Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MANUEL CAMPOS SÁNCHEZ-BORDONA
présentées le 20 avril 2023 [1]

Affaire C-548/21

C. G.
contre
Bezirkshauptmannschaft Landeck

[demande de décision préjudicielle formée par le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol, Autriche)]

« Renvoi préjudiciel – Télécommunications – Protection des données à caractère personnel – Directive (UE) 2016/680 – Procédure pénale – Tentative d'accès des autorités publiques aux données enregistrées sur un téléphone portable sans l'autorisation d'une juridiction ou d'une autorité administrative indépendante »

1. La présente demande de décision préjudicielle porte, en substance, sur les conditions auxquelles les autorités de police doivent se conformer pour accéder aux données stockées dans le téléphone portable de la personne visée par une enquête pénale.

2. Comme je vais tenter de l'expliquer, le renvoi préjudiciel présente des insuffisances notables quant à sa recevabilité. Si la Cour décide néanmoins d'engager le débat au fond, elle devra se prononcer sur les champs d'application respectifs de la directive 2002/58/CE [2] et de la directive (UE) 2016/680 [3].

1 Langue originale : l'espagnol.

2 Directive 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).

3 Directive 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).

I. Le cadre juridique

A. Le droit de l'Union

1. Le règlement (UE) 2016/679

3. L'article 2 (« Champ d'application matériel »), paragraphe 2, du règlement 2016/679 [4] dispose :

« Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

[...]

d) 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 des menaces pour la sécurité publique et la prévention de telles menaces. »

2. La directive 2016/680

4. Le deuxième considérant de la directive 2016/680 est libellé comme suit :

« 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 [...] 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. »

5. Le considérant 46 de la directive 2016/680 énonce ce qui suit :

« Toute limitation des droits de la personne concernée doit respecter la [charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »)] et la convention européenne [de sauvegarde] des droits de l'homme [et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »)], 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 [5] dans leur jurisprudence, et notamment respecter l'essence desdits droits et libertés. »

6. Le considérant 49 de la directive 2016/680 est libellé comme suit :

« Lorsque les données à caractère personnel sont traitées dans le cadre d'une enquête pénale ou d'une procédure judiciaire en matière pénale, les États membres devraient pouvoir prévoir que le droit à l'information, le droit d'accès aux données à caractère personnel, de rectification ou d'effacement de celles-ci, et le droit de limitation du traitement sont exercés conformément aux règles nationales relatives à la procédure judiciaire. »

[4] Règlement 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, ci-après le « RGPD »).

[5] Ci-après la « Cour EDH ».

7. L'article 1er (« Objet et objectifs ») de la directive 2016/680 dispose :

« 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

[...]

3. La présente directive n'empêche pas les États membres 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. »

8. L'article 2 (« Champ d'application »), paragraphe 1, de la directive 2016/680 dispose :

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

9. L'article 3 (« Définitions ») de la directive 2016/680 est libellé comme suit :

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

[...]

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

[...] ».

10. L'article 4 (« Principes relatifs au traitement des données à caractère personnel »), paragraphe 1, de la directive 2016/680 dispose :

« 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 ;

[...]

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. »

11. L'article 8 (« Licéité du traitement ») de la directive 2016/680 est libellé comme suit :

« 1. Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement. »

12. L'article 13 (« Informations à mettre à la disposition de la personne concernée ou à lui fournir ») de la directive 2016/680 est libellé comme suit :

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

[...]

d) le droit d'introduire une réclamation auprès d'une autorité de contrôle et les coordonnées de ladite autorité ;

[...]

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.

[...] »

13. L'article 15 (« Limitation du droit d'accès »), paragraphe 1, de la directive 2016/680 énonce ce qui suit :

« Les États membres peuvent adopter des mesures législatives limitant, entièrement ou partiellement, le droit d'accès de la personne concernée, dès lors et aussi longtemps qu'une telle limitation partielle ou complète 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. »

14. L'article 27 (« Analyse d'impact relative à la protection des données ») de la directive 2016/680 est libellé comme suit :

« 1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

2. L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées. »

15. L'article 28 (« Consultation préalable de l'autorité de contrôle ») de la directive 2016/680 dispose :

« 1. Les États membres prévoient que le responsable du traitement ou le sous-traitant consulte l'autorité de contrôle préalablement au traitement des données à caractère personnel qui fera partie d'un nouveau fichier à créer :

a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 27, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ; ou

b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées.

[...] ».

16. L'article 54 (« Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant ») de la directive 2016/680 énonce ce qui suit :

« 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 ».

B. Le droit autrichien

17. L'article 18 de la Strafprozessordnung[6] charge la police judiciaire de missions au service de l'administration de la justice pénale (paragraphe 1). Les enquêtes de police judiciaire relèvent de la responsabilité des autorités de sûreté (paragraphe 2). Les organes du service de sûreté publique assurent le service exécutif de la police judiciaire, qui consiste à investiguer et à poursuivre les infractions pénales (paragraphe 3).

18. Conformément à l'article 99 de la StPO, la police judiciaire enquête d'office ou sur la base d'une plainte et est tenue de se conformer aux ordres du ministère public et des juridictions (paragraphe 1). Lorsqu'une mesure d'enquête nécessite un ordre du ministère public, la police judiciaire peut exercer le pouvoir en question, même en l'absence d'un tel ordre, en cas de danger imminent. Dans ce cas, elle doit demander immédiatement l'autorisation (paragraphe 2).

[6] Code de procédure pénale (BGBl 631/1975), dans la version en vigueur au moment des faits (BGBl I, 24/2020) (ci-après la « StPO »).

19. Conformément à l'article 111, paragraphe 2, de la StPO, lorsque des informations stockées sur des supports de données doivent faire l'objet d'une saisie, toute personne est tenue d'accorder l'accès à ces informations et, sur demande, de remettre ou de laisser réaliser un support de données électronique dans un format de fichier couramment utilisé. En outre, elle doit laisser réaliser une copie de sauvegarde des informations stockées sur les supports de données.

II. Les faits, le litige et les questions préjudicielles

20. C. G. est un ressortissant allemand qui travaille et réside en Autriche.

21. Le 23 février 2021, lors d'un contrôle en matière de stupéfiants, des fonctionnaires du bureau de douane d'Innsbruck (Autriche) ont saisi un colis adressé à C. G. contenant 85 grammes de cannabis.

22. Le 6 mars 2021, deux agents de police ont interrogé C. G. au sujet de l'expéditeur du colis et ont fouillé son logement. Au cours de cette perquisition, ils ont saisi son téléphone portable (comportant une carte SIM et une carte SD) et lui ont remis le procès-verbal de la saisie.

23. C. G. s'est opposé à la requête visant à accéder aux données de connexion de son téléphone portable et a refusé de divulguer le code d'accès au téléphone.

24. Le poste de police du district de Landeck (Autriche) n'a pas réussi à déverrouiller le téléphone portable. Ce dernier a été envoyé au Bundeskriminalamt (Office fédéral de la police judiciaire) à Vienne (Autriche), où une nouvelle tentative a été faite, sans succès, pour le déverrouiller et lire les données y étant stockées.

25. Au moment où ces mesures ont été prises par la police, elles n'étaient pas couvertes par un ordre du ministère public ni par la décision d'un juge.

26. Le 31 mars 2021, C. G. a introduit un recours devant le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol, Autriche) contre la mesure coercitive qui lui avait été imposée, en contestant la saisie de son téléphone portable. Ce dernier lui a été restitué le 20 avril 2021.

27. C. G. n'a pas été informé des tentatives d'analyse du contenu du téléphone portable ; il en a eu connaissance parce que l'officier de police qui a procédé à la saisie et a, par la suite, entamé l'exploitation des données numériques a été interrogé en tant que témoin tenu de dire la vérité. Ces tentatives n'ont pas non plus été documentées dans le dossier de la police judiciaire.

28. Dans ce contexte, le Landesverwaltungsgericht Tirol (tribunal régional du Tyrol) a posé à la Cour les questions préjudicielles suivantes :

« 1) L'article 15, paragraphe 1 (lu, le cas échéant, conjointement avec l'article 5), de la directive 2002/58, telle que modifiée par la directive 2009/136/CE, 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 par 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, telle que modifiée par la directive 2009/136, doit-il, à la lumière des articles 7, 8 et 11 ainsi que 52, paragraphe 1, de la [Charte], se comprendre en ce sens qu'il s'oppose à une réglementation nationale, telle que les dispositions combinées des articles 18 et 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, le cas échéant conjointement 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 des articles 18 et 99, paragraphe 1, de la [StPO], permet l'exploitation des données numériques d'un téléphone portable sans que la personne concernée soit informée de la mesure au préalable ou, au moins, après qu'elle a été prise ? »

III. La procédure devant la Cour

29. La demande de décision préjudicielle a été enregistrée auprès du greffe de la Cour le 6 septembre 2021.

30. Le 20 octobre 2021, la Cour a invité la juridiction de renvoi à indiquer si la directive 2016/680 pouvait être pertinente dans la présente affaire.

31. Le 11 novembre 2021, la juridiction de renvoi a répondu que la directive 2016/680 devait être appliquée dans l'affaire au principal.

32. Des observations écrites ont été déposées par les gouvernements autrichien, danois, allemand, estonien, irlandais, français, chypriote, hongrois, néerlandais, polonais, suédois et norvégien ainsi que par la Commission européenne.

33. Lors de l'audience, qui s'est tenue le 16 janvier 2023, ces derniers ont comparu – à l'exception des gouvernements allemand, hongrois et polonais – ainsi que le gouvernement finlandais. Ils ont tous été invités par la Cour à concentrer leurs arguments sur la directive 2016/680 et à répondre oralement à certaines questions ayant trait à cette dernière.

IV. Analyse

A. Sur l'irrecevabilité

34. La juridiction de renvoi a initialement formulé ses questions en sollicitant uniquement l'interprétation de la directive 2002/58. Toutefois, la quasi-totalité des intervenants dans la présente procédure conviennent que cette directive ne s'applique pas dans la présente affaire et que, partant, son interprétation n'est pas nécessaire pour trancher le litige.

35. Aux termes de son article 3, la directive 2002/58 régit le « [...] 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 [l'Union], y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification ».

36. La Cour a jugé 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] »[7].

37. Dans la présente affaire, la tentative d'accès aux données a été effectuée directement par les autorités de police dans le cadre d'une enquête pénale. Il n'y a pas eu d'intervention des fournisseurs de services de communications électroniques et la communication de données à caractère personnel n'a pas été requise auprès de ces derniers. La directive 2002/58 n'entre dès lors pas en jeu.

38. La règle du droit de l'Union régissant cette situation est la directive 2016/680 ; en vertu de son article 2, paragraphe 1, cette dernière s'applique au traitement de données à caractère personnel par les autorités compétentes à des « fins [...] d'enquêtes [en matière d'infractions pénales] ».

39. Ce qui précède suffirait à faire pencher pour l'irrecevabilité du renvoi préjudiciel, tel qu'il avait été formulé par la juridiction nationale, puisque la règle du droit de l'Union dont elle demandait l'interprétation n'était pas applicable à l'affaire en cause.

40. Il est vrai, toutefois, que l'article 267 TFUE permet à la Cour de reformuler les questions qui lui sont posées ou d'indiquer l'existence d'autres règles du droit de l'Union éventuellement pertinentes, afin de donner au juge national une réponse utile[8].

41. La Cour a invité la juridiction de renvoi à se prononcer sur l'incidence éventuelle de la directive 2016/680. Elle lui a donc offert la possibilité de compléter ou de reformuler elle-même ses questions. Au lieu de cela, la juridiction de renvoi s'est bornée à constater que « [l]es prescriptions de la directive [2016/680] sont en tout état de cause à respecter dans la présente affaire », sans toutefois identifier les dispositions de cette dernière à l'égard desquelles elle nourrit des doutes ni développer d'autres considérations de fond[9].

42. Selon une jurisprudence constante de la Cour, « il est indispensable, comme l'énonce l'article 94, sous c), du règlement de procédure, que la décision de renvoi contienne l'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 législation nationale applicable au litige au principal »[10].

7 Arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, ci-après l'« arrêt La Quadrature du Net », EU:C:2020:791, point 103).

8 Voir, notamment, arrêt du 28 avril 2016, Oniors Bio (C-233/15, EU:C:2016:305, point 30).

9 La Cour a jugé nécessaire d'inviter les parties à indiquer « quelles sont, selon elles, les dispositions pertinentes de la directive 2016/680, à la lumière desquelles la Cour devrait, le cas échéant, reformuler les trois questions préjudicielles posées par la juridiction de renvoi » (quatrième question pour réponse orale lors de l'audience).

10 Arrêt du 6 octobre 2021, Consorzio Italian Management et Catania Multiservizi (C-561/19, EU:C:2021:799, point 69).

43. Or, il ressort clairement de ce qui précède que les exigences de l'article 94 du règlement de procédure ne sont pas satisfaites dans le cadre du présent renvoi. Même si la Cour fait preuve d'une certaine souplesse à cet égard, la coopération avec la juridiction de renvoi doit être réciproque : dès lors que cette dernière ne collabore pas, et ce de manière injustifiée, en vue d'exposer ses doutes relatifs à l'interprétation du droit de l'Union qu'elle considère applicable (en l'occurrence, la directive 2016/680), il me semble logique de rejeter la demande de décision préjudicielle pour irrecevabilité [11].

44. À ce qui précède s'ajoute le fait que la juridiction de renvoi :

– n'a pas précisé la nature du traitement qu'ont tenté d'effectuer les autorités de police, ni des données à caractère personnel précisément recherchées. Dans un premier temps, elle semble indiquer que celui-ci se limitait aux données de connexion (c'est-à-dire relatives au trafic et à la localisation), mais, dans un second temps, elle n'exclut pas que le déverrouillage du téléphone facilite l'accès à « l'ensemble des données numériques stockées » [12], et même au contenu des communications et des messages électroniques échangés par son intermédiaire [13] ;

– se réfère tant à la saisie du téléphone et à l'accès, ou tentative d'accès, aux données qui y sont contenues qu'à son « exploitation » (*Auswertung*), autrement dit, à son analyse et à sa lecture. Elle ajoute que cette dernière « implique un accès complet et non contrôlé à l'ensemble des communications numériques de la personne concernée », ce qui permet de « se faire une image très détaillée et approfondie de presque tous les domaines de la vie privée ».

45. Dans ces conditions, plutôt qu'à une *reformulation* des questions de la juridiction de renvoi, la Cour procéderait à une véritable *reconstruction* du renvoi préjudiciel, partiellement fondée, de surcroît, sur des considérations hypothétiques, plutôt que sur des faits établis. Tout cela, j'insiste, après avoir accordé à la juridiction la possibilité de compléter ou de reformuler elle-même ses questions.

46. Je propose, dès lors, de rejeter la demande de décision préjudicielle comme étant irrecevable, ainsi que l'ont demandé plusieurs États intervenants.

47. La circonstance, soulignée lors de l'audience, selon laquelle il n'existe plus de véritable litige nécessitant l'interprétation de règles du droit de l'Union devant la juridiction de renvoi devrait conduire à ce même constat d'irrecevabilité.

48. En effet, le gouvernement autrichien (dont dépendent les autorités de police impliquées dans l'enquête) reconnaît que le comportement de ces autorités a été illicite et a porté atteinte aux droits de la personne concernée. Dès lors que, selon l'ordonnance de renvoi, la demande du requérant devant la juridiction administrative était dirigée, à juste titre, contre les mesures de police considérées comme illicites par l'administration défenderesse, le litige soumis au jugement de la juridiction de renvoi a disparu.

[11] Je partage cette appréciation du gouvernement français (points 36 à 41 de ses observations écrites).

[12] Il en est ainsi dans la deuxième question préjudicielle.

[13] La juridiction de renvoi affirme qu'« en ce qui concerne les données de connexion, il est possible de reconstituer presque tous les contacts en fonction de la fréquence, de l'heure et de la durée de la communication, et en ce qui concerne les communications par SMS et autres services de messagerie, le contenu peut également être reconstitué ; l'exploitation des photographies stockées et des historiques de navigation permet aussi d'obtenir un aperçu très intime de la vie privée de la personne concernée ».

49. En tout état de cause, pour le cas où la Cour ne partagerait pas mon avis, je me pencherai dans la suite des présentes conclusions, à titre subsidiaire, sur les problèmes de fond qui sous-tendent les questions préjudicielles.

50. Au préalable, il me semble cependant nécessaire d'écarter l'existence d'un autre motif d'irrecevabilité soulevé par certains intervenants à la procédure [14]. Selon eux, dès lors que la directive 2016/680 vise à protéger les personnes physiques à l'égard du *traitement* de leurs données, elle ne régirait pas des cas tels que celui de l'espèce, dans lesquels il n'y aurait pas eu de traitement, mais une simple *tentative d'accès* à des données qui n'ont finalement pas pu être obtenues.

51. En revanche, pour la Commission, l'effet utile de la directive 2016/680 devrait privilégier une interprétation de son objet qui ne serait pas limitée au traitement des données au sens strict, mais couvrirait également des questions qui lui sont directement liées. L'une de ces dernières serait la tentative d'accès aux données dont le traitement est envisagé [15].

52. À mon avis, sans qu'il soit nécessaire de repousser les limites du champ d'application de la directive 2016/680 [16], son application dans la présente affaire se justifie non pas parce qu'une saisie du téléphone portable a été effectuée [17], mais en raison du comportement subséquent des autorités de police pour obtenir de celui-ci certaines données à caractère personnel de la personne concernée, en vue de quoi elles ont tenté de le déverrouiller et de permettre l'accès à son contenu.

53. Parmi les opérations définies comme « traitement » par l'article 3, point 2, de la directive 2016/680 figure « toute autre forme de mise à disposition » des données à caractère personnel, effectuée dans le cadre d'une enquête pénale. Je considère que, lorsque l'autorité de police saisit un téléphone dans lequel ces données sont conservées et le manipule à des fins d'extraction, elle entame une « opération » de traitement, quand bien même cette dernière échouerait pour des raisons techniques tenant à la sécurité cryptographique.

54. Une tentative infructueuse d'accès aux données à caractère personnel conservées dans un téléphone portable, dans le cadre d'une enquête pénale, est régie par la directive 2016/680, pour des raisons analogues à celles ayant conduit la Cour à déclarer la directive 2002/58 applicable à la tentative (également infructueuse) d'obtenir l'autorisation judiciaire afin d'accéder à certaines données de la personne faisant l'objet de l'enquête, détenues par un opérateur de communications électroniques [18].

55. Dans ce contexte, si la juridiction de renvoi devait se prononcer sur l'illicéité de l'action de la police (reconnue par le gouvernement autrichien, comme je l'ai déjà exposé), son appréciation pourrait dépendre de la légalité du but visé par cette dernière, que la mesure ait été couronnée de succès ou que son exécution ait seulement été entamée, en vain.

[14] Je me réfère précisément aux gouvernements autrichien, français, néerlandais et norvégien.

[15] Pour la Commission, « il est [...] indifférent que les tentatives d'accès aient été couronnées de succès ou non. L'apparition de difficultés techniques empêchant le succès des tentatives d'accès est une circonstance qui ne peut pas être connue d'avance et qui n'affecte pas les risques en matière de protection des données à caractère personnel ».

[16] Il me semble, notamment, que le recours aux articles 27 et 28 de la directive 2016/680, suggéré par la Commission dans ses observations écrites, n'est pas nécessaire. L'« analyse d'impact relative à la protection des données » prévue à cet article 27 vise, de manière générale, un « type de traitement » et non des traitements précis ou spécifiques. Il ressort du considérant 58 de la directive 2016/680 que « [l]es analyses d'impact devraient porter sur les systèmes et processus pertinents des opérations de traitement, et *non sur des cas individuels* » (mise en italique par mes soins). Lors de l'audience, la Commission a nuancé son invocation des deux articles, qu'elle n'aurait cités que pour souligner que la directive 2016/680 envisage également des situations antérieures au traitement proprement dit.

[17] La directive 2016/680 ne réglemente pas la saisie du téléphone en tant que moyen de preuve dans le cadre d'une enquête pénale.

[18] Arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

B. Sur le fond

1. Sur la première question préjudicielle

56. La juridiction de renvoi souhaite savoir si, conformément à l'article 15, paragraphe 1 (lu, le cas échéant, conjointement avec l'article 5), de la directive 2002/58 et à la lumière des articles 7 et 8 de la Charte, « l'accès des autorités publiques aux données stockées dans les téléphones portables constitue une ingérence dans les droits fondamentaux garantis par 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 ».

57. Si la présente demande de décision préjudicielle était recevable, l'inapplicabilité de la directive 2002/58 imposerait de reformuler la première question, de sorte que la réponse de la Cour interpréterait la directive 2016/680.

58. Cette réponse devrait, successivement, clarifier le point de savoir si l'on peut parler d'ingérence dans des cas comme celui de l'espèce et, dans l'affirmative, si la directive 2016/680 exige que l'accès aux données soit limité aux cas de lutte contre la criminalité grave.

59. Les opérations de traitement de données sont, par définition, susceptibles de porter atteinte au droit au respect de la vie privée (article 7 de la Charte) et à la protection des données à caractère personnel (article 8 de la Charte). Les autorités publiques doivent donc se conformer aux conditions prévues à l'article 52, paragraphe 1, de la Charte pour justifier leur atteinte à l'exercice de ces droits fondamentaux.

60. L'ingérence dans les droits protégés par les articles 7 et 8 de la Charte sera d'autant plus importante que, par celle-ci : a) on demande l'accès à des données à caractère sensible habituellement enregistrées sur les téléphones portables et dont la connaissance peut révéler des facettes de la vie de ses propriétaires qui doivent être tenues à l'abri des tiers, et b) l'accès au contenu des communications est rendu possible.

61. Toutefois, d'un point de vue général et eu égard à son contenu, la directive 2016/680 ne saurait être interprétée en ce sens que les traitements de données qu'elle vise sont circonscrits aux seuls cas de lutte contre la criminalité grave.

62. La directive 2016/680 a pour objet toute opération de traitement [19] de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection de *tout type* d'infractions pénales, d'enquêtes et de poursuites en la matière.

63. Il ne ressort pas des principes instaurés par la directive 2016/680 en ce qui concerne le traitement des données à caractère personnel effectué à ces fins (article 4), ni des conditions de licéité de celui-ci (article 8), que, en règle générale, le traitement des données ne soit réalisable que dans les hypothèses de criminalité grave.

[19] La typologie des « opérations » visées à l'article 3, point 2, de la directive 2016/680 est très étendue. Voir point 9 des présentes conclusions.

64. Une limitation restreinte aux cas de lutte contre la criminalité grave ne pourrait pas non plus être simplement fondée sur l'extrapolation de la jurisprudence de la Cour relative à la directive 2002/58 [20] à des cas tels que celui de l'espèce.

65. Selon moi, ce n'est pas possible, car, sous réserve de ce que j'exposerai dans la suite des présentes conclusions, cette jurisprudence concerne la conservation généralisée et indifférenciée des données à caractère personnel d'un groupe générique et indéterminé, effectuée de manière systématique par les fournisseurs de services de communications électroniques. L'ampleur de l'ingérence qu'implique ce type de conservation pour la société dans son ensemble explique que la Cour se soit montrée particulièrement rigoureuse en la proscrivant et en prévoyant les dérogations à cette interdiction.

66. Tel n'est pas le cas lorsque l'accès demandé ne concerne pas l'ensemble ou de grands groupes de la population (autrement dit, les données à caractère personnel d'un groupe générique et indéterminé), mais les informations stockées dans un téléphone portable particulier, dans le cadre d'une procédure d'enquête pénale également particulière, que la directive 2016/680 régit spécifiquement.

67. La directive 2016/680 n'a d'autre objet que le traitement de données par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Il s'agit de toute sorte d'infractions pénales et non pas uniquement de celles ayant un caractère grave.

68. Par ailleurs, ainsi que l'ont souligné certains des intervenants dans la procédure préjudicielle, en l'absence de toute indication relative à la gravité des infractions pénales dans la directive 2016/680, cette dernière pourrait ne pas être appliquée de manière uniforme dans les États membres, dès lors que les appréciations de chaque droit national relatives à la gravité plus ou moins importante d'un comportement passible de sanctions diffèrent sensiblement [21].

69. La directive 2016/680 n'impose donc pas, en tant que condition de licéité, que le traitement des données à caractère personnel qu'elle réglemente ne soit réalisable qu'à des fins de lutte contre la criminalité grave.

70. Il n'en demeure pas moins que, en application du principe de proportionnalité et au cas par cas, le traitement des données que les autorités compétentes entendent effectuer au titre de la directive 2016/680 doit être tempéré en fonction de : a) la nature des infractions pénales poursuivies ; et b) la qualité des données à caractère personnel ciblées par ce traitement.

71. Dans le même ordre d'idées, je suis d'accord avec certaines des affirmations du gouvernement allemand concernant la limitation de l'accès aux données contenues dans les téléphones saisis lorsqu'elles permettent d'établir un profil complet de la personnalité de leurs propriétaires à partir du contenu numérique de ceux-ci. Pour le gouvernement allemand, cet accès devrait se

[20] Arrêt La Quadrature du Net et arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) ; du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788) ; du 6 octobre 2020, Privacy International (C-623/17, EU:C:2020:790), et du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, ci-après l'« arrêt Prokuratuur », EU:C:2021:152).

[21] Le gouvernement français cite, à titre d'exemple, les infractions en matière de possession et de trafic de stupéfiants, pour lesquelles les règles pénales en Autriche et en France diffèrent s'agissant de leur gravité. Le gouvernement suédois s'exprime de manière analogue.

limiter aux données qui sont nécessaires comme moyen de preuve dans un cas particulier et pourrait ne pas être adéquat en présence de facteurs tels que « le caractère mineur de l'infraction faisant l'objet de l'enquête ou la faible valeur probante des données à saisir » [22].

72. In abstracto, la directive 2016/680 n'implique donc pas que soit systématiquement illicite l'accès aux données à caractère personnel stockées dans un téléphone portable en vue de faciliter l'enquête sur des comportements susceptibles de relever de la criminalité générale ou de droit commun. La question de savoir si, in concreto, un tel accès est approprié devra être appréciée, au cas par cas, par l'autorité concernée, à la lumière de sa nécessité et du critère de proportionnalité auquel je viens de me référer.

73. C'est ce qui ressort, selon moi, des dispositions de la directive 2016/680 qui fixent les conditions de validité des traitements de données à caractère personnel dans le cadre de la lutte contre la criminalité :

– l'article 4, paragraphe 1, sous a), en vertu duquel les données doivent être « traitées de manière licite » ;

– l'article 8, paragraphe 1, qui souligne que le traitement doit être *nécessaire* et fondé sur le droit de l'Union ou le droit d'un État membre.

2. Sur la deuxième question préjudicielle

74. Par sa deuxième question préjudicielle, la juridiction de renvoi souhaite savoir si l'article 15, paragraphe 1, de la directive 2002/58, lu conjointement avec les articles 7, 8, 11 et 52, paragraphe 1, de la Charte, « s'oppose à une réglementation nationale, telle que les dispositions combinées des articles 18 et 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 ».

75. La formulation de la question présente une certaine ambiguïté. La juridiction de renvoi :

– reconnaît que l'article 110, paragraphe 2, de la StPO prévoit que les saisies d'objets nécessitent, en principe, l'autorisation du ministère public. En l'absence d'une telle autorisation, l'autorité de police ne peut procéder à ces saisies que dans les hypothèses exceptionnelles visées au paragraphe 3 de ce même article (qui ne semblent pas se présenter dans l'affaire au principal) ;

– elle ajoute toutefois que l'exploitation des informations stockées dans les téléphones portables « n'est pas réglementée [dans la StPO] de façon univoque » et qu'elle pourrait être effectuée par les autorités responsables de la sûreté, de leur propre initiative, sans autorisation préalable.

76. Le gouvernement autrichien fournit une version de la réglementation nationale qui ne correspond pas à celle exposée dans l'ordonnance de renvoi. En particulier, il affirme que, conformément au droit national, la saisie du téléphone (sauf dans les cas d'urgence) ainsi que

[22] Observations écrites du gouvernement allemand, point 20.

l'analyse des données qui y sont stockées ne sont possibles qu'après autorisation du ministère public [23]. En l'absence d'un ordre de la part du ministère public, l'exploitation par la police des données conservées dans ce téléphone est illicite.

77. Il appartient à la juridiction de renvoi de vérifier les termes de la réglementation interne. Dans le cadre de la procédure prévue à l'article 267 TFUE, la Cour n'a pas compétence pour interpréter le droit national, et il appartient au seul juge national de déterminer l'exacte portée des dispositions législatives, réglementaires ou administratives nationales [24].

78. Sans vouloir prendre part à la polémique relative à l'interprétation du droit autrichien, il me semble difficile d'inférer des seules dispositions que la juridiction de renvoi identifie (article 18 de la StPO, lu conjointement avec son article 99, paragraphe 1) la conséquence qu'elle en tire elle-même. Cependant, je le répète, il appartient à cette seule juridiction de statuer à cet égard.

79. Quoi qu'il en soit, la juridiction de renvoi considère que la jurisprudence contenue dans l'arrêt Prokuratuur [25] concernant le contrôle préalable, par une juridiction ou par une autorité indépendante, de l'accès aux données conservées serait transposable à un cas tel que celui de l'affaire au principal.

80. Pour le gouvernement néerlandais, au contraire, cette jurisprudence doit être considérée dans le contexte d'une réglementation nationale qui permettait l'accès *général* des autorités compétentes à *l'ensemble* des données relatives au trafic et des données de localisation conservées. Cela expliquerait l'exigence relative à l'autorisation préalable d'une juridiction qui pourrait toutefois ne pas être justifiée dans le cas de l'accès aux données d'un seul téléphone portable.

81. Dans le même ordre d'idées, le gouvernement norvégien fait valoir que, parmi les multiples garanties prévues par la directive 2016/680 [26], ne figure pas explicitement celle relative à la nécessité d'une autorisation préalable de la part d'une autorité juridictionnelle ou administrative indépendante.

82. Partant du fait que les dispositions de la directive 2016/680 doivent être interprétées à la lumière de la Charte, la Commission soutient que l'obligation imposée aux États membres à l'article 8, paragraphe 1, de cette directive (conditions de licéité du traitement) comporte la nécessité de respecter les droits fondamentaux garantis par les articles 7 et 8 de la Charte.

83. Je partage l'avis de la Commission selon lequel, dans le respect de ces articles de la Charte, les législateurs nationaux sont tenus de définir les règles nécessaires pour garantir que l'accès aux données soit justifié au cas par cas et limité à ce qui est strictement nécessaire et proportionné.

[23] Point 19 des observations du gouvernement autrichien. Il cite la décision de l'Oberster Gerichtshof (Cour suprême, Autriche) du 13 octobre 2020 (affaire 11 Os 56/20z) qui qualifie d'« illicite », en ce qu'elle viole les droits subjectifs de la personne concernée, l'exploitation par la police judiciaire des données stockées dans un téléphone portable sans en avoir reçu l'autorisation de la part du ministère public.

[24] Voir, notamment, arrêt du 28 avril 2022, SeGEC e.a. (C-277/21, EU:C:2022:318, point 21).

[25] Voir arrêt Prokuratuur, point 51 : « il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales ».

[26] Outre les garanties figurant à ses articles 4 et 8, celles contenues à ses chapitres III (« Droits de la personne concernée »), IV (« Responsable du traitement et sous-traitant »), VI (« Autorités de contrôle indépendantes ») et VIII (« Voies de recours, responsabilité et sanctions »).

84. Toutefois, de telles règles nationales ne doivent pas nécessairement être spécifiques à l'accès aux données à caractère personnel contenues, comme c'est le cas dans la présente affaire, dans un téléphone portable, mais peuvent être celles prévues en droit interne, de manière générale, en matière d'obtention de preuves.

85. À cet égard, j'ai déjà reproduit le point 103 de l'arrêt La Quadrature du Net en ce qui concerne les mesures des États membres touchant à la confidentialité des communications électroniques, sans imposer d'obligations de traitement aux fournisseurs de services de telles communications [27].

86. Sans qu'il soit dès lors nécessaire de déduire de la directive 2016/680 des règles *spécifiques* de nature procédurale, garantissant la licéité de l'accès aux informations stockées dans un téléphone portable [28], les règles nationales régissant l'exercice des pouvoirs de perquisition et de saisie dans le cadre des enquêtes pénales s'appliquent [29].

87. Le renvoi aux dispositions du droit interne en vue de garantir la licéité de l'accès au titre de la directive 2016/680 est en outre conforme à la jurisprudence de la Cour EDH. C'est précisément dans une affaire concernant la République d'Autriche au regard de l'article 8 de la CEDH (droit au respect de la vie privée et familiale ainsi que du domicile et de la correspondance) que la Cour EDH a constaté que la législation autrichienne relative à la saisie d'objets, et notamment de documents, s'applique à la fouille et à la saisie de données conservées sur des supports informatiques [30].

88. Si, comme le soutient le gouvernement autrichien en se référant à la jurisprudence de l'Oberster Gerichtshof (Cour suprême), les autorités de police ne sont pas habilitées à accéder aux données conservées dans un téléphone portable déterminé sans en avoir reçu l'autorisation de la part du ministère public, la deuxième question préjudicielle perd une grande partie de son sens.

89. En tout état de cause, la réponse à cette question ne saurait exclure que l'accès aux données à caractère personnel, qui sont conservées dans le téléphone saisi, conduise à « se faire une image très détaillée et approfondie de presque tous les domaines de la vie privée » de la personne concernée [31]. Si tel était le cas, les autorités de police ne pourraient se dispenser de l'autorisation préalable mentionnée dans l'arrêt Prokuratuur.

90. À première vue, cette affirmation semblerait ne pas cadrer avec la non-application dans la présente affaire de la directive 2002/58 (qu'interprète l'arrêt Prokuratuur), ainsi que je l'ai soutenu précédemment. Je considère, toutefois, que la ratio de cet arrêt plaide en faveur de la même solution.

27 Voir point 36 des présentes conclusions.

28 Il s'agit d'une entreprise dont la difficulté est bien illustrée par les efforts fournis par la Commission aux points 34 et 39 de ses observations écrites en vue de contribuer à la définition de règles claires et précises pour la configuration des limites ou des garanties adéquates en matière d'accès aux données d'un téléphone portable.

29 Ce sont des règles qui, comme le rappellent, par exemple, les gouvernements danois et irlandais, ne relèvent pas du champ d'application du droit de l'Union, mais qui peuvent servir à satisfaire à une exigence découlant de ce droit.

30 Cour EDH, 16 octobre 2007, Wieser et Bicos Beteiligungen GmbH c. Autriche (CE :ECHR :2007 :1016JUD007433601, point 54) : « [l]e code autrichien de procédure pénale ne renferme aucune disposition spéciale régissant la fouille et la saisie de données électroniques. Il contient en revanche des dispositions détaillées sur la saisie d'objets et, en outre, des règles précises concernant la saisie de documents. Il est établi par la jurisprudence des tribunaux internes que ces dispositions s'appliquent aussi à la fouille et à la saisie de données électroniques [...] ».

31 Voir affirmations de la juridiction de renvoi citées au point 44 des présentes conclusions.

91. Le litige ayant donné lieu à l'arrêt Prokuratuur portait, comme dans la présente affaire, sur une enquête pénale individuelle, dirigée contre une personne déterminée, bien que l'accès aux données (métadonnées) ait été obtenu auprès de fournisseurs de services de communications électroniques. Il s'agissait de recueillir des « données concernant plusieurs numéros de téléphone de [...] et différentes identités internationales d'équipement mobile de celle-ci » [32].

92. Selon moi, dans l'arrêt Prokuratuur, deux plans peuvent être distingués : a) celui qui met en cause la réglementation générale d'un État membre relative à la conservation généralisée et indifférenciée ainsi qu'à l'accès ultérieur aux données détenues par les fournisseurs de services, et b) celui du contrôle préalable, dans un cas particulier, de l'accès à ces métadonnées, lorsqu'elles permettent de configurer un profil précis de la vie privée d'une personne.

93. La circonstance que, dans la présente affaire, les données révélant la vie privée ne sont pas détenues par les fournisseurs de services et sont obtenues (ou que l'on tente de les obtenir) à partir d'un seul téléphone saisi me semble d'une importance secondaire par rapport à la ratio de l'exigence d'un contrôle préalable préconisée dans l'arrêt Prokuratuur.

94. Ce contrôle préalable trouve son fondement ultime dans la protection garantie par les articles 7 et 8 de la Charte. L'autorité qui l'exerce doit être « en mesure d'assurer un juste équilibre entre, d'une part, les intérêts 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 » [33].

3. Sur la troisième question préjudicielle

95. Par la troisième question préjudicielle, la juridiction de renvoi souhaite savoir si l'article 47 de la Charte (le cas échéant, lu conjointement avec ses articles 41 et 52) s'oppose à une réglementation telle que la législation autrichienne [34] qui « permet l'exploitation des données numériques d'un téléphone portable sans que la personne concernée soit informée de la mesure au préalable ou, au moins, après qu'elle a été prise ».

96. J'estime que la question ainsi rédigée pourrait ne pas être nécessaire pour résoudre le litige, dès lors que la personne concernée a pu exercer le droit consacré à l'article 47 de la Charte, en demandant à la juridiction de renvoi de déclarer la nullité de l'action de la police sur le téléphone saisi, qui incluait l'exploitation ultérieure (et infructueuse) des données qui y sont conservées.

97. En ce qui concerne ces deux moments de l'action de la police, il conviendrait d'opérer la distinction suivante :

– s'agissant de la saisie du téléphone en soi, il ressort des éléments du dossier que la personne concernée en a eu connaissance et qu'elle a refusé de fournir aux autorités de police le code d'accès lors de la saisie ;

– s'agissant de la tentative d'analyse des données, tout paraît indiquer que le responsable du traitement n'a pas informé la personne concernée de cette opération, bien que le

[32] Arrêt Prokuratuur, point 17.

[33] Arrêt Prokuratuur, point 52.

[34] Elle se réfère de nouveau à l'article 18 de la StPo, lu conjointement avec son article 99.

gouvernement autrichien affirme que cette dernière a eu connaissance d'un rapport constatant l'intervention de la police judiciaire sur le téléphone [35].

98. Il subsiste donc autour de l'exploitation des données et de leur connaissance par la personne concernée certaines ambiguïtés qui, comme je l'ai déjà indiqué, auraient dû être clarifiées par la juridiction de renvoi dans l'ordonnance de renvoi et qui empêchent de donner une réponse utile à la troisième question préjudicielle.

99. En tout état de cause, dans le cas où la Cour ne considérerait pas cette question comme irrecevable, je me prononcerai sur celle-ci. Dans cette hypothèse, et compte tenu de l'inapplicabilité de la directive 2002/58, il conviendrait de la reformuler à la lumière de la directive 2016/680, dont les articles 13, 15 et 54 fournissent les pistes pour y répondre.

100. Conformément à la directive 2016/680, les informations relatives au traitement des données qu'il convient de fournir à la personne concernée sont celles qui sont nécessaires, entre autres, pour : a) introduire une réclamation auprès d'une autorité de contrôle [article 13, paragraphe 1, sous d)], et b) bénéficier d'un recours juridictionnel effectif contre la violation des droits garantis par la directive 2016/680, sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert (article 54).

101. Toutefois, il convient de ne pas oublier que tant l'article 13, paragraphe 3, que l'article 15, paragraphe 1, de la directive 2016/680 autorisent les États membres à adopter des mesures législatives par lesquelles :

– la fourniture des informations à la personne concernée en application de l'article 13, paragraphe 2, est retardée, limitée ou omise ;

– le droit d'accès de la personne concernée aux données traitées est limité, entièrement ou partiellement, dès lors et aussi longtemps qu'une telle limitation constitue une mesure nécessaire et proportionnée afin, notamment, d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ou de nuire aux enquêtes en matière d'infractions pénales [36].

102. En tout état de cause, la licéité du traitement des données dépend non pas du respect par les autorités compétentes des obligations (ultérieures) que leur impose l'article 13 de la directive 2016/680, mais de la légalité de la finalité qui l'a justifié ; autrement dit, du fait que ces autorités administratives étaient en droit de procéder au traitement des données à caractère personnel.

103. De ce point de vue, le fait que la personne concernée ait été informée des tentatives d'accès aux données conservées dans le téléphone qui a été saisi est étranger, en soi, à la licéité pour des motifs de fond de l'action de la police. Le comportement du responsable du traitement qui est éventuellement contraire aux obligations que lui impose l'article 13 de la directive 2016/680 pourra avoir d'autres conséquences, mais, je le répète, il n'affecte pas en soi la licéité ou l'illicéité de ce traitement.

[35] Point 37 de ses observations écrites.

[36] Voir, en ce sens, arrêt du 21 décembre 2016, Tele2 Sverige et Watson (C-203/15 et C-698/15, EU:C:2016:970, point 121). Sa jurisprudence relative à la directive 2002/58 peut être transposée à la directive 2016/680 dans le contexte de la garantie de la protection juridictionnelle des droits des titulaires de données faisant l'objet de traitement.

104. Il appartient à la juridiction de renvoi de déterminer si la réglementation nationale permet l'exercice efficace de ces droits par la personne concernée.

V. Conclusion

105. Eu égard à ce qui précède, je propose à la Cour de déclarer irrecevable la demande de décision préjudicielle introduite par le Landesverwaltungsgericht Tirol (tribunal administratif régional du Tyrol, Autriche).

À titre subsidiaire, je suggère de répondre à cette demande dans les termes suivants :

1) L'article 4, paragraphe 1, sous a), et l'article 8, paragraphe 1, 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, lus conjointement avec les articles 7, 8 et 52 de la charte des droits fondamentaux de l'Union européenne,

   doivent être interprétés en ce sens que :

   dans le cadre d'une enquête pénale, l'accès par les autorités publiques aux données à caractère personnel stockées dans un téléphone portable, en vue de leur traitement, n'est pas limité aux cas de lutte contre la criminalité grave.

   Un tel accès doit être justifié au cas par cas et limité à ce qui est strictement nécessaire et proportionné, en fonction de la nature des infractions pénales poursuivies et des données à caractère personnel auxquelles l'accès est demandé.

   Les autorités de police ne sauraient obtenir, de leur propre initiative et sans l'autorisation préalable d'une juridiction, dans le cadre d'une enquête pénale, un accès complet et non contrôlé à l'ensemble des données stockées dans un téléphone portable, lorsque celles-ci permettent d'obtenir une image précise de la vie privée d'une personne.

2) Les articles 13, 15 et 54 de la directive 2016/680, lus conjointement avec les articles 47 et 52 de la charte des droits fondamentaux,

   doivent être interprétés en ce sens que :

   sans préjudice des limitations autorisées par l'article 15, paragraphe 1, de la directive 2016/680, ou de tout recours administratif ou extrajudiciaire qui lui est ouvert, le propriétaire d'un téléphone portable doit être informé du traitement qu'effectuent les autorités concernées des données à caractère personnel qui y sont stockées, au moment opportun et dans les conditions nécessaires pour garantir l'exercice effectif de son droit au recours juridictionnel contre une éventuelle violation des droits conférés par la directive 2016/680.