disproportionné compte tenu de l'ensemble des éléments pertinents.
- 106 Un refus ou une restriction de l'accès aux données contenues dans un téléphone portable, par les autorités de police compétentes, doit ainsi être opéré si, compte tenu de la gravité de l'infraction et des besoins de l'enquête, un accès au contenu des communications ou à des données sensibles n'apparaît pas justifié.
- 107 S'agissant, en particulier, des traitements de données sensibles, il convient de tenir compte des exigences posées à l'article 10 de la directive 2016/680, dont la finalité est d'assurer une protection accrue à l'égard de ces traitements qui sont susceptibles d'engendrer, ainsi qu'il ressort du considérant 37 de cette directive, des risques importants pour les libertés et les droits fondamentaux, tels que le droit au respect de la vie privée et familiale ainsi que le droit à la protection des données à caractère personnel, garantis aux articles 7 et 8 de la Charte. À cet effet, ainsi qu'il résulte des termes mêmes de cet article 10, l'exigence selon laquelle le traitement de telles données est autorisé « uniquement en cas de nécessité absolue » doit être interprétée comme définissant des conditions renforcées de licéité du traitement des données sensibles, au regard de celles qui découlent de l'article 4, paragraphe 1, sous b) et c), ainsi que de l'article 8, paragraphe 1, de ladite directive, lesquelles se réfèrent seulement à la « nécessité » d'un traitement de données relevant, de manière générale, du champ d'application de la même directive [arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), C-205/21, EU:C:2023:49 points 116 et 117 ainsi que jurisprudence citée].
- 108 Ainsi, d'une part, l'emploi de l'adverbe « uniquement » devant l'expression « en cas de nécessité absolue » souligne que le traitement de catégories particulières de données, au sens dudit article 10, ne pourra être considéré comme étant nécessaire que dans un nombre limité de cas. D'autre part, le caractère « absolu » de la nécessité d'un traitement de telles données implique que cette nécessité soit appréciée de manière particulièrement rigoureuse [arrêt du 26 janvier 2023, Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police), C-205/21, EU:C:2023:49, point 118].
- 109 Or, en l'occurrence, la juridiction de renvoi indique que, au cours d'une procédure d'enquête pénale, les autorités de police autrichiennes sont habilitées à accéder aux données contenues dans un téléphone portable. De plus, elle précise que cet accès n'est pas soumis, en principe, à l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante. Il appartient toutefois à cette seule juridiction de tirer les conséquences des précisions apportées notamment aux points 102 à 108 du présent arrêt dans le litige au principal.

- 110 Il ressort de ce qui précède qu'il convient de répondre aux première et deuxième questions que l'article 4, paragraphe 1, sous c), de la directive 2016/680, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, si cette réglementation :
- définit de manière suffisamment précise la nature ou les catégories des infractions concernées,
 - garantit le respect du principe de proportionnalité, et
 - soumet l'exercice de cette possibilité, sauf cas d'urgence dûment justifié, à un contrôle préalable d'un juge ou d'une entité administrative indépendante.

Sur la troisième question

- 111 Il ressort de la décision de renvoi que, par sa troisième question, la juridiction de renvoi vise, en substance, à déterminer si CG aurait dû être informé des tentatives d'accès aux données contenues dans son téléphone portable afin de pouvoir exercer son droit à un recours effectif garanti à l'article 47 de la Charte.
- 112 À cet égard, les dispositions pertinentes de la directive 2016/680 sont, d'une part, l'article 13 de cette directive, intitulé « Informations à mettre à la disposition de la personne concernée ou à lui fournir », et, d'autre part, l'article 54 de ladite directive, intitulé « Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant ».
- 113 Il importe également de rappeler, ainsi que le considérant 104 de la directive 2016/680 le met en exergue, que les limitations apportées par cette directive au droit à un recours effectif et à accéder à un tribunal impartial, protégé par l'article 47 de la Charte, doivent être interprétées conformément aux exigences de l'article 52, paragraphe 1, de celle-ci, lesquelles incluent le respect du principe de proportionnalité.
- 114 Il convient donc de considérer que, par sa troisième question, la juridiction de renvoi demande, en substance, si les articles 13 et 54 de la directive 2016/680, lus à la lumière de l'article 47 et de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui permet aux autorités compétentes en matière pénale de tenter d'accéder aux données contenues dans un téléphone portable sans en informer la personne concernée.
- 115 Il découle de l'article 13, paragraphe 2, sous d), de la directive 2016/680 que, outre les informations visées au paragraphe 1, telles que l'identité du responsable du traitement, la finalité de ce traitement et le droit d'introduire une réclamation auprès d'une autorité de contrôle qui doivent être mises à la disposition de la personne concernée, les États membres prévoient, par la loi, que le responsable du traitement fournit à la personne concernée afin de lui permettre d'exercer ses droits, au besoin, des informations complémentaires, en particulier lorsque les données à caractère personnel sont collectées à l'insu de cette personne.
- 116 L'article 13, paragraphe 3, sous a) et b), de la directive 2016/680 autorise toutefois le législateur national à limiter la fourniture d'informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations « dès lors et aussi longtemps qu'une mesure

de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée », notamment, pour « éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires » ou « éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ».

- 117 Enfin, il y a lieu de relever que l'article 54 de la directive 2016/680, qui donne expression à l'article 47 de la Charte, impose aux États membres de prévoir que, lorsqu'une personne considère que ses droits prévus dans les dispositions adoptées en vertu de cette directive ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation de ces dispositions, cette personne a droit à un recours juridictionnel effectif.
- 118 Il ressort de la jurisprudence que le droit à un recours juridictionnel effectif, garanti à l'article 47 de la Charte, exige, en principe, que l'intéressé puisse connaître les motifs sur lesquels est fondée la décision prise à son égard, afin de lui permettre de défendre ses droits dans les meilleures conditions possibles et de décider en pleine connaissance de cause s'il est utile de saisir le juge compétent, ainsi que pour mettre ce dernier pleinement en mesure d'exercer le contrôle de la légalité de cette décision [arrêt du 16 novembre 2023, Ligue des droits humains (Vérification du traitement des données par l'autorité de contrôle), C-333/22, EU:C:2023:874, point 58].
- 119 Si ce droit ne constitue pas une prérogative absolue et que, conformément à l'article 52, paragraphe 1, de la Charte, des limitations peuvent y être apportées, c'est à condition que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel des droits et des libertés en cause et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui [arrêt du 16 novembre 2023, Ligue des droits humains (Vérification du traitement des données par l'autorité de contrôle), C-333/22, EU:C:2023:874, point 59].
- 120 Partant, il découle des dispositions citées aux points 115 à 119 du présent arrêt qu'il incombe aux autorités nationales compétentes ayant été autorisées, par un juge ou une entité administrative indépendante, à accéder aux données conservées d'informer les personnes concernées, dans le cadre des procédures nationales applicables, des motifs sur lesquels cette autorisation repose, dès le moment où cela n'est pas susceptible de compromettre les enquêtes menées par ces autorités et de mettre à leur disposition l'ensemble des informations visées à l'article 13, paragraphe 1, de la directive 2016/680. Ces informations sont, en effet, nécessaires pour permettre à ces personnes d'exercer, notamment, le droit de recours, explicitement prévu à l'article 54 de la directive 2016/680 [voir, en ce sens, arrêt du 17 novembre 2022, Spetsializirana prokuratura (Conservation des données relatives au trafic et à la localisation), C-350/21, EU:C:2022:896, point 70 et jurisprudence citée].
- 121 En revanche, une réglementation nationale qui exclurait, de manière générale, tout droit à obtenir de telles informations ne serait pas conforme au droit de l'Union [voir, en ce sens, arrêt du 17 novembre 2022, Spetsializirana prokuratura (Conservation des données relatives au trafic et à la localisation), C-350/21, EU:C:2022:896, point 71].

- 122 En l'occurrence, il ressort de la décision de renvoi que CG savait que son téléphone portable avait été saisi lorsque les autorités de police autrichiennes ont vainement tenté de le déverrouiller afin d'accéder aux données contenues dans celui-ci. Dans ces conditions, il n'apparaît pas qu'informer CG du fait que ces autorités allaient tenter d'accéder à ces données était susceptible de nuire aux enquêtes, de sorte qu'il aurait dû en être informé au préalable.
- 123 Il ressort de ce qui précède qu'il convient de répondre à la troisième question que les articles 13 et 54 de la directive 2016/680, lus à la lumière de l'article 47 et de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui autorise les autorités compétentes à tenter d'accéder à des données contenues dans un téléphone portable sans informer la personne concernée, dans le cadre des procédures nationales applicables, des motifs sur lesquels repose l'autorisation d'accéder à ces données, délivrée par un juge ou une entité administrative indépendante, à partir du moment où la communication de cette information n'est plus susceptible de compromettre les missions incombant à ces autorités en vertu de cette directive.

Sur les dépens

- 124 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 :

- 1) L'article 4, paragraphe 1, sous c), de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne,**

doit être interprété en ce sens que :

il ne s'oppose pas à une réglementation nationale qui octroie aux autorités compétentes la possibilité d'accéder aux données contenues dans un téléphone portable, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, si cette réglementation :

- définit de manière suffisamment précise la nature ou les catégories des infractions concernées,**
- garantit le respect du principe de proportionnalité, et**
- soumet l'exercice de cette possibilité, sauf cas d'urgence dûment justifié, à un contrôle préalable d'un juge ou d'une entité administrative indépendante.**

2) Les articles 13 et 54 de la directive 2016/680, lus à la lumière de l'article 47 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux,

doivent être interprétés en ce sens que :

ils s'opposent à une réglementation nationale qui autorise les autorités compétentes à tenter d'accéder à des données contenues dans un téléphone portable sans informer la personne concernée, dans le cadre des procédures nationales applicables, des motifs sur lesquels repose l'autorisation d'accéder à ces données, délivrée par un juge ou une entité administrative indépendante, à partir du moment où la communication de cette information n'est plus susceptible de compromettre les missions incombant à ces autorités en vertu de cette directive.

Signatures