Version anonymisée

Affaire C-241/22

Demande de décision préjudicielle

Date de dépôt :

6 avril 2022

Juridiction de renvoi :

Hoge Raad der Nederlanden (Pays-Bas)

Date de la décision de renvoi :

5 avril 2022

Partie requérante :

Advocaat-generaal bij de Hoge Raad der Nederlanden

HOGE RAAD DER NEDERLANDEN

CHAMBRE PÉNALE

[OMISSIS]

Date 5 avril 2022

ARRÊT

rendu sur le pourvoi en cassation formé dans l'intérêt de la loi par l'avocat général près le Hoge Raad der Nederlanden (Cour suprême, Pays-Bas) contre l'ordonnance du rechtbank Gelderland (tribunal de la Gueldre) du 15 septembre 2021, [OMISSIS] dans l'affaire

concernant

DX,

[OMISSIS] ci-après : le suspect[*].

1. L'ordonnance du rechtbank (tribunal) [Gueldre]

Le rechtbank (tribunal) a annulé la décision du rechter-commissaris (juge d'instruction) par laquelle ce dernier a rejeté la demande de l'officier van justitie (procureur) visant à obtenir l'autorisation de demander la communication de données historiques relatives au trafic, et le rechtbank (tribunal) a accédé à cette demande.

2. Le pourvoi en cassation

L'avocat général B.F. Keulen a formé un pourvoi en cassation dans l'intérêt de la loi. Le pourvoi en cassation est joint au présent arrêt dont il fait partie intégrante. La demande tend à la suspension de l'examen du pourvoi en cassation afin de poser des questions préjudicielles à la Cour de justice de l'Union européenne sur l'interprétation 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) (ci-après la « directive 2002/58 ») ou, à tout le moins, à obtenir l'annulation de l'ordonnance du rechtbank (tribunal).

3. L'objet de la présente affaire

En résumé, dans son pourvoi, l'avocat général constate qu'il y a en pratique un manque de clarté sur les conditions d'application auxquelles le procureur doit se conformer pour demander la communication de données relatives au trafic ou de données de localisation d'un utilisateur d'un service de télécommunication. Il s'agit, en particulier, d'identifier les exigences qui découlent de la directive 2002/58 [1] et de la jurisprudence de la Cour concernant cette directive. Dans son pourvoi, l'avocat général aborde un certain nombre de questions

[*] Ndt : En néerlandais, « verdachte ». L'intéressé a sans aucun doute un autre statut, puisqu'il a été mis en détention, mais le terme est utilisé à plusieurs endroits dans le texte, et notamment dans la législation, en un sens moins étroit pour lequel les notions de « prévenu » ou « inculpé » seraient inadéquates. Pour la demande de décision préjudicielle, le statut précis de l'intéressé est au demeurant dépourvu de pertinence.

[1] JO 2002, L 201, p. 37 ; modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (JO 2009, L 337, p. 11).

relatives aux conséquences de la directive 2002/58 et de la jurisprudence de la Cour sur l'application du droit de la procédure pénale néerlandais, et il soumet ces questions au Hoge Raad (Cour suprême, Pays-Bas) sur la base de la décision du rechtbank (tribunal) et de deux décisions d'un juge d'instruction. Ces dernières décisions sont inscrites au rôle dans les affaires 21/04309 CW (ECLI:NL:HR:2022:476) et 21/04311 CW (ECLI:NL:HR:2022:477).

[OMISSIS]

4. Les considérations du rechtbank (tribunal)

4.1 La décision du rechtbank (tribunal) a été rendue sur l'appel formé par le procureur contre le rejet d'une demande d'octroi d'une autorisation écrite visant l'obtention de données historiques/futures visées à l'article 126n, paragraphe 1, du code de procédure pénale. [OMISSIS]

> [OMISSIS]
>
> [OMISSIS] [le contenu de la décision du juge d'instruction est repris au point 4.2]

4.2 Le rechtbank (tribunal) a annulé l'ordonnance du juge d'instruction et a accédé à la demande du procureur. L'ordonnance du rechtbank (tribunal) s'énonce comme suit :

> « [OMISSIS]
>
> La demande [du procureur] vise des données d'un utilisateur d'un service de télécommunication et le trafic des communications concernant cet utilisateur, qui peut être désigné comme étant « DX ». Il s'agit des données concernant le numéro de téléphone portable néerlandais (voix uniquement) : 316(...), entre le 9 août 2021 et le 12 août 2021.
>
> [OMISSIS]
>
> [OMISSIS] [procédure]
>
> L'appréciation du juge d'instruction
>
> Le juge d'instruction a fondé sa décision de rejet sur le fait qu'il découle de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152) que l'accès aux données demandées ne peut être accordé que dans des procédures visant la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique. Dans le contexte néerlandais, on peut rattacher cette condition au critère du soupçon d'infraction visée à l'article 67, paragraphe 1, du

code de procédure pénale qui, compte tenu de sa nature ou de sa connexité avec d'autres infractions pénales commises par le suspect, constitue une atteinte grave à l'ordre juridique. En outre, le recours à cet outil d'investigation doit être proportionné et de nature subsidiaire. Le juge d'instruction estime qu'il y a lieu de rejeter la présente demande parce que le vol d'une pelleteuse, par nature, ne constitue pas une atteinte grave à l'ordre juridique et qu'il n'y a aucune connexité avec d'autres infractions pénales commises (par le suspect).

Le point de vue du procureur

L'appel tend à obtenir l'annulation de la décision du juge d'instruction. Le procureur considère que le juge d'instruction a appliqué un critère erroné à la question de savoir s'il y a ou non « criminalité grave », au sens de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152). Selon le procureur, le critère appliqué est (beaucoup) trop strict aux fins de l'appréciation exigée aux articles 126n et 126ng du code de procédure pénale. Il s'agit de techniques d'enquête spéciales relativement peu intrusives pour le suspect, par rapport à des techniques plus intrusives telles que des écoutes téléphoniques. En appliquant ce critère strict lors de l'appréciation de la demande d'autorisation, le juge d'instruction s'écarte de la décision que le législateur a associée à l'obtention de données relatives au trafic et/ou de données de localisation visées aux articles 126n et 126ng du code de procédure pénale. Selon le procureur, la circonstance que le suspect soit passible d'un emprisonnement de six ans maximum et qu'il puisse faire l'objet d'une détention provisoire fait que l'on peut parler d'une « criminalité grave » au sens de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152). En outre, la chambre du conseil a ordonné un maintien en détention de 90 jours sur le fondement d'un risque de récidive important. Le fait que le suspect fasse l'objet de poursuites implique une raison impérieuse de sécurité publique qui impose une privation de liberté immédiate. Selon le procureur, la circonstance que le suspect est poursuivi démontre *a fortiori* l'existence d'une « criminalité grave » au sens de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152).

Recevabilité

[OMISSIS] [recevabilité de la demande du procureur]

Appréciation

Conformément à l'appréciation opérée par le Rotterdamse rechtbank (tribunal de Rotterdam) dans l'arrêt du 30 avril 2021 (ECLI:NL:RBROT:2021:3906), la chambre du conseil considère qu'il ressort notamment de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152) que l'accès, à des fins répressives, aux données de communications visées dans cet arrêt, à savoir les données relatives au trafic et les données de localisation, ne peut être accordé que dans le cadre de procédures visant la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique. Il s'agit en effet d'une ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »), les données à caractère personnel demandées permettant de tirer des conclusions précises concernant la vie privée de la personne concernée.

En l'espèce, il convient donc d'examiner, en premier lieu, si la demande portant sur les données concernées a été faite dans le cadre d'une procédure visant la lutte contre la criminalité grave. La chambre du conseil estime que cette question appelle une réponse affirmative. La demande a été faite dans le cadre d'une enquête pénale concernant un vol qualifié, commis par deux ou plusieurs personnes, d'un bien d'une valeur d'environ 18 000 euros. Il s'agit d'une infraction pénale passible d'un emprisonnement de six ans maximum, pour lequel la détention provisoire est autorisée (une ordonnance de détention a d'ailleurs été prononcée à l'encontre du suspect) et qui constitue une atteinte grave à l'ordre juridique.

Eu égard à ce qui précède, il y a lieu d'annuler l'ordonnance du juge d'instruction et d'accéder à la demande du procureur.

[OMISSIS]

5. Cadre juridique

Le code de procédure pénale

5.1.1 Le code de procédure pénale confère au procureur le pouvoir de demander, dans l'intérêt de l'enquête, la communication de données (historiques et/ou futures) concernant i) un utilisateur d'un service de communication, et ii) le trafic des communications concernant cet utilisateur. Il s'agit des données dites relatives au trafic et des données dites de localisation. Ces données concernent notamment les connexions qui ont été établies par ou avec l'utilisateur et la localisation d'un point de terminaison du réseau ou la position géographique de l'équipement périphérique d'un utilisateur en cas

de connexion ou de tentative de connexion [2]. Le procureur a en outre le pouvoir de demander la communication des données d'identification, c'est-à-dire les données relatives au nom, à l'adresse, au code postal, au domicile, au numéro et au type de service d'un utilisateur d'un service de communication. Ces demandes peuvent être adressées à tout fournisseur d'un service de communication.

5.1.2 Ces pouvoirs sont avant tout établis aux articles 126n et 126na du code de procédure pénale.

L'article 126n du code de procédure pénale dispose que :

> « 1. En cas de soupçon d'infraction visée à l'article 67, paragraphe 1, le procureur peut demander, dans l'intérêt de l'enquête, la communication de données concernant un utilisateur d'un service de communication et le trafic des communications concernant cet utilisateur. La demande ne peut porter que sur des données désignées par mesure générale d'administration. Il peut s'agir :
>
> a. de données qui ont été traitées à la date de la demande, ou
>
> b. de données qui seront traitées après la date de la demande.
>
> 2. La demande visée au paragraphe 1 peut être adressée à tout fournisseur d'un service de communication. L'article 96a, paragraphe 3, s'applique *mutatis mutandis*. Si la demande visée au paragraphe 1 concerne une personne qui peut se prévaloir de la protection des sources, cette demande ne peut être adressée qu'après autorisation écrite accordée par le juge d'instruction sur demande du procureur. L'article 218a, paragraphe 2, s'applique *mutatis mutandis*.
>
> 3. Si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), cette demande est formulée pour une période de trois mois maximum.
>
> 4. Le procureur fait dresser un procès-verbal de la demande, mentionnant :
>
> a. l'infraction et, s'il est connu, le nom ou un autre moyen d'identification aussi précis que possible du suspect ;
>
> b. les faits ou les circonstances attestant du respect des conditions visées au paragraphe 1, première phrase ;

[2] Voir également l'article 2 de l'arrêté relatif à la demande de données de télécommunication, cité au point 5.3.

c. s'il est connu, le nom ou un autre moyen d'identification aussi précis que possible de la personne visée par la demande de données ;

d. les données demandées ;

e. si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), la période visée par la demande.

5. Si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), celle-ci expire immédiatement lorsque les conditions visées au paragraphe 1, première phrase, ne sont plus remplies. Le procureur fait dresser un procès-verbal de toute modification, complément, prolongation ou expiration de la demande.

6. Des règles concernant les modalités à respecter par le procureur pour demander les données peuvent être établies par la voie d'une mesure générale d'administration. »

L'article 67, paragraphe 1, du code de procédure pénale, auquel renvoie l'article 126n du code de procédure pénale, dispose que :

« Une ordonnance de détention provisoire peut être prononcée en cas de soupçon :

a. d'une infraction légalement passible d'un emprisonnement de quatre ans ou plus ;

b. de l'une des infractions décrites à l'article 132, l'article 138a, l'article 138aa, l'article 138ab, l'article 138b, l'article 138c, l'article 139c, l'article 139d, paragraphes 1 et 2, l'article 139h, paragraphes 1 et 2, l'article 139g, l'article 140, paragraphe 2, l'article 141a, l'article 137c, paragraphe 2, l'article 137d, paragraphe 1, l'article 137e, paragraphe 2, l'article 137g, paragraphe 2, l'article 151, l'article 184a, l'article 254a, l'article 248d, l'article 248e, l'article 272, l'article 284, paragraphe 1, l'article 285, paragraphe 1, l'article 285b, l'article 285c, l'article 300, paragraphe 1, l'article 321, l'article 326c, paragraphe 2, l'article 326d, l'article 340, l'article 342, l'article 344a, l'article 344b, l'article 347, paragraphe 1, l'article 350, l'article 350a, l'article 350c, l'article 350d, l'article 351, l'article 395, l'article 417bis, l'article 420bis.1, l'article 420quater et l'article 420quater.1 du code de procédure pénale ;

c. de l'une des infractions décrites aux articles suivants :

article 86i, paragraphe 1, de l'*Elektriciteitswet 1998* (loi relative à l'électricité de 1998) ;

article 66h, paragraphe 1, du *Gaswet* (loi relative au gaz) ;

article 8.12, paragraphes 1 et 2, du *Wet dieren* (loi relative aux animaux) ;

article 175, paragraphe 2, sous b), ou 3, lu en combinaison avec le paragraphe 1, sous b), et article 176, paragraphe 2, dans la mesure où l'objet relève de l'article 7, paragraphe 1, sous a) et c), du *Wegenverkeerswet 1994* (loi relative à la circulation routière de 1994) ;

article 30, paragraphe 2, du *Wet buitengewone bevoegdheden burgerlijk gezag* (loi relative aux compétences extraordinaires de l'autorité civile) ;

article 52, article 53, paragraphe 1, et article 54 du *Wet gewetensbezwaren militaire dienst* (loi relative à l'objection de conscience dans le cadre du service militaire) ;

article 36 du *Wet op de kansspelen* (loi relative aux jeux de hasard) ;

article 11, paragraphe 2, et article 11 a de l'*Opiumwet* (loi relative à l'opium) ;

article 55, paragraphe 2, du *Wet wapens en munitie* (loi relative aux armes et aux munitions) ;

article 11 du *Wet tijdelijk huisverbod* (loi relative à l'interdiction temporaire de résidence) ;

article 8 du *Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding* (loi temporaire concernant des mesures administratives de lutte contre le terrorisme). »

L'article 126na du code de procédure pénale dispose que :

« 1. En cas de soupçon d'infraction, l'officier de police judiciaire peut demander, dans l'intérêt de l'enquête, la communication de données relatives au nom, à l'adresse, au code postal, au domicile, au numéro et au type de service d'un utilisateur d'un service de communication. L'article 126n, paragraphe 2, est applicable.

2. Si le fournisseur ne connaît pas les données visées au paragraphe 1, et si ces données sont nécessaires aux fins de l'application des articles 126m ou 126n, le procureur peut demander, dans l'intérêt de l'enquête, que le fournisseur collecte et fournisse les données demandées selon des modalités définies par la voie d'une mesure générale d'administration.

3. En cas de demande visée aux paragraphes 1 ou 2, l'article 126n, paragraphe 4, sous a), b), c) et d), s'applique *mutatis mutandis* et l'article 126bb est inapplicable.

4. Des règles concernant les modalités à respecter par l'officier de police judiciaire ou le procureur pour demander les données peuvent être établies par la voie d'une mesure générale d'administration. »

Les termes « fournisseur d'un service de communication » et « utilisateur d'un service de communication », employés dans les dispositions ci-dessus, sont définis aux articles 138g et 138h du code de procédure pénale.

L'article 138g du code de procédure pénale dispose que :

« On entend par "fournisseur d'un service de communication" la personne physique ou morale qui, dans l'exercice de sa profession ou des activités de son entreprise, permet aux utilisateurs de son service de communiquer au moyen d'un dispositif automatisé, ou qui traite ou conserve des données aux fins de ce service ou au profit des utilisateurs de ce service. »

L'article 138h du code de procédure pénale dispose que :

« On entend par "utilisateur d'un service de communication" la personne physique ou morale qui conclut un contrat avec le fournisseur d'un service de communication concernant l'utilisation de ce service ou qui, dans les faits, a recours à ce service. »

5.1.3 Outre les pouvoirs établis aux articles 126n et 126na du code de procédure pénale, l'article 126ng du même code prévoit un mécanisme permettant d'adresser une demande de communication de données à un fournisseur d'un service de communication. Il s'agit des situations dans lesquelles la demande concerne des données autres que celles visées aux articles 126n et 126na du code de procédure pénale. En résumé, l'article 126ng du code de procédure pénale permet d'exercer les pouvoirs de demander, dans ces situations, des données visées aux articles 126nc (données d'identification), 126nd (données autres que les données d'identification) et 126ne (données futures) du code de procédure pénale. L'article 126ng, paragraphe 2, impose par ailleurs des exigences supplémentaires lorsque la demande concerne des données qui sont conservées dans le dispositif automatisé du fournisseur mais qui ne sont pas destinées à ce fournisseur ou qui ne proviennent pas de celui-ci.

L'article 126ng du code de procédure pénale dispose que :

« 1. Une demande visée à l'article 126nc, paragraphe 1, l'article 126nd, paragraphe 1, ou l'article 126ne, paragraphes 1 et 3, et l'article 126nf, paragraphe 1, peut être adressée au fournisseur d'un

service de communication au sens de l'article 138g, pour autant que cette demande porte sur des données autres que celles qui peuvent faire l'objet d'une demande au titre des articles 126n et 126na. La demande ne peut pas concerner des données qui sont conservées dans le dispositif automatisé du fournisseur et qui ne sont pas destinées à ce fournisseur ou qui ne proviennent pas de celui-ci.

2. En cas de soupçon d'infraction visée à l'article 67, paragraphe 1, qui, compte tenu de sa nature ou de sa connexité avec d'autres infractions pénales commises par le suspect, constitue une atteinte grave à l'ordre juridique, le procureur peut, si l'intérêt de l'enquête l'exige de manière impérieuse, demander la communication des données visées à la dernière phrase du paragraphe 1 au fournisseur dont on peut raisonnablement présumer qu'il a accès à ces données, pour autant que les données en question proviennent manifestement du suspect, qu'elles lui soient destinées, qu'elles le concernent ou qu'elles aient servi à commettre l'infraction, ou que l'infraction pénale ait manifestement été commise en lien avec ces données.

3. Une demande visée au paragraphe 2 ne peut pas être adressée au suspect. L'article 96a, paragraphe 3, s'applique *mutatis mutandis*.

4. Une demande visée au paragraphe 2 ne peut être adressée qu'après autorisation écrite accordée par le juge d'instruction sur demande du procureur. L'article 126l, paragraphe 7, s'applique *mutatis mutandis*.

5. L'article 126nd, paragraphes 3, 4, 5 et 7, s'applique *mutatis mutandis*. »

5.1.4 L'article 126ni, paragraphe 1, du code de procédure pénale permet en outre de demander à la personne dont on peut raisonnablement présumer qu'elle a accès à certaines données qui sont conservées dans un dispositif automatisé à la date de la demande et dont on peut raisonnablement présumer qu'elles sont particulièrement susceptibles de perte ou de modification qu'elle conserve et mette à disposition ces données pendant une période de 90 jours maximum. L'article 126ni, paragraphe 2, du code de procédure pénale dispose que si cette demande est adressée à un fournisseur d'un service de communication et qu'elle concerne, en tout ou en partie, des données visées à l'article 126n, paragraphe 1, du code de procédure pénale (et donc des données concernant un utilisateur d'un service de communication et le trafic des communications concernant cet utilisateur), le fournisseur est tenu de communiquer, dans les meilleurs délais, les données permettant d'identifier les autres fournisseurs dont les services ont été utilisés aux fins de la communication. Le pouvoir établi à l'article 126ni du code de procédure pénale peut également s'exercer en cas de soupçon d'infraction visée à l'article 67, paragraphe 1, du code de procédure pénale qui, compte tenu de

sa nature ou de sa connexité avec d'autres infractions pénales commises par le suspect, constitue une atteinte grave à l'ordre juridique.

L'article 126ni du code de procédure pénale dispose que :

> « 1. En cas de soupçon d'infraction visée à l'article 67, paragraphe 1, du code de procédure pénale qui, compte tenu de sa nature ou de sa connexité avec d'autres infractions pénales commises par le suspect, constitue une atteinte grave à l'ordre juridique, le procureur peut, si l'intérêt de l'enquête l'exige de manière impérieuse, demander à la personne dont on peut raisonnablement présumer qu'elle a accès à certaines données qui sont conservées dans un dispositif automatisé à la date de la demande et dont on peut raisonnablement présumer qu'elles sont particulièrement susceptibles de perte ou de modification qu'elle conserve et mette à disposition ces données pendant une période de 90 jours maximum. La demande ne peut pas être adressée au suspect.
>
> 2. Si la demande est adressée à un fournisseur d'un service de communication au sens de l'article 138g et qu'elle concerne, en tout ou en partie, des données visées à l'article 126n, paragraphe 1, le fournisseur est tenu de communiquer, dans les meilleurs délais, les données permettant d'identifier les autres fournisseurs dont les services ont été utilisés aux fins de la communication.
>
> 3. La demande est adressée par écrit ou oralement. En cas de demande orale, le procureur la fait mettre par écrit dans les meilleurs délais et en délivre une copie certifiée conforme au destinataire dans les trois jours qui suivent la demande orale. La demande, et sa mise par écrit, mentionnent les éléments suivants :
>
> a. une description aussi précise que possible des données qui doivent être mises à disposition ;
>
> b. la date de la demande ;
>
> c. l'intitulé de la demande ;
>
> d. la période pendant laquelle les données doivent rester disponibles, et
>
> e. l'application, le cas échéant, du paragraphe 2.
>
> 4. Le procureur fait dresser un procès-verbal de la demande et, si elle a été faite oralement, de la constatation par écrit de cette demande. Le procès-verbal mentionne :
>
> a. les données visées au paragraphe 3 ;

b. l'infraction et, s'il est connu, le nom ou un autre moyen d'identification aussi précis que possible du suspect ; et

c. les faits ou les circonstances attestant du respect des conditions visées au paragraphe 1.

5. La demande ne peut être prolongée qu'une seule fois pour une période de 90 jours maximum. Les paragraphes 2, 3 et 4 s'appliquent *mutatis mutandis*. »

5.2 Les pouvoirs évoqués au point 5.1 peuvent également être exercés si, eu égard aux faits et aux circonstances, on peut raisonnablement présumer que des infractions visées à l'article 67, paragraphe 1, du code de procédure pénale sont planifiées ou commises en bande organisée, lorsque ces infractions, compte tenu de leur nature ou de leur connexité avec d'autres infractions pénales planifiées ou commises dans le cadre de cette bande organisée, constituent une atteinte grave à l'ordre juridique (voir article 126o, paragraphe 1, du code de procédure pénale). Ces pouvoirs peuvent également être exercés lorsqu'il existe des indices d'une infraction terroriste. Ces questions sont régies par les articles 126u, 126ua, 126ug, 126ui, 126zh, 126zi, 126zja et 126zo du code de procédure pénale.

L'article 126u du code de procédure pénale dispose que :

« 1. Dans un cas tel que visé à l'article 126o, paragraphe 1, le procureur peut, dans l'intérêt de l'enquête, demander la communication de données concernant un utilisateur d'un service de communication au sens de l'article 126la et le trafic des communications concernant cet utilisateur. La demande ne peut porter que sur des données désignées par mesure générale d'administration. Il peut s'agir :

a. de données qui ont été traitées à la date de la demande, ou

b. de données qui seront traitées après la date de la demande.

2. La demande visée au paragraphe 1 peut être adressée à tout fournisseur d'un service de communication. L'article 96a, paragraphe 3, s'applique *mutatis mutandis*. Si la demande visée au paragraphe 1 concerne une personne qui peut se prévaloir de la protection des sources, cette demande ne peut être adressée qu'après autorisation écrite accordée par le juge d'instruction sur demande du procureur. L'article 218a, paragraphe 2, s'applique *mutatis mutandis*.

3. Si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), celle-ci est adressée pour une période de trois mois maximum.

4. Le procureur fait dresser un procès-verbal de la demande, reprenant :

a. une description de la bande organisée ;

b. les faits ou les circonstances attestant du respect des conditions visées au paragraphe 1 ;

c. s'il est connu, le nom ou un autre moyen d'identification aussi précis que possible de la personne visée par la demande de données ;

d. les données demandées ;

e. si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), la période visée par la demande.

5. Si la demande concerne des données visées au paragraphe 1, deuxième phrase, sous b), celle-ci expire immédiatement lorsque les conditions visées au paragraphe 1, première phrase, ne sont plus remplies. Le procureur fait dresser un procès-verbal de toute modification, complément, prolongation ou expiration de la demande.

6. Des règles concernant les modalités à respecter par le procureur pour demander les données peuvent être établies par la voie d'une mesure générale d'administration. »

L'article 126ua du code de procédure pénale dispose que :

« 1. Dans un cas tel que visé à l'article 126o, paragraphe 1, l'officier de police judiciaire peut demander, dans l'intérêt de l'enquête, la communication de données relatives au nom, à l'adresse, au code postal, au domicile, au numéro et au type de service d'un utilisateur d'un service de communication au sens de l'article 126la. L'article 126u, paragraphe 2, est applicable.

2. Si le fournisseur ne connaît pas les données visées au paragraphe 1, et si ces données sont nécessaires aux fins de l'application des articles 126t ou 126u, le procureur peut demander, dans l'intérêt de l'enquête, que le fournisseur obtienne et fournisse les données demandées selon des modalités définies par la voie d'une mesure générale d'administration.

3. En cas de demande visée aux paragraphex 1 ou 2, l'article 126u, paragraphe 4, sous a), b), c) et d), s'applique *mutatis mutandis* et l'article 126bb n'est pas applicable.

4. Des règles peuvent être établies par la voie d'une mesure générale d'administration concernant les modalités à respecter par

l'officier de police judiciaire ou le procureur pour demander les données. »

L'article 126ug du code de procédure pénale dispose que :

« 1. Une demande visée à l'article 126uc, paragraphe 1, à l'article 126ud, paragraphe 1, ou à l'article 126ue, paragraphes 1 et 3, et à l'article 126uf, paragraphe 1, peut être adressée au fournisseur d'un réseau de télécommunication public ou non public, ou au fournisseur d'un service de télécommunication accessible au public ou non, pour autant que cette demande porte sur des données autres que celles qui peuvent faire l'objet d'une demande au titre des articles 126u et 126ua. La demande ne peut concerner des données qui sont conservées dans le dispositif automatisé du fournisseur mais qui ne sont pas destinées à ce fournisseur ou qui ne proviennent pas de celui-ci.

2. Dans les cas visés à l'article 126o, paragraphe 1, le procureur peut, si l'intérêt de l'enquête l'exige de manière impérieuse, demander la communication des données visées à la dernière phrase du paragraphe 1 au fournisseur dont on peut raisonnablement présumer qu'il a accès à ces données, pour autant que ces données proviennent manifestement d'une personne dont, compte tenu des faits et des circonstances, on peut raisonnablement présumer qu'elle est impliquée dans la planification ou la commission d'infractions en bande organisée, pour autant qu'elles lui soient destinées, qu'elles la concernent ou qu'elles aient servi à planifier ou commettre une infraction dans le cadre de cette bande organisée, ou qu'une infraction soit manifestement planifiée ou commise dans le cadre de cette bande organisée en lien avec ces données.

3. Une demande visée au paragraphe 2 ne peut pas être adressée au suspect. L'article 96a, paragraphe 3, s'applique *mutatis mutandis*.

4. Une demande visée au paragraphe 2 ne peut être adressée qu'après autorisation écrite accordée par le juge d'instruction sur demande du procureur. L'article 126l, paragraphe 7, s'applique *mutatis mutandis*.

5. L'article 126nd, paragraphes 3, 4, 5 et 7, s'applique *mutatis mutandis*. »

L'article 126ui du code de procédure pénale dispose que :

« 1. Dans les cas visés à l'article 126o, paragraphe 1, le procureur peut, si l'intérêt de l'enquête l'exige de manière impérieuse, demander à la personne dont on peut raisonnablement présumer qu'elle a accès à certaines données qui sont conservées dans un dispositif automatisé à

la date de la demande et dont on peut raisonnablement présumer qu'elles sont particulièrement susceptibles de perte ou de modification, qu'elle conserve et mette à disposition ces données pendant une période de 90 jours maximum. La demande ne peut être adressée au suspect.

2. L'article 126ni, paragraphes 2 à 5, s'applique *mutatis mutandis*, étant entendu que les faits et circonstances visés à l'article 126ni, paragraphe 4, sous c), incluent également une description de la bande organisée visée à l'article 126o, paragraphe 1. »

L'article 126zh du code de procédure pénale dispose que :

« 1. En cas d'indices d'une infraction terroriste, le procureur peut demander, dans l'intérêt de l'enquête, la communication de données concernant un utilisateur d'un service de communication au sens de l'article 126la et le trafic des communications lié à cet utilisateur. La demande ne peut porter que sur des données désignées par mesure générale d'administration. Il peut s'agir :

a. de données qui ont été traitées à la date de la demande, ou

b. de données qui seront traitées après la date de la demande.

2. L'article 126n, paragraphes 2 à 6, s'applique *mutatis mutandis*. »

L'article 126zi du code de procédure pénale dispose que :

« 1. En cas de soupçon d'infraction terroriste, l'officier de police judiciaire peut demander, dans l'intérêt de l'enquête, la communication de données relatives au nom, à l'adresse, au code postal, au domicile, au numéro et au type de service d'un utilisateur d'un service de communication au sens de l'article 138h. L'article 126n, paragraphe 2, est applicable.

2. Si le fournisseur ne connaît pas les données visées au paragraphe 1, et si ces données sont nécessaires aux fins de l'application des articles 126zf ou 126zg, le procureur peut demander, dans l'intérêt de l'enquête, que le fournisseur obtienne et fournisse les données demandées selon des modalités définies par la voie d'une mesure générale d'administration.

3. L'article 126na, paragraphes 3 et 4, s'applique *mutatis mutandis*. »

L'article 126zja du code de procédure pénale dispose que :

« 1. En cas d'indices d'une infraction terroriste, le procureur peut, si l'intérêt de l'enquête l'exige de manière impérieuse, demander à la personne dont on peut raisonnablement présumer qu'elle a accès à certaines données qui sont conservées dans un dispositif automatisé à la date de la demande et dont on peut raisonnablement présumer qu'elles sont particulièrement susceptibles de perte ou de modification, qu'elle conserve et mette à disposition ces données pendant une période de 90 jours maximum. La demande ne peut pas être adressée au suspect.

2. L'article 126ni, paragraphes 2 à 5, s'applique *mutatis mutandis*. »

L'article 126zo du code de procédure pénale dispose que :

« 1. Une demande visée à l'article 126zk, paragraphe 1, l'article 126zl, paragraphe 1, ou l'article 126zm, paragraphe 1, peut être adressée au fournisseur d'un service de communication au sens de l'article 138g, pour autant que cette demande porte sur des données autres que celles qui peuvent faire l'objet d'une demande au titre de l'article 126zh et l'article 126zi. La demande ne peut concerner des données qui sont conservées dans le dispositif automatisé du fournisseur mais qui ne sont pas destinées à ce fournisseur ou qui ne proviennent pas de celui-ci.

2. Si l'intérêt de l'enquête l'exige de manière impérieuse, le procureur peut demander la communication des données visées à la dernière phrase du paragraphe 1 au fournisseur dont on peut raisonnablement présumer qu'il a accès à ces données.

3. L'article 126nd, paragraphes 3, 4, 5 et 7, et l'article 126nf, paragraphes 2 et 3, s'appliquent *mutatis mutandis*. »

5.3 La mesure générale d'administration à laquelle se réfèrent les articles 126n, 126u et 126zh du code de procédure pénale est le *Besluit vorderen gegevens telecommunicatie* (arrêté relatif à la demande de données de télécommunication). Cet arrêté dispose notamment que :

« Article 1er

Dans le présent arrêté, on entend par :

a. utilisateur : un utilisateur visé à l'article 138h du code de procédure pénale ;

b. numéro : un numéro visé à l'article 1.1 du *Telecommunicatiewet* (loi relative aux télécommunications).

Article 2

Les données suivantes sont des données au sens de l'article 126n, paragraphe 1, deuxième phrase, l'article 126u, paragraphe 1, deuxième phrase, et l'article 126zh, paragraphe 1, deuxième phrase, du code de procédure pénale :

a. le nom, l'adresse et le domicile de l'utilisateur ;

b. les numéros de l'utilisateur ;

c. le nom, l'adresse, le domicile et le numéro de la personne physique ou morale avec laquelle l'utilisateur établit une connexion, a établi une connexion ou a tenté d'établir une connexion, ou de la personne physique ou morale qui a tenté d'établir une connexion avec l'utilisateur ;

d. la date et l'heure auxquelles la connexion avec l'utilisateur a été établie et achevée ainsi que la durée de la connexion ou, si aucune connexion n'a été établie, la date et l'heure auxquelles la tentative de connexion avec l'utilisateur a été effectuée, ainsi que l'écart entre cette heure et l'heure légale visée à l'article 1er, paragraphe 1 du *Wet van 16 juli 1958 tot nadere regeling van de wettelijke tijd* (loi du 16 juillet 1958 portant réglementation de l'heure légale) (Stb. 352) ;

e. les données de localisation du point de terminaison du réseau ou les données concernant la position géographique de l'équipement périphérique d'un utilisateur en cas de connexion ou de tentative de connexion ;

f. les numéros de l'équipement périphérique que l'utilisateur utilise ou a utilisé ;

g. les types de services auxquels l'utilisateur a recours ou a eu recours, ainsi que les données y afférentes ;

h. le nom, l'adresse et le domicile de la personne qui paie les décomptes concernant les services de télécommunication accessibles au public et les réseaux de télécommunication mis à la disposition de l'utilisateur, si cette personne n'est pas l'utilisateur.

5.4.1 La demande de communication des données visées au point 5.1 fait l'objet d'un procès-verbal [3]. Ces procès-verbaux et les autres pièces relevant de

[3] Article 126n, paragraphe 4, article 126na, paragraphe 3, article 126ng, paragraphe 5, en combinaison avec l'article 126nd, paragraphe 5, article 126ni, paragraphe 4, article 126u, paragraphe 4, article 126ua, paragraphe 3, article 126ug, paragraphe 5, en combinaison avec l'article 126nd, paragraphe 5, article 126ui, paragraphe 2, en combinaison avec l'article 126ni, paragraphe 4, article 126zh, paragraphe 2, article 126zh, paragraphe 3, article 126zja, paragraphe 2, en combinaison avec l'article 126ni, paragraphe 4, et article 126zo, paragraphe 3, en combinaison avec l'article 126nd, paragraphe 5, du code de procédure pénale.

l'exercice de ces pouvoirs sont, dans la mesure où ils sont pertinents pour l'instruction de l'affaire, versés au dossier de procédure dès que l'intérêt de l'enquête le permet [4]. Si aucun procès-verbal n'a été établi, il est fait mention de l'exercice des pouvoirs dans le dossier de procédure [5]. Le suspect peut consulter ces pièces de procédure. Il n'en va autrement, en résumé, que si, sur le fondement de l'article 149b du code de procédure pénale, il existe des motifs impérieux de ne pas verser les pièces au dossier de procédure [6].

5.4.2 L'article 126bb du code de procédure pénale établit en outre une obligation dite de notification. Au titre de l'article 126bb, paragraphe 1, du code de procédure pénale, le procureur, dès que l'intérêt de l'enquête le permet, notifie par écrit à la personne concernée, notamment, que les pouvoirs établis à l'article 126n, l'article 126ng, l'article 126ni, l'article 126u, l'article 126ug, l'article 126ui, l'article 126zh, l'article 126zja et l'article 126zo du code de procédure pénale ont été exercés. Cette obligation complète la réglementation de la consultation des pièces de procédure et vise à informer des personnes autres que le suspect de l'exercice des pouvoirs concernés. L'obligation de notification ne s'applique pas à l'exercice des pouvoirs établis aux articles 126na, 126ua et 126zi du code de procédure pénale.

5.4.3 Pour ce qui nous intéresse dans la présente affaire, l'article 126cc, paragraphe 1, du code de procédure pénale impose au procureur de conserver, tant que l'affaire n'est pas close, les procès-verbaux et les autres objets dont peuvent être tirées des données obtenues au moyen d'une demande de données concernant un utilisateur et le trafic des communications lié à cet utilisateur, dans la mesure où ces pièces n'ont pas été versées au dossier de procédure. Le procureur tient ces procès-verbaux et autres objets à la disposition de l'instruction. Lorsque l'affaire est close, le procureur procède à leur destruction, conformément à l'article 126cc, paragraphes 2 et 3, du code de procédure pénale. Les modalités de conservation et de destruction sont régies par le *Besluit bewaren en vernietigen niet-gevoegde stukken* (arrêté concernant la conservation et la destruction des pièces non versées). Conformément à l'article 126dd, paragraphe 1, du code de procédure pénale, il est possible de renoncer à la destruction lorsque les pièces concernées peuvent être utilisées aux fins d'une enquête pénale autre que celle pour laquelle les pouvoirs ont été exercés ou, dans certains cas, aux fins de leur traitement sur la base du *Wet politiegegevens* (loi relative aux données de police). Dans ces situations,

4 Article 126aa, paragraphe 1, et article 149a, paragraphe 2, du code de procédure pénale.

5 Article 126aa, paragraphe 4, du code de procédure pénale.

6 Voir, également, article 149b du code de procédure pénale (en combinaison avec l'article 187d, paragraphe 1, du code de procédure pénale) et article 126aa, paragraphe 4, deuxième phrase, du code de procédure pénale.

l'article 126dd, paragraphe 2, du code de procédure pénale précise à quel moment les données seront finalement détruites.

5.5 Le code de procédure pénale n'impose pas aux fournisseurs de télécommunications une obligation générale d'enregistrer les données pouvant être demandées en application des pouvoirs mentionnés ci-dessus [7]. Ainsi que l'avocat général l'énonce aux points 20 à 22 de son pourvoi, les dispositions incluses – aux fins de la lutte contre la criminalité – dans le *Telecommunicatiewet* (loi relative aux télécommunications) qui concerne les délais de conservation des données relatives au trafic, des données de localisation et des données d'identification ont été écartées par le juge. Cette décision d'écarter ces dispositions est la conséquence de la déclaration d'invalidité de la directive 2006/24/CE prononcée par la Cour [8]. La législation qui a pour objet d'établir un régime modifié pour ces obligations de conservation est toujours en préparation [9]. Le code de procédure pénale prévoit l'exercice des pouvoirs évoqués ci-dessus à l'égard des données qui sont enregistrées et conservées sur un autre fondement que ces dispositions légales rendues inopérantes.

Le droit de l'Union

5.6 Le droit de l'Union prévoit des règles pour le traitement et la conservation, par les fournisseurs de services de communications électroniques, des données relatives au trafic et des données de localisation (y compris les données d'identification [10]). Ces règles sont établies par la directive 2002/58. Les dispositions pertinentes de cette directive s'énoncent comme suit :

« Article 1

Champ d'application et objectif

7 Des obligations de conservation spécifiques, dans la mesure où elles découlent des régimes de l'article 126ni et l'article 126n, paragraphe 1, phrase liminaire et sous b), du code de procédure pénale, sont abordées aux points 6.3.3 et 6.3.4.

8 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54).

9 Proposition de loi 34537.

10 Par « données relatives au trafic », on entend : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation (article 2, sous b), de la directive 2002/58). Ces données incluent toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Lorsque ces données sont traduites par le réseau par lequel la communication est transmise en vue d'effectuer la transmission, elles constituent des données relatives au trafic. Voir quinzième considérant du préambule de la directive 2002/58.

1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, 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 des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas (…) aux activités de l'État dans des domaines relevant du droit pénal.

Article 2

Définitions

Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive « cadre ») s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) « utilisateur » : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

b) « données relatives au trafic » : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;

c) « données de localisation » : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

d) « communication » : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de

communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ;

(...)

Article 3

Services concernés

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.

(...)

Article 5

Confidentialité des communications

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.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information

claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

Article 6

Données relatives au trafic

1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

(...)

Article 9

Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou

des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée.

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

Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152).

Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) ; et arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18 ; EU:C:2020:791).

(...)

Article 15

Application de certaines dispositions de la directive 95/46/CE

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. 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, du traité sur l'Union européenne. »

5.7 Dans les arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) et du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), la Cour, en bref, a examiné la question des conditions auxquelles une obligation de conservation des données relatives au trafic et des données de localisation incombant aux fournisseurs de services de télécommunications électroniques, aux fins – en substance – de la lutte contre la criminalité, était compatible avec l'article 15, paragraphe 1, de la directive 2002/58 [11]. Dans ces arrêts, et dans l'arrêt Ministerio Fiscal [12], la Cour a (également) abordé la question des conditions auxquelles les autorités nationales compétentes pouvaient se voir accorder l'accès aux données conservées par les fournisseurs de services de télécommunications électroniques. Les considérations pertinentes de ces arrêts de la Cour sont reproduites aux points 26 à 41 du pourvoi de l'avocat général.

5.8 Dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), la Cour a répondu à des questions préjudicielles concernant les conditions auxquelles les autorités nationales peuvent obtenir l'accès à un ensemble de données relatives au trafic ou de données de localisation [13]. La Cour a en outre examiné les exigences relatives au contrôle (juridictionnel) préalable à l'octroi de l'accès aux données conservées et, en lien avec cela, la question de savoir si le procureur pouvait également effectuer ce contrôle. Les considérations pertinentes de cet arrêt sont reproduites aux points 42 à 47 du pourvoi de l'avocat général.

11 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791.

12 Arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788.

13 Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152.

5.9 Le Hoge Raad (Cour suprême, Pays-Bas) examinera ci-dessous la signification et les (éventuelles) conséquences de cette jurisprudence de la Cour sur l'exercice des pouvoirs établis par le code de procédure pénale, cités aux points 5.1 et 5.2.

6. Le sens et les (éventuelles) conséquences du droit de l'Union sur l'exercice des pouvoirs établis par le code de procédure pénale

6.1 La jurisprudence de la Cour concernant, en particulier, la conservation des données relatives au trafic et des données de localisation ainsi que l'octroi de l'accès à ces données a soulevé dans la pratique juridique – ainsi qu'il ressort du pourvoi de l'avocat général – des questions concernant le lien existant entre les pouvoirs établis par le code de procédure pénale, évoqués aux points 5.1 et 5.2 ci-dessus, et le droit de l'Union. Le Hoge Raad (Cour suprême, Pays-Bas) examinera plusieurs de ces questions dans ce qui suit.

Le champ d'application de la directive 2002/58 et la jurisprudence de la Cour concernant cette directive

6.2.1 Conformément à son article 1er, paragraphe 1, la directive 2002/58 concerne « le traitement des données à caractère personnel dans le secteur des communications électroniques ». Cette directive s'applique lorsqu'un État membre adopte des mesures sur le traitement de ces données par des fournisseurs de services de communications électroniques et sur l'octroi de l'accès à ces données aux autorités publiques. À cet égard, la directive 2002/58 est pertinente pour l'exercice des pouvoirs légaux examinés aux points 5.1 et 5.2 ci-dessus. Les mesures dérogeant à la confidentialité des communications électroniques sans que soient pour autant imposées des obligations de traitement aux fournisseurs de services de communications électroniques ne relèvent toutefois pas de la directive 2002/58 [14]. Le Hoge Raad (Cour suprême, Pays-Bas) en déduit que, par exemple, l'enquête concernant des appareils téléphoniques saisis ne relèvent pas de la directive 2002/58.

[14] Arrêt 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 : « En revanche, 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 (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), de telle sorte que les mesures en cause doivent respecter notamment le droit national de rang constitutionnel et les exigences de la CEDH. »

6.2.2 Dans la jurisprudence de la Cour citée aux points 5.7 et 5.8, la question de la signification de l'article 15, paragraphe 1, de la directive 2002/58 ainsi que du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et de la liberté d'expression et d'information consacrés par la Charte est au cœur de l'appréciation de la possibilité de conserver et de (faire) communiquer les données relatives au trafic et les données de localisation [15]. L'article 15, paragraphe 1, de la directive 2002/58 concerne les mesures législatives que les États membres peuvent adopter pour conserver des données pendant une durée limitée aux fins, notamment, de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales.

6.2.3 Pour ce qui nous intéresse ici, le code de procédure pénale ne confère que des pouvoirs permettant de demander des données relatives au trafic, des données de localisation et des données d'identification. Compte tenu de la décision du juge, évoquée au point 5.5, d'écarter un certain nombre de dispositions du *Telecommunicatiewet* (loi relative aux télécommunications), il n'existe pas d'obligation légale générale de conservation de ces données. Les pouvoirs établis par le code de procédure pénale s'appliquent donc à des données qui sont conservées par les fournisseurs d'un service de communication sur un autre fondement (par exemple, contractuel).

Compte tenu de cette décision du juge d'écarter un certain nombre de dispositions du *Telecommunicatiewet* (loi relative aux télécommunications), il importe, pour la situation néerlandaise, de savoir si les considérations énoncées par la Cour dans la jurisprudence citée aux points 5.7 et 5.8, en ce qu'elles visent les données relatives au trafic et les données de la localisation (y compris les données d'identification), ne concernent que des données qui sont conservées sur le fondement de dispositions légales adoptées par un État membre au titre de l'article 15, paragraphe 1, de la directive 2002/58, ou si elles concernent également des données qui sont conservées sur un autre fondement (par exemple, contractuel).

6.2.4 Le Hoge Raad considère, pour les raisons exposées ci-dessous, qu'il convient de répondre à cette question en ce sens que les considérations énoncées par la Cour dans la jurisprudence citée aux points 5.7 et 5.8 concernent également la mise à disposition, dans le cadre d'une enquête pénale, des données visées au point 6.2.3 qui sont conservées sur un autre fondement que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58.

Tout d'abord, il importe de souligner que la directive 2002/58 vise à assurer la protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère

[15] Articles 7, 8 et 11 de la Charte.

personnel dans le secteur des communications électroniques [16]. Cet objectif est pertinent, qu'il s'agisse des données conservées sur le fondement de mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 ou des données conservées sur un autre fondement.

L'article 5 de la directive 2002/58 vise en outre à garantir que ce que ne peut faire toute personne autre que les utilisateurs que si cela est autorisé par la loi au titre de l'article 15, paragraphe 1, de la directive 2002/58, c'est non seulement écouter, intercepter et stocker les communications et les données relatives au trafic y afférentes, mais également « les soumettre à tout autre moyen d'interception ou de surveillance ». Cela pointe en ce sens que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 visent (peuvent viser) non seulement la conservation des données relatives au trafic, mais également l'obtention de l'accès à ces données. Il en découle qu'il convient d'interpréter la réglementation établie par le code de procédure pénale sur les pouvoirs permettant d'obtenir des données relatives au trafic aux fins de la détection et de la poursuite des infractions pénales comme étant une mesure législative au sens de l'article 15, paragraphe 1, de la directive 2002/58. La lecture combinée des articles 9 et 15, paragraphe 1, de la directive 2002/58 fait apparaître que cette conclusion s'applique également aux données de localisation [17].

Par ailleurs, il ressort des termes des arrêts de la Cour que la réponse à la question des conditions auxquelles peut être accordé l'accès aux données relatives au trafic et aux données de localisation conservées ne dépend pas « de l'étendue de l'obligation de conservation de données qui serait imposée aux fournisseurs de services de communications électroniques » [18]. Dans cette jurisprudence, ces conditions ne sont pas exclusivement liées aux données conservées sur le fondement de mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 [19]. Elles concernent

16 Voir article 1, paragraphe 1, de la directive 2002/58.

17 Voir également arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 78, dans lequel la Cour considère qu'« une mesure législative par laquelle un État membre impose, sur le fondement de l'article 15, paragraphe 1, de la directive 2002/58, aux fournisseurs de services de communications électroniques, aux fins mentionnées par cette disposition, d'accorder aux autorités nationales, dans les conditions prévues par une telle mesure, l'accès aux données conservées par lesdits fournisseurs » relève également du champ d'application de la directive 2002/58. Cette considération est reprise dans une jurisprudence ultérieure, certes dans des termes quelque peu différents qui peuvent éventuellement contredire la formulation précitée. Voir arrêts du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 35, et 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 96, ainsi que, en relation avec cela, le point 60 du pourvoi de l'avocat général.

18 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 113.

également des données conservées par un fournisseur au titre des articles 5, 6 et 9 de la directive 2002/58 [20].

6.2.5 Compte tenu de ce qui précède, le Hoge Raad (Cour suprême, Pays-Bas) part du principe que la jurisprudence de la Cour, en ce qu'elle concerne l'octroi de l'accès aux données relatives au trafic et aux données de localisation (y compris les données d'identification), vise non seulement les données qui sont conservées sur le fondement de mesures législatives adoptées par un État membre au titre de l'article 15, paragraphe 1, de la directive 2002/58, mais également les données évoquées au point 6.2.3, qui sont conservées sur un autre fondement que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58. Le Hoge Raad (Cour suprême, Pays-Bas) estime toutefois qu'il y a lieu de poser une question préjudicielle à la Cour. En effet, la jurisprudence de la Cour ne contient pas de réponse explicite à la question visée au point 6.2.3 et – ainsi qu'il ressort du point 61 du pourvoi de l'avocat général – il est possible de tirer du droit de l'Union des arguments plaidant en faveur d'une réponse contraire à celle figurant au point 6.2.4.

Les conditions de l'octroi d'un accès aux autorités publiques

6.3.1 Dans la jurisprudence citée aux points 5.7 et 5.8, la Cour a notamment élaboré les conditions applicables i) à la conservation des données relatives au trafic et des données de localisation et ii) à l'octroi aux autorités publiques d'un accès aux données relatives au trafic et aux données de localisation conservées. En développant ces conditions, la Cour a précisé, en particulier, les circonstances dans lesquelles et les garanties moyennant lesquelles la conservation des données relatives au trafic et des données de localisation ainsi que la mise à disposition de ces données sont compatibles avec le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et la liberté d'expression et d'information consacrés par la Charte, eu égard également au principe de proportionnalité [21].

6.3.2 Compte tenu des considérations figurant au point 5.5 concernant l'absence d'obligation générale de conservation, le droit néerlandais ne connaît pas de mesure législative au sens de l'article 15, paragraphe 1, de la directive 2002/58, à l'exception de ce qui sera indiqué aux points 6.3.3 et 6.3.4 ci-après. Le principe formulé au point 6.2.5 implique toutefois qu'en cas d'exercice des pouvoirs établis par le code de procédure pénale, évoqués

19 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 125 ; arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 45.

20 Arrêt 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 167.

21 Articles 7, 8 et 11 de la Charte.

aux points 5.1 et 5.2, il convient de satisfaire aux conditions énoncées par la Cour en ce qui concerne l'octroi aux autorités publiques d'un accès aux données relatives au trafic et aux données de localisation conservées.

6.3.3 Le fait qu'il n'existe pas d'obligation légale et générale de conservation en droit néerlandais n'empêche pas que des obligations de conservation spécifiques et limitées puissent être établies. Ainsi, le régime de l'article 126ni du code procédure pénale (voir, également, articles 126ui et 126zja du code de procédure pénale) permet, dans certaines circonstances, d'adresser à un fournisseur d'un service de télécommunication une demande tendant à la conservation et à la mise à disposition de certaines données concernant un utilisateur pendant une période de 90 jours. En outre, une demande de communication de données relatives au trafic et de données de localisation peut également viser des données « qui seront traitées après la date de la demande » [article 126n, paragraphe 1, phrase liminaire et sous b), du code de procédure pénale ; voir, également, article 126u, paragraphe 1, et article 126zh, paragraphe 1, du code de procédure pénale]. Il s'agit alors de la communication des données futures qui seront traitées par le fournisseur d'un service de communication, après la date de la demande, dans le cadre de ses activités commerciales. Ce pouvoir vise à éviter que ces données traitées soient perdues ou modifiées et à ce qu'elles soient communiquées au procureur telles qu'enregistrées et non modifiées.

À cet égard, nous pouvons nous référer aux considérations énoncées par la Cour dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) concernant la conservation dite « rapide » :

« 160 En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161 Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162 À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – nº 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163 Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

164 Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, *a fortiori*, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

165 À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées

d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée).

166 Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, *a fortiori*, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

167 À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58. »

6.3.4 En substance, les considérations précitées concernent la conservation rapide de données qui sont déjà conservées par le fournisseur de services de

communications électroniques mais qui, sans cette conservation rapide, risqueraient d'être perdues et, par conséquent, de ne plus pouvoir être mises à disposition. Ce pouvoir de demander la conservation rapide est établi à l'article 126ni du code de procédure pénale. Les considérations précitées semblent également viser le pouvoir de demander la communication de données relatives au trafic futures et de données de localisation futures lorsqu'il n'est pas certain que les données concernées resteront conservées dans le cadre de l'exercice normal des activités commerciales du fournisseur de services de communications. Il en résulte que lorsque le pouvoir de demander la communication de ces données futures est exercé, il convient également de respecter les conditions établies par la Cour en ce qui concerne la conservation rapide et l'octroi de l'accès aux données ainsi conservées.

6.4.1 S'agissant des conditions de l'octroi aux autorités publiques d'un accès aux données conservées par des fournisseurs de services de communications électroniques, l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) énonce notamment que :

« 115 S'agissant des objectifs susceptibles de justifier une réglementation nationale dérogeant au principe de confidentialité des communications électroniques, il convient de rappeler que, dans la mesure où, ainsi qu'il a été constaté aux points 90 et 102 du présent arrêt, l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, l'accès aux données conservées doit répondre effectivement et strictement à l'un de ces objectifs. En outre, dès lors que l'objectif poursuivi par cette réglementation doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, il s'ensuit que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données conservées.

116 En ce qui concerne le respect du principe de proportionnalité, une réglementation nationale régissant les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données conservées doit assurer, conformément à ce qui a été constaté aux points 95 et 96 du présent arrêt, qu'un tel accès n'ait lieu que dans les limites du strict nécessaire.

(...)

119 Ainsi, et dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire, la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des

abonnés ou des utilisateurs inscrits. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction (voir, par analogie, Cour EDH, 4 décembre 2015, Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, § 260). Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités.

120 Aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, 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 (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 62 ; voir également, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:ECHR:2016:0112JUD003713814, §§ 77 et 80).

121 De même, il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits (voir, par analogie, arrêts du 7 mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, point 52, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 95).

(...)

124 Il appartient aux juridictions de renvoi de vérifier si et dans quelle mesure les réglementations nationales en cause au principal respectent les exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, telles qu'explicitées aux points 115 à 123 du présent arrêt, en ce

qui concerne tant l'accès des autorités nationales compétentes aux données conservées que la protection et le niveau de sécurité de ces données.

125 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question dans l'affaire C-203/15 et à la première question dans l'affaire C-698/15 que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union. »

6.4.2 Cet arrêt définit les données auxquelles les autorités publiques peuvent accéder en se fondant sur le critère du cercle des personnes concernées par ces données. Cette jurisprudence implique essentiellement que, en relation avec l'objectif de lutte contre la criminalité, un accès aux données conservées par les fournisseurs de services de communications électroniques ne saurait, en principe, être accordé aux autorités publiques que s'il s'agit de données de personnes soupçonnées « de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction ». À titre de conditions supplémentaires, l'accès – sauf dans les cas urgents – doit être accordé après « un contrôle préalable effectué par une juridiction ou une entité administrative indépendante », et les personnes concernées, à moins que l'intérêt de l'enquête ne s'y oppose, doivent être informées de l'accès qui a été accordé à ces données.

Selon cette jurisprudence, l'accès à des données de personnes autres que celles qui sont soupçonnées « de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction » ne peut être accordé, en relation avec l'objectif de lutte contre la criminalité, que dans des situations particulières. Ces situations concernent notamment – en résumé – les activités terroristes. L'octroi de l'accès aux données doit alors apporter une contribution effective à la lutte contre de telles activités.

Nous examinons au point 6.10 ci-dessous la question de savoir si l'accès aux données doit toujours être lié à un soupçon concret à l'égard d'une personne déterminée.

6.4.3 Dans l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), la Cour examine, en résumé, les possibilités d'accorder

aux autorités publiques l'accès à des données conservées par des fournisseurs de services de communications électroniques, y compris les données d'identification. Cette jurisprudence énonce notamment que :

« 50 En particulier, cette juridiction s'interroge sur les éléments à prendre en compte afin d'apprécier si les infractions au regard desquelles des autorités policières peuvent être autorisées, à des fins d'enquête, à accéder à des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, sont d'une gravité suffisante pour justifier l'ingérence que comporte un tel accès dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, tels qu'interprétés par la Cour dans ses arrêts du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238), et Tele2 Sverige et Watson e.a.

51 Quant à l'existence d'une ingérence dans ces droits fondamentaux, il y a lieu de rappeler que […] l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de "grave" et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée].

52 En ce qui concerne les objectifs susceptibles de justifier une réglementation nationale, telle que celle en cause au principal, régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, il convient de rappeler que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., points 90 et 115).

53 Or, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, il y a lieu d'observer que le libellé de l'article 15, paragraphe 1, première phrase, de la directive 2002/58 ne limite pas cet objectif à la lutte contre les seules infractions graves, mais vise les "infractions pénales" en général.

54 À cet égard, la Cour a, certes, jugé que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte

contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 99).

55 La Cour a toutefois motivé cette interprétation par le fait que l'objectif poursuivi par une réglementation régissant cet accès doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux en cause que cette opération entraîne (voir, en ce sens, arrêt Tele2 Sverige et Watson e.a., point 115).

56 En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de "grave".

57 En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales" en général.

58 Il convient donc, avant tout, de déterminer si, en l'occurrence, en fonction des circonstances de l'espèce, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire aux données en cause au principal comporterait doit être considérée comme étant "grave".

59 À cet égard, la demande en cause au principal par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. Ainsi qu'il a été relevé au point 40 du présent arrêt, cette demande vise l'accès aux seuls numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche, ces données ne portent pas, comme l'ont confirmé tant le gouvernement espagnol que le ministère public lors de l'audience, sur les communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.

60 Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées

avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.

61 Dans ces conditions, l'accès aux seules données visées par la demande en cause au principal ne saurait être qualifié d'ingérence "grave" dans les droits fondamentaux des personnes dont les données sont concernées.

62 Ainsi qu'il ressort des points 53 à 57 du présent arrêt, l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales" en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58, sans qu'il soit nécessaire que ces infractions soient qualifiées de "graves".

63 Eu égard aux considérations qui précèdent, il convient de répondre aux questions posées que 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 que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. »

Se référant à cette jurisprudence, la Cour a notamment jugé, dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), que :

« 157 En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59 et 60).

158 Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 62). »

En outre, la Cour a considéré, dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), que :

« 33 En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause au principal, conformément au principe de proportionnalité, seule la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif, poursuivi par la réglementation en cause au principal, de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 140 ainsi que 146).

34 À cet égard, il a notamment été jugé que les mesures législatives visant le traitement des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques en tant que telles, notamment leur conservation et l'accès à celles-ci, à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58. En effet, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées des utilisateurs des moyens de communications électroniques, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une mesure visant ces données ne saurait,

en principe, être qualifiée de grave (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 157 et 158 ainsi que jurisprudence citée).

35 Dans ces conditions, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 54), sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès. »

6.4.4 La Cour fait du principe de proportionnalité un élément central de cette jurisprudence. Lorsque des autorités publiques souhaitent obtenir l'accès, à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales, à des données conservées par des fournisseurs de services de communications électroniques, la gravité de l'ingérence dans les droits fondamentaux concernés joue un rôle important. Il s'agit en particulier de l'ingérence dans le droit au respect de la vie privée. La jurisprudence de la Cour énonce, en substance, qu'une ingérence grave ne saurait être justifiée que par l'objectif de lutte contre la « criminalité grave ». Si l'octroi de l'accès aux données n'implique pas une ingérence grave, cet accès peut être justifié par l'objectif de prévention, de recherche, de détection et de poursuite des infractions pénales en général, y compris les infractions pénales qui ne répondent pas à la qualification de « criminalité grave » [22].

Dans ce contexte, la Cour a considéré, dans la jurisprudence précitée, que l'accès aux seules données d'identification [23] pouvait être accordé à des fins de prévention, de recherche, de détection et de poursuite des infractions pénales, sans que soit exigé qu'il s'agisse exclusivement d'infractions pénales graves. En tout état de cause, ces données sont celles qui servent à identifier l'utilisateur concerné sans qu'elles puissent être associées à des

22 Voir, en particulier, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 56 et 57.

23 Bien que – s'agissant du trafic de communication par courriel et de la téléphonie internet – les adresses IP de la source de communication, et non du destinataire, ont un caractère moins sensible que les données relatives au trafic, ces adresses IP ne saurait être mises sur le même plan que les données d'identification. Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 152 à 156.

informations relatives aux communications effectuées [24]. En effet, ces données ne fournissent aucune information précise sur la vie privée de l'utilisateur. Par conséquent, l'octroi de l'accès à ces données n'implique pas d'ingérence grave dans, notamment, le droit à la protection de la vie privée. C'est également la raison pour laquelle la Cour n'a, pour ces seules données d'identification, pas imposé les conditions supplémentaires citées au point 6.4.2 du « contrôle préalable par une juridiction ou une autorité administrative indépendante » et de la notification aux personnes concernées.

6.4.5 Il convient, dans toute la mesure du possible, d'interpréter conformément à la directive 2002/58 les dispositions de code de procédure pénale concernant la demande des données relatives au trafic et des données de localisation, ainsi que des données d'identification, en se fondant sur l'interprétation que la Cour a donnée aux dispositions de cette directive. S'agissant des pouvoirs qui concernent exclusivement la demande des seules données d'identification, il découle de ce qui précède que la directive 2002/58 n'impose pas de conditions supplémentaires. S'agissant des pouvoirs légaux qui concernent la demande des données relatives au trafic et des données de localisation, autre que les seules données d'identification [25], il convient de prendre en considération – compte tenu du principe de proportionnalité – la gravité de l'ingérence dans (notamment) le droit au respect de la vie privée. Si l'exercice de ces pouvoirs implique une ingérence grave, il est exigé qu'il soit question de « criminalité grave » (et donc d'infractions pénales graves) et que ces pouvoirs soient exercés après un « contrôle préalable par une juridiction ou une autorité administrative indépendante ».

La jurisprudence de la Cour à cet égard, et les notions qui y sont utilisées, soulèvent des questions concernant i) la gravité de l'ingérence dans (notamment) le droit à la protection de la privée qu'implique ou que peut impliquer l'octroi aux autorités publiques d'un accès aux données relatives au trafic ou aux données de localisation (autres que les seules données d'identification), et ii) la définition des notions d'« infractions pénales graves » et de « criminalité grave ». Ces questions sont examinées aux points 6.5 à 6.9 ci-dessous. Nous aborderons ensuite, au point 6.10, la définition du cercle des personnes visées par les données auxquelles l'accès peut être accordé.

24 Voir, notamment, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 34.

25 La demande de données au titre des articles 126n, 126u et 126zh du code de procédure pénale concerne les données relatives au trafic et les données de localisation, mais elle pourrait également se limiter aux données d'identification dans un cas concret. En effet, ainsi qu'il ressort de l'article 2 de l'arrêté relatif à la demande de données de télécommunication, les données visées par les articles 126n, 126u et 126zh du code de procédure pénale comprennent également les données mentionnées aux articles 126na, 126ua et 126zi du code de procédure pénale.

Conclusions précises sur la vie privée ; infractions pénales graves et criminalité grave

6.5.1 Ainsi que nous l'avons indiqué au point 6.4.5, on peut déduire de la jurisprudence de la Cour que, si l'exercice des pouvoirs légaux concernant les données relatives au trafic et les données de localisation implique une ingérence grave dans, notamment, le droit à la protection de la vie privée, cette ingérence ne peut se justifier, compte tenu du principe de proportionnalité, que s'il est question de criminalité grave (et donc d'infractions pénales graves). Dans son pourvoi, l'avocat général soulève la question, importante pour la pratique juridique, de savoir si, au vu de la jurisprudence de la Cour, les autorités publiques peuvent également se voir accorder l'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) en l'absence d'infractions pénales graves ou de criminalité grave, lorsqu'il s'agit, comme l'espèce, de données relatives au trafic et de données de localisation qui ne devraient, vraisemblablement, impliquer qu'une ingérence limitée dans le droit à la protection de la vie privée. Dans son pourvoi, l'avocat général se réfère en particulier à la jurisprudence de la Cour dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152). La Cour a répondu de la manière suivante à la première question préjudicielle posée dans cette affaire :

« 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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période. »

6.5.2 Aux points 97 à 110 de son pourvoi, l'avocat général examine la manière dont la jurisprudence de la Cour concernant la question précitée peut être

interprétée. Il précise que cette jurisprudence n'est pas univoque, en ce sens qu'elle peut se prêter à plusieurs lectures. La première lecture consiste à considérer que les autorités publiques ne peuvent se voir accorder l'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) qu'en cas d'infractions pénales graves ou de criminalité grave [26]. Selon la deuxième lecture, l'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) peut également être accordé en cas d'infractions pénales moins graves ou de criminalité moins grave, si cet accès aux données n'implique qu'une ingérence limitée dans, notamment, le droit à la protection de la vie privée de l'utilisateur.

6.5.3 Le Hoge Raad (Cour suprême, Pays-Bas) estime que les considérations relatives au principe de proportionnalité exposées dans la jurisprudence de la Cour appuient la deuxième lecture précitée. Ainsi que nous l'avons indiqué au point 6.4.4, sur le fondement du principe de proportionnalité, l'accès aux données conservées par un fournisseur d'un service de télécommunication accordé aux autorités publiques peut être justifié par l'objectif de prévention, de recherche, de détection et de poursuite des infractions pénales en général, si l'octroi de cet accès n'implique pas concrètement une ingérence, ou une ingérence grave, dans, notamment, le droit à la protection de la vie privée [27]. Dans ce cas, le principe de proportionnalité ne s'oppose pas à ce que l'accès soit accordé dans le cas d'une infraction pénale en général, sans que cette infraction doive être qualifiée de « grave » au sens susvisé.

Si l'accès des autorités publiques à des données relatives au trafic ou à des données de localisation implique une ingérence grave dans (notamment) le droit à la protection de la vie privée, parce que ces données sont susceptibles de fournir des informations sur les communications effectuées par un utilisateur ou sur la localisation des équipements qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, cette ingérence ne peut être justifiée que par l'objectif de lutte contre la criminalité grave. Le seul fait que l'accès soit accordé à une quantité limitée de données ou qu'il soit accordé pour une période limitée pendant laquelle les données sont enregistrées n'a aucune incidence. Le critère déterminant est la gravité de

[26] Soit parce qu'il convient de considérer que toute consultation de ces données relatives au trafic et de ces données de localisation emporte une ingérence grave dans, notamment, le droit à la protection de la vie privée de l'utilisateur, soit parce que, aux fins de l'octroi de l'accès à ces données relatives au trafic et à ces données de localisation, le fait qu'il s'agisse concrètement de données permettant de tirer des conclusions précises concernant la vie privée de l'utilisateur n'a aucune incidence.

[27] Parce qu'il s'agit d'un cas dans lequel les données reçues ne permettent d'obtenir aucune information sur la vie privée d'une personne spécifique, ou seulement dans une mesure limitée. On peut citer comme exemple la situation dans laquelle il n'y pas encore concrètement de suspect et où la demande d'accès aux données se limite à la question de savoir quel appareil de télécommunication a établi une connexion avec un pylône de transmission en un certain lieu et pendant une certaine période.

l'ingérence dans, notamment, le droit à la protection de la vie privée. À cet égard, le Hoge Raad (Cour suprême, Pays-Bas) se réfère à nouveau à la considération suivante exposée par la Cour dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152) :

> « 35 Dans ces conditions, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 54), sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès. »

6.6.1 Une question qui se pose par rapport à la jurisprudence de la Cour est celle des notions d'« infraction pénale grave » et de « criminalité grave ». La jurisprudence de la Cour citée aux points 5.7 et 5.8 ne contient aucune précision quant à ces notions. La question se pose de savoir s'il appartient aux autorités compétentes des États membres de préciser elles-mêmes ces notions ou s'il s'agit de notions autonomes du droit de l'Union.

6.6.2 À cet égard, il convient d'abord d'observer que la directive 2002/58 mentionne uniquement, en son article 15, paragraphe 1, « la prévention, la recherche, la détection et la poursuite d'infractions pénales » sans préciser davantage la notion d'« infractions pénales ». Les notions d'« infractions pénales graves » et de « criminalité grave », citées dans la jurisprudence de la Cour, ne se retrouvent pas dans la directive 2002/58. À l'examen de la directive 2002/58 – et en particulier de son article 1er – il ne semble pas qu'elle tendait à l'harmonisation des notions d'« infractions pénales », d'« infractions pénales graves » et de « criminalité grave ». À cet égard, la directive 2002/58 diffère, par exemple, de la décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO 2002, L 190, p. 1). Cette décision-cadre contient une description spécifique des infractions pénales pouvant donner lieu à une remise sans contrôle de la double incrimination du fait.

La jurisprudence de la Cour concernant l'octroi de l'accès aux données relatives au trafic et aux données de localisation, citée au point 6.4.1, est également importante. Dans cette jurisprudence, la Cour considère qu'il

appartient aux juridictions de renvoi de vérifier si et dans quelle mesure les réglementations nationales concernant, notamment, l'accès aux données conservées par les autorités nationales compétentes respectent les exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58 [28]. Il s'ensuit que c'est aux autorités concernées des États membres qu'il appartient de déterminer s'il est question d'« infractions pénales graves » et de « criminalité grave ». La jurisprudence de la Cour ne contient aucun angle de vue ou critère qui puisse être considéré comme pertinent pour répondre concrètement à la question de savoir s'il est question d'infraction pénale grave ou de criminalité grave [29].

6.6.3 Selon le Hoge Raad (Cour suprême, Pays-Bas), il convient donc de considérer que, dans la jurisprudence de la Cour, les notions d'« infractions pénales graves » et de « criminalité grave » ne sont pas des notions autonomes du droit de l'Union [30]. On peut cependant déduire de cette jurisprudence que les autorités nationales qui exercent les pouvoirs d'accéder aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) doivent s'assurer que cet exercice est concrètement compatible avec le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et la liberté d'expression et d'information consacrés par la Charte. Ainsi que nous l'avons énoncé ci-dessus, il s'ensuit que l'ingérence dans les droits garantis par la Charte doit être justifiée concrètement par la gravité de l'infraction pénale (présumée) qui donne lieu à l'exercice du pouvoir. À cet égard, le premier élément à prendre en considération est la gravité de l'infraction pénale en général, telle qu'elle ressort notamment de la peine maximale prévue par la loi. Est en outre également pertinente la gravité de l'infraction pénale (présumée) telle qu'elle s'est produite concrètement. Cette gravité doit être proportionnée à l'ingérence dans, notamment, le droit à la protection de la vie privée.

6.7 Ainsi que nous l'avons indiqué au point 6.5.2, la jurisprudence de la Cour autorise plusieurs lectures quant à la question de savoir si l'accès aux données relatives au trafic et aux données de localisation peut également être accordé, dans certaines circonstances, lorsque la criminalité ne présente pas un caractère grave. En outre, la jurisprudence de la Cour, ainsi que nous l'avons relevé au point 6.6.3, n'a pas confirmé à ce jour qu'il appartenait aux

28 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 124.

29 Comparer, sur les critères d'appréciation possibles, conclusions de l'avocat général Saugmandsgaard Øe dans l'affaire Ministerio Fiscal (C-207/16, EU:C:2018:300, point 105).

30 Dans ce sens, voir également conclusions de l'avocat général Saugmandsgaard Øe dans l'affaire Ministerio Fiscal (C-207/16, EU:C:2018:300, point 100) et conclusions de l'avocat général Pitruzzella dans l'affaire Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2020:18, point 91).

autorités nationales compétentes de préciser elles-mêmes les notions d'« infractions pénales graves » et de « criminalité grave ». Partant, il y a lieu de poser des questions préjudicielles à la Cour afin de clarifier la jurisprudence abordée aux points 6.5 et 6.6. À cet égard, nous observons ce qui suit sur l'importance de poser ces questions préjudicielles aux fins de l'application du droit national.

6.8.1 Pour l'exercice des pouvoirs permettant de demander les données relatives au trafic et les données de localisation établis par le code de procédure pénale, la seule existence d'un soupçon d'infraction ne suffit pas, sauf en ce qui concerne la demande des données d'identification sur le fondement des articles 126na, 126ua et 126zi du même code. Il est notamment exigé, pour l'exercice de ces pouvoirs, que le soupçon concerne une infraction visée à l'article 67, paragraphe 1, du code de procédure pénale, ou que l'on puisse raisonnablement présumer que des infractions visées à l'article 67, paragraphe 1, du code de procédure pénale sont planifiées ou commises en bande organisée, lorsque ces infractions, compte tenu de leur nature ou de leur connexité avec d'autres infractions pénales planifiées ou commises dans le cadre de cette bande organisée, constituent une atteinte grave à l'ordre juridique, ou encore qu'il y ait des indices d'une infraction terroriste. À cet égard, l'infraction ou les infractions visées à l'article 67, paragraphe 1, du code de procédure pénale sont celles qui sont énumérées dans cette disposition. Cette liste recense d'abord les infractions passibles d'un emprisonnement de quatre ans ou plus, puis une série d'infractions spécifiques établies par le code de procédure pénale et des législations particulières. Il s'ensuit que les pouvoirs susvisés peuvent s'exercer non pas à l'égard de toute infraction, mais uniquement à l'égard des infractions que le législateur a reprises dans la liste de l'article 67, paragraphe 1, du code de procédure pénale en raison de leur nature et de leur gravité et qu'il convient donc – selon le Hoge Raad – de considérer de manière générale comme des infractions « graves » au sens de la jurisprudence de la Cour. En outre, ainsi que nous l'exposerons plus en détail au point 6.8.3, la gravité de l'infraction pénale concrète présente également une importance.

6.8.2 S'agissant de la conservation rapide évoquée aux points 6.3.3 et 6.3.4, il convient d'observer que, sur le fondement des articles 126ni, 126ui et 126zja du code de procédure pénale, il est exigé qu'il soit question d'un soupçon d'infraction visée à l'article 67, paragraphe 1, du code de procédure pénale qui, compte tenu de sa nature ou de sa connexité avec d'autres infractions pénales commises par le suspect, constitue une atteinte grave à l'ordre juridique, ou que l'on puisse raisonnablement présumer que des infractions visées à l'article 67, paragraphe 1, du code de procédure pénale sont planifiées ou commises en bande organisée, lorsque ces infractions, compte tenu de leur nature ou de leur connexité avec d'autres infractions pénales planifiées ou commises dans le cadre de cette bande organisée, constituent une atteinte grave à l'ordre juridique, ou encore qu'il y ait des indices d'une infraction terroriste. S'agissant du pouvoir de demander la communication

de données futures, les exigences exposées au point 6.8.1 sont applicables. Par conséquent, s'agissant également de la conservation rapide évoquée aux points 6.3.3 et 6.3.4, les pouvoirs concernés ne peuvent s'exercer qu'à l'égard des infractions que le législateur a inscrites dans la liste de l'article 67, paragraphe 1, du code de procédure pénale en raison de leur nature et de leur gravité.

6.8.3 Lors de l'exercice des pouvoirs susvisés tendant, dans le cadre d'une enquête pénale, à obtenir l'accès aux données relatives au trafic et aux données de localisation, il convient de respecter, en particulier, l'exigence générale de proportionnalité applicable à la procédure pénale. Cette exigence implique que l'infraction pénale concrète, à l'égard de laquelle il existe une présomption raisonnable ou des indices, doit être suffisamment grave pour justifier l'exercice du pouvoir de demander les données relatives au trafic et les données de localisation. La personne qui décide d'exercer ce pouvoir doit préalablement procéder à cette appréciation. Dans le cadre de cette appréciation, il convient donc d'évaluer la mesure dans laquelle l'obtention des données relatives au trafic et des données de localisation porte (éventuellement) atteinte à la vie privée de l'utilisateur, ainsi que le rapport de proportionnalité entre cette atteinte et la gravité de l'infraction pénale telle qu'elle s'est produite concrètement.

Le Hoge Raad (Cour suprême, Pays-Bas) souligne à cet égard qu'une ligne de démarcation peut certes être tracée, sur le plan abstrait, entre les infractions pénales graves et les infractions pénales qui ne présentent pas un caractère grave, mais que la gravité de l'infraction pénale concrète peut varier considérablement. En outre, lorsqu'une demande de communication d'un certain type de données est adressée, il n'est pas toujours possible de savoir exactement si des données seront obtenues ni, le cas échéant, quelles données seront obtenues, ni encore de connaître le contenu de ces données et les personnes qui sont concernées par ces données en dehors de l'utilisateur. Par conséquent, l'appréciation visant à déterminer si l'exercice d'un pouvoir permettant d'obtenir des données relatives au trafic et des données de localisation est conforme au droit à la protection de la vie privée consiste également à évaluer puis à pondérer un ensemble de facteurs [31]. Parmi ces facteurs figurent la gravité de l'infraction pénale en général, la gravité de l'infraction pénale concrète sur laquelle porte le soupçon, les données qui – en fonction de la formulation et de la délimitation de la demande – seront (pourront être) vraisemblablement obtenues concernant l'utilisateur et, éventuellement, d'autres personnes, la pertinence de l'obtention de ces données aux fins de l'enquête pénale et la question de savoir si et dans quelle mesure ces données permettent de tirer des conclusions sur la vie privée. En un certain sens, il s'agit d'une échelle variable : plus la violation

31 Comparer arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 40.

(attendue) du droit à la protection de la vie privée de l'utilisateur est importante, plus les exigences susceptibles d'être imposées quant à la gravité de l'infraction pénale concrète seront strictes. D'autres facteurs jouent également un rôle. Il s'agit des garanties légales que les données obtenues ne seront pas utilisées à des fins autres que l'enquête pénale et des règles relatives à la conservation et à la destruction des données obtenues.

6.9 Compte tenu de ce qui précède, un exercice correct des pouvoirs établis par le code de procédure pénale garantit la conformité du résultat de cet exercice à la directive 2002/58 et au principe de proportionnalité. À cet égard, le Hoge Raad (Cour suprême, Pays-Bas) part du principe que la jurisprudence de la Cour peut être interprétée de la manière décrite aux points 6.5.3 et 6.6.3 ci-dessus. Le renvoi de questions préjudicielles à la Cour vise à obtenir la certitude sur ce point au profit de la pratique juridique.

Ainsi que nous l'avons énoncé au point 6.6.1, la jurisprudence de la Cour n'a pas encore confirmé qu'il appartenait aux autorités nationales compétentes de préciser les notions d'« infractions pénales graves » et de « criminalité grave ». S'il s'avère, contrairement à ce qu'a estimé le Hoge Raad (Cour suprême, Pays-Bas) au point 6.6.3, qu'il s'agit de notions autonomes du droit de l'Union, il importe de savoir comment interpréter ces notions pour pouvoir déterminer si et, le cas échéant, comment les pouvoirs établis par le code de procédure pénale peuvent être exercés conformément à la directive 2002/58. Il importe en outre de clarifier la question, soulevée au point 6.5, de savoir si l'octroi de l'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) se limite ou non aux cas de criminalité grave. Cette question est également liée à la pertinence et à la signification du principe de proportionnalité lorsqu'il s'agit d'identifier la manière de réguler l'accès aux données conservées par les fournisseurs de services de communications électroniques.

Le cercle de personnes

6.10.1 Ainsi que nous l'avons indiqué au point 6.4.2, dans l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), la Cour a considéré qu'il y avait lieu de se fonder sur des critères objectifs pour déterminer si les autorités publiques pouvaient se voir accorder l'accès aux données conservées par des fournisseurs de services de communications électroniques. À cet égard, « un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction ». L'accès aux données d'autres personnes pourrait être accordé « dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par

des activités de terrorisme […] lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités » [32].

6.10.2 À première vue, cette jurisprudence de la Cour peut soulever la question de savoir si – en dehors des situations particulières mentionnées par la Cour – l'accès aux données, y compris les données relatives au trafic et les données de localisation, ne peut être accordé aux autorités publiques que si ces données concernent, en somme, une personne à l'égard de laquelle il existe un soupçon. L'application d'un tel critère peut entraver de manière considérable la recherche, la détection et la poursuite des infractions pénales [33]. Selon ce critère, les autorités publiques ne pourraient demander les données relatives au trafic et les données de localisation que lorsqu'elles tentent d'identifier l'auteur (présumé) de l'infraction pénale ou qu'elles essaient de comprendre le mode de perpétration de l'infraction pénale. Les informations concernant les numéros de téléphone utilisés, les numéros d'identification des appareils téléphoniques, les pylônes de transmission avec lesquels les appareils ont établi une connexion ou les adresses IP liées aux formes électroniques de communication peuvent constituer des points de départ importants pour l'enquête pénale. Une détection efficace exige de pouvoir obtenir des données qui ne sont pas (encore) liées à des personnes spécifiques et qui, souvent aussi, ne permettent pas d'obtenir des informations sur la vie privée des personnes, ou seulement dans une mesure très limitée. Pour obtenir ces données, la police et la justice se fondent sur l'exercice des pouvoirs de demander les données relatives au trafic et les données de localisation dans les cas également où le soupçon d'infraction pénale ne vise pas encore concrètement une personne spécifique.

6.10.3 Pour les raisons exposées ci-dessous, il convient de partir du principe que l'exercice des pouvoirs de demander les données relatives au trafic et les données de localisation – y compris en dehors des exceptions mentionnées au point 6.10.1 – ne doit pas toujours se limiter à des personnes spécifiques pouvant être considérées comme des suspects.

Tout d'abord, il importe d'observer que, dans son arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), la Cour se réfère à l'arrêt de la Cour EDH du 4 décembre 2015, Roman Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306). Cette affaire porte sur une plainte concernant, en résumé, la possibilité d'intercepter le trafic de téléphonie mobile (« l'interception secrète des communications de téléphonie mobile »). Dans cet arrêt, la Cour EDH

32 Point 119.

33 À cet égard, les obligations dites « positives » peuvent également être pertinentes. Comparer notamment arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 126 à 128.

expose les « principes généraux » relatifs à l'admissibilité des « mesures de surveillance secrète ». Le point 260 de cet arrêt de la Cour EDH, auquel se réfère la Cour, énonce que :

« Pour ce qui est de la portée de l'examen effectué par le service délivrant l'autorisation, la Cour rappelle que celui-ci doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale. Il doit également s'assurer que l'interception requise satisfait au critère de "nécessité dans une société démocratique" prévu à l'article 8 § 2 de la Convention, notamment qu'elle est proportionnée aux buts légitimes poursuivis, en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs (Klass et autres, précité, § 51, Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev, précité, §§ 79-80, Iordachi et autres, précité, § 51, et Kennedy, précité, §§ 31-32). »

En soi, l'octroi de l'accès aux données relatives au trafic et aux données de localisation n'est pas une interception de télécommunications. Il convient manifestement de déduire de cette considération de la Cour EDH que si l'application de techniques d'enquête permettant l'obtention secrète d'informations liées au trafic des télécommunications vise une personne spécifique, il ressort de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme que cette personne doit faire l'objet d'un soupçon et que ce soupçon doit concerner une infraction pénale d'une gravité et d'une nature telles qu'elles justifient le recours à ces techniques d'enquête secrètes. Il convient à cet égard de respecter une exigence de proportionnalité. Eu égard au caractère nécessaire que doit avoir la violation de la vie privée dans une société démocratique, on peut également déduire de cette considération qu'il y a une exigence de subsidiarité, en ce sens que si les informations peuvent être obtenues par un procédé moins intrusif, il convient de choisir ce procédé. Cependant, on ne saurait déduire de cette considération de la Cour EDH que l'application des techniques d'enquête citées n'est autorisée que si le soupçon d'infraction pénale vise concrètement une personne spécifique. Il ne s'ensuit pas davantage que, si un suspect est concrètement visé, ces techniques d'enquête ne peuvent être utilisées que pour obtenir des données concernant ce suspect. Ainsi que nous l'avons observé au point 6.10.2, ces limitations réduiraient, en particulier, les possibilités d'enquêter et de poursuivre – et donc de protéger les citoyens contre – les formes graves de criminalité.

Il convient en outre de tenir compte de la jurisprudence de la Cour concernant la conservation des données par les fournisseurs de services de communications électroniques. En effet, il n'apparaît pas avec évidence que

certains types de données, telles que les données relatives au trafic et les données de localisation, pourraient (ou devraient) être conservées alors que l'accès à ces données ne serait pas (entièrement) autorisé. On peut déduire de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970) qu'une obligation de conservation est conforme à la directive 2002/58 lorsqu'elle est limitée à « des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité » [34]. S'agissant de la conservation rapide des données relatives au trafic et des données de localisation, il ressort de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) que la conservation rapide « ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale ». Dans le même arrêt, la Cour considère ensuite que la conservation rapide « peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause » [35]. L'accès aux données décrites ici peut également être accordé, dans le respect des conditions exposées ci-dessus [36].

6.10.4 Il découle de ce qui précède que l'octroi de l'accès aux autorités publiques, sur le fondement de la directive 2002/58, ne se limite pas aux données conservées par les fournisseurs de services de communications électroniques qui concernent, en bref, une personne à l'égard de laquelle il existe un soupçon. Il convient toutefois, à cet égard, de respecter les exigences de proportionnalité et de subsidiarité. Ainsi que nous l'avons observé au point 6.4.4, il s'ensuit que si l'octroi de l'accès emporte une ingérence grave dans le droit à la protection de la vie privée, cet accès n'est accordé qu'à des fins de lutte contre la criminalité grave. En outre, lorsqu'on décide

[34] Point 106. Voir également arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 147 à 150.

[35] Point 165.

[36] Points 166 et 167.

d'accorder cet accès, il convient d'apprécier s'il est possible d'obtenir les informations nécessaires selon une méthode moins intrusive.

Le contrôle préalable à l'exercice des pouvoirs établis par le code de procédure pénale

6.11.1 Ainsi que nous l'avons exposé au point 6.4.5, il ressort de la jurisprudence de la Cour que, dans l'état actuel des choses, – sauf cas d'urgence – l'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) ne peut, lorsque l'exercice des pouvoirs concernés emporte une ingérence grave dans le droit à la protection de la vie privée de l'utilisateur, être accordé qu'après « un contrôle préalable effectué par une juridiction ou une entité administrative indépendante ». Ce contrôle préalable n'est pas exigé lorsqu'il s'agit uniquement d'accorder l'accès à des données permettant d'identifier l'utilisateur concerné sans que les données puissent être associées à des informations relatives aux communications effectuées.

Dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), la Cour a examiné la question de savoir si le ministère public pouvait également procéder à ce contrôle préalable. Les considérations suivantes sont pertinentes :

> « 51 (...) [I]l 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. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais (voir, en ce sens, arrêt 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 189 ainsi que jurisprudence citée).
>
> 52 Ce contrôle préalable requiert entre autres, ainsi que l'a relevé, en substance, M. l'avocat général au point 105 de ses conclusions, que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et 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 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.

53 Lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure [voir, en ce sens, arrêt du 9 mars 2010, Commission/Allemagne, C-518/07, EU:C:2010:125, point 25, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 229 et 230].

54 Il résulte des considérations qui précèdent que l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable, rappelé au point 51 du présent arrêt, impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique, ainsi que l'a relevé M. l'avocat général en substance au point 126 de ses conclusions, que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale.

55 Tel n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. En effet, le ministère public a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale.

56 La circonstance que le ministère public soit, conformément aux règles régissant ses compétences et son statut, tenu de vérifier les éléments à charge et à décharge, de garantir la légalité de la procédure d'instruction et d'agir uniquement en vertu de la loi et de sa conviction ne saurait suffire à lui conférer le statut de tiers par rapport aux intérêts en cause au sens décrit au point 52 du présent arrêt.

57 Il s'ensuit que le ministère public n'est pas en mesure d'effectuer le contrôle préalable visé au point 51 du présent arrêt.

58 La juridiction de renvoi ayant soulevé, par ailleurs, la question de savoir s'il peut être suppléé à l'absence de contrôle effectué par une autorité indépendante par un contrôle ultérieur exercé par une juridiction de la légalité de l'accès d'une autorité nationale aux données relatives au trafic et aux données de localisation, il importe de

relever que le contrôle indépendant doit intervenir, ainsi que l'exige la jurisprudence rappelée au point 51 du présent arrêt, préalablement à tout accès, sauf cas d'urgence dûment justifiée, auquel cas le contrôle doit intervenir dans de brefs délais. Ainsi que l'a relevé M. l'avocat général au point 128 de ses conclusions, un tel contrôle ultérieur ne permettrait pas de répondre à l'objectif d'un contrôle préalable, consistant à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire.

59 Dans ces conditions, il convient de répondre à la troisième question préjudicielle que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale. »

6.11.2 Il ressort de cette jurisprudence de la Cour que l'exercice des pouvoirs de demander les données relatives au trafic et les données de localisation établis par le code de procédure pénale contrevient aux exigences de la directive 2002/58 lorsque cet exercice implique une ingérence grave dans le droit à la protection de la vie privée et que la décision d'exercer ces pouvoirs a été prise par le procureur. Par conséquent, la question se pose de savoir si (le système de) la loi autorise un autre mode d'exercice de ces pouvoirs de demander les données relatives au trafic et les données de localisation, qui serait conforme à ces exigences.

6.11.3 Aux points 117 à 125 de son pourvoi, l'avocat général a exposé les principes du régime du code de procédure pénale régissant le rôle du juge d'instruction dans l'information. Il découle de cet exposé que le régime du code de procédure pénale ne s'oppose pas à ce que le procureur sollicite l'autorisation du juge d'instruction pour exercer un pouvoir visant à obtenir des données relatives au trafic et des données de localisation (autres que les seules données d'identification) visées à l'article 2, sous b) et c), de la directive 2002/58. Par conséquent, le procureur peut également demander cette autorisation dans les cas où le code de procédure pénale n'exige pas qu'il obtienne l'autorisation du juge d'instruction avant de demander la communication des données relatives au trafic et des données de localisation. Comme c'est le cas pour d'autres pouvoirs concernant la demande de données et les communications au moyen d'un dispositif automatisé, le juge d'instruction donne son autorisation par écrit. En cas de nécessité urgente, l'autorisation du juge d'instruction peut être donnée oralement. Dans ce cas, le juge d'instruction met son autorisation par écrit dans les trois jours (voir article 126nf et article 126m, paragraphe 5, du code

de procédure pénale, chaque fois en combinaison avec l'article 1261, paragraphe 7, du code de procédure pénale).

6.11.4 S'agissant de la question de savoir dans quelles situations le procureur est tenu de solliciter l'autorisation écrite du juge d'instruction, le Hoge Raad (Cour suprême, Pays-Bas) observe ce qui suit. Pour répondre à la question de savoir si la demande des données relatives au trafic et des données de localisation implique une ingérence grave dans le droit à la protection de la vie privée de l'utilisateur et, dans l'affirmative, si cette ingérence peut être justifiée dans un cas concret, il convient d'avoir égard, en particulier, à la nature des données, de l'infraction pénale ou des infractions pénales visées par la demande, ainsi qu'à la personne ou aux personnes concernées par les données à fournir. À cet égard, ainsi que nous l'avons énoncé au point 6.8.3, il n'est pas toujours possible, au moment de la demande, de savoir exactement si des données seront obtenues ni, le cas échéant, quelles données seront obtenues, ni encore de connaître le contenu de ces données. Par conséquent, il n'est pas toujours possible de déterminer par avance s'il y aura une ingérence grave dans le droit à la protection de la vie privée.

Selon le Hoge Raad (Cour suprême, Pays-Bas), il s'ensuit que, si un procureur souhaite obtenir des données relatives au trafic et des données de localisation qui ne se limitent pas à des données d'identification, celui-ci est tenu de solliciter l'autorisation écrite du juge d'instruction avant de demander ces données. En pratique, cela implique que, si le procureur exerce les pouvoirs établis aux articles 126na, 126ua et 126zi du code de procédure pénale, il n'a pas besoin de l'autorisation écrite du juge d'instruction. En revanche, s'il exerce les pouvoirs établis aux articles 126n, 126u et 126zh du code de procédure pénale, les pouvoirs établis aux articles 126ni, 126ui et 126zja du code de procédure pénale, pour autant que la demande soit adressée au fournisseur d'un service de communication, ou le pouvoir établi à l'article 126zo du code de procédure pénale, le procureur doit – bien que cela ne soit pas prescrit par la loi – solliciter l'autorisation écrite du juge d'instruction.

6.11.5 Si le procureur demande une autorisation écrite, le juge d'instruction est tenu de statuer sur cette demande. La circonstance que – selon le juge d'instruction – la demande des données concernées n'impliquera pas de violation (si ce n'est limitée) de la vie privée de l'utilisateur n'est pas un motif d'irrecevabilité de la demande du procureur.

Lorsqu'il statue sur une demande d'autorisation, le juge d'instruction examine si les exigences établies par loi concernant une demande de communication des données relatives au trafic et des données de localisation sont remplies, et il apprécie si cette demande est conforme aux critères de proportionnalité et de subsidiarité, ainsi que nous l'avons exposé en détail aux points 6.8.1 à 6.8.3, 6.10.3 et 6.10.4 ci-dessus. Cet examen permet de garantir que le contrôle poursuit « 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 » [37].

6.11.6 Il découle de ce qui précède que – contrairement au principe dont était parti le législateur lors de l'élaboration des dispositions concernées – il est nécessaire que le juge d'instruction assume un rôle de contrôle afin que les pouvoirs établis aux articles 126n, 126u et 126zh du code de procédure pénale, les pouvoirs établis aux articles 126ni, 126ui et 126zja du code de procédure pénale, pour autant que la demande soit adressée au fournisseur d'un service de communication, et le pouvoir établi à l'article 126zo du code de procédure pénale soient exercés conformément à la directive. À cette fin, il convient de mettre à la disposition des juridictions des capacités suffisantes pour apprécier les demandes adressées par le procureur à cet égard.

Les irrégularités formelles

6.12.1 Si une irrégularité formelle est commise dans l'exercice des pouvoirs exposés aux points 5.1 et 5.2, la question se pose de savoir s'il convient d'assortir cette irrégularité formelle d'une conséquence juridique et, si oui, laquelle. On peut notamment imaginer la situation dans laquelle la demande de données relatives au trafic et de données de localisation (autres que les seules données d'identification) a été adressée sans l'obtention préalable d'une autorisation du juge d'instruction, alors que cette autorisation était requise au vu des considérations énoncées au point 6.11. Savoir s'il convient d'assortir une telle irrégularité d'une conséquence juridique est particulièrement pertinent puisque la Cour a clarifié progressivement le sens des dispositions de la directive 2002/58 par des arrêts successifs. Il se peut donc que des cas se soient produits, ou se produisent, dans lesquels ce n'est qu'après que le procureur a exercé les pouvoirs exposés aux points 5.1 et 5.2 qu'il s'est avéré que cet exercice n'était pas totalement conforme aux exigences du droit de l'Union.

6.12.2 Dans l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), la Cour a jugé qu'il appartenait, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans les matières pénales, d'informations et d'éléments de preuve qui ont été obtenus par (notamment) un accès des autorités nationales aux données relatives au

[37] Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 52.

trafic et aux données de localisation à l'encontre du droit de l'Union [38]. À cet égard, la Cour a également considéré ce qui suit :

« 41 Enfin, compte tenu du fait que la juridiction de renvoi est saisie d'une demande concluant à l'irrecevabilité des procès-verbaux établis à partir des données relatives au trafic et des données de localisation, au motif que les dispositions de l'article 111[1] de la loi relative aux communications électroniques seraient contraires à l'article 15, paragraphe 1, de la directive 2002/58 tant en ce qui concerne la conservation des données que l'accès à celles-ci, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, d'informations et d'éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée de ces données, contraire au droit de l'Union (arrêt 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 222), ou encore par un accès des autorités nationales auxdites données, contraire à ce droit.

42 En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (arrêt 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 223 ainsi que jurisprudence citée).

43 Pour ce qui est plus particulièrement du principe d'effectivité, il convient de rappeler que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine (arrêt du 6 octobre 2020,

38 Arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 41.

La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 225).

44 La nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable. Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation. Partant, le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 226 et 227). »

6.12.3 Les irrégularités formelles liées à l'exercice de pouvoirs visant à obtenir des données relatives au trafic et des données de localisation sont appréciées sur le fondement de l'article 359 du code de procédure pénale. Les principes du régime de l'article 359 du code de procédure pénale, tels qu'ils ont été développés par la jurisprudence du Hoge Raad (Cour suprême, Pays-Bas) [39], sont conformes aux considérations de la Cour, citées au point 6.12.2, sur le sens, notamment, du principe d'effectivité lorsque l'accès aux données relatives au trafic et aux données de localisation a été accordé en violation du droit de l'Union. Il importe à cet égard, ainsi que l'exige également le droit de l'Union, que la défense soit en mesure – et soit mise en mesure – de commenter les éléments de preuve et (la régularité de) leur obtention lors de l'instruction de l'affaire pénale.

6.12.4 L'exclusion des preuves à titre de conséquence juridique d'une irrégularité formelle peut tout d'abord être envisagée s'il s'avère nécessaire d'exclure certains résultats de l'information découlant de l'utilisation des preuves pour empêcher une violation du droit à un procès équitable tel que garanti par l'article 6 de la Convention européenne des droits de l'homme – et par la

[39] Voir, en particulier, Hoge Raad (Cour suprême, Pays-Bas) 1er décembre 2020, ECLI:NL:HR:2020:1889.

disposition correspondante de l'article 47, deuxième alinéa, de la Charte [40]. On peut également exclure des preuves en cas de violation grave d'une règle ou d'un principe juridique de la procédure pénale ; ensuite, dans certaines circonstances, on peut considérer que l'exclusion des preuves est nécessaire pour garantir l'État de droit et pour empêcher les fonctionnaires chargés de l'enquête et des poursuites d'agir de manière irrégulière, et donc pour éviter que des irrégularités formelles comparables se produisent à l'avenir [41]. La circonstance que le procureur a adressé une demande de communication des données relatives au trafic et des données de localisation (autres que les seules données d'identification) sans avoir obtenu préalablement l'autorisation du juge d'instruction, alors que cette autorisation était requise sur la base des considérations énoncées au point 6.11.4, ne justifie pas en soi l'exclusion des preuves.

6.12.5 Pour pouvoir bénéficier d'une réduction de peine, le suspect doit avoir effectivement subi un préjudice du fait de l'irrégularité formelle et cette réduction de peine doit également être justifiée compte tenu de l'importance de la règle violée et de la gravité de l'irrégularité. Une réduction de peine en tant que conséquence juridique permettant de réparer le préjudice subi par le suspect est possible, notamment, en cas d'irrégularité formelle ayant causé une violation de la vie privée du suspect [42]. Une réduction de peine peut être justifiée si le procureur a adressé une demande de communication des données relatives au trafic et des données de localisation (autres que les seules données d'identification) sans avoir obtenu préalablement l'autorisation du juge d'instruction, alors que cette autorisation était requise sur la base des considérations énoncées au point 6.11.4, et si des moyens de preuve à charge du suspect ont été obtenus via cette demande. À cet égard, la question de savoir si et dans quelle mesure la vie privée du suspect a été violée est déterminante au regard de la gravité de l'irrégularité et du préjudice effectivement subi en raison de l'irrégularité. Pour pouvoir appliquer une réduction de peine, il doit être question d'une irrégularité formelle suffisamment grave, qui a concrètement lésé les intérêts du suspect dans l'affaire pénale. Si l'irrégularité formelle n'a porté qu'une atteinte limitée au droit à la protection de la vie privée, le juge peut se contenter de constater cette irrégularité formelle [43].

40 Hoge Raad (Cour suprême, Pays-Bas) 1er décembre 2020, ECLI:NL:HR:2020:1889, point 2.4.1.

41 Hoge Raad (Cour suprême, Pays-Bas) 1er décembre 2020, ECLI:NL:HR:2020:1889, point 2.4.4.

42 Hoge Raad (Cour suprême, Pays-Bas) 1er décembre 2020, ECLI:NL:HR:2020:1889, points 2.3.2 et 2.3.4.

43 Hoge Raad (Cour suprême, Pays-Bas) 1er décembre 2020, ECLI:NL:HR:2020:1889, point 2.3.2.

Le cadre décisionnel et les conséquences pour d'autres affaires pénales

6.13.1 Conformément à la jurisprudence de la Cour exposée ci-dessus, le Hoge Raad (Cour suprême, Pays-Bas) considère que la réglementation établie par le code de procédure pénale concernant la demande des données relatives au trafic et des données de localisation n'est pas conforme aux exigences de la directive 2002/58 lorsque l'exercice de ces pouvoirs implique une ingérence grave dans le droit à la protection de la vie privée et lorsque la décision d'exercer ces pouvoirs est prise par le procureur. Dans ces situations, en dehors des cas urgents, un « contrôle préalable effectué par une juridiction ou une entité administrative indépendante » s'impose. Ce contrôle ne saurait être effectué par le ministère public, et donc par le procureur. Il n'est pas exigé qu'il soit effectué lorsque ce dont il s'agit, c'est exclusivement de données permettant d'identifier l'utilisateur concerné sans que les données puissent être associées à des informations relatives aux communications effectuées.

6.13.2 Compte tenu de ce qui précède, le Hoge Raad (Cour suprême, Pays-Bas) estime que, si le procureur souhaite obtenir des données relatives au trafic et des données de localisation qui ne se limitent pas exclusivement aux données d'identification, il est tenu d'obtenir une autorisation écrite du juge d'instruction pour pouvoir demander ces données. En pratique, il s'ensuit que si le procureur exerce les pouvoirs établis aux articles 126na, 126ua et 126zi du code de procédure pénale, il n'a pas besoin de l'autorisation écrite du juge d'instruction. En revanche, si le procureur exerce les pouvoirs établis aux articles 126n, 126u en 126zh du code de procédure pénale, les pouvoirs établis aux articles 126ni, 126ui et 126zja du code de procédure pénale, pour autant que la demande soit adressée au fournisseur d'un service de communication, et le pouvoir établi à l'article 126zo du même code, le procureur doit – bien que cela ne soit pas prescrit par la loi – solliciter l'autorisation écrite du juge d'instruction.

6.13.3 Si le procureur demande une autorisation écrite, le juge d'instruction est tenu de statuer sur cette demande. Lorsqu'il statue sur cette demande, le juge d'instruction examine si les exigences établies par loi concernant une demande de communication des données relatives au trafic et des données de localisation sont remplies, et il apprécie si cette demande est conforme aux critères de proportionnalité et de subsidiarité.

6.13.4 Dès lors que la jurisprudence de la Cour soulève des questions sur l'interprétation qu'il convient de donner à la directive 2002/58, le Hoge Raad (Cour suprême, Pays-Bas) posera des questions préjudicielles à la Cour (voir point 8 ci-dessous).

6.13.5 Il n'y a pas lieu, compte tenu également de ce que l'avocat général a observé à ce sujet aux points 145 et 146 de son pourvoi, de suspendre les autres affaires traitant d'une demande de communication des données

relatives au trafic et des données de localisation dans l'attente de la réponse de la Cour aux questions préjudicielles. Le cadre décisionnel exposé ci-dessus par le Hoge Raad (Cour suprême, Pays-Bas) peut servir de base aux affaires en cours.

7. L'appréciation du moyen de cassation

7.1 Le moyen de cassation fait grief au rechtbank (tribunal) d'avoir considéré que l'octroi d'une autorisation écrite aux fins d'une demande de données visée à l'article 126n du code de procédure pénale était conforme en l'espèce aux exigences imposées par la directive 2002/58 en ce qui concerne, en particulier, l'infraction pénale à l'égard desquelles ces données peuvent être demandées.

7.2 L'ordonnance du rechtbank (tribunal) concerne une demande de communication de données d'un utilisateur (le suspect) d'un service de télécommunication et le trafic des communications lié à cet utilisateur entre le 9 août 2021 et le 12 août 2021. Il s'agit donc d'une demande de communication de données (historiques) relatives au trafic et de données (historiques) de localisation telles que visées à l'article 126n, paragraphe 1, du code de procédure pénale.

7.3 Il convient d'abord de formuler les observations suivantes sur le cadre dans lequel l'examen doit être effectué. Le rechtbank (tribunal) a apprécié si le procureur pouvait se voir accorder l'autorisation de demander des données relatives au trafic et des données de localisation sur le fondement de l'article 126n du code de procédure pénale. L'article 126n, paragraphe 1, du code de procédure pénale exige qu'il y ait un soupçon d'infraction visée à l'article 67, paragraphe 1, du code de procédure pénale. Contrairement à l'article 126ng, paragraphe 2, du code de procédure pénale, cette disposition n'exige pas que l'infraction pénale constitue une atteinte grave à l'ordre juridique. Il ne ressort pas davantage de la jurisprudence de la Cour qu'il y aurait lieu d'établir l'existence d'une infraction constituant une atteinte grave à l'ordre juridique. Il convient de considérer que la référence faite par le rechtbank (tribunal), dans les considérations énoncées au point 4.2-ci-dessus, au critère d'une infraction constituant une atteinte grave à l'ordre juridique procède d'une erreur manifeste. Il y a lieu de faire une lecture corrigée des considérations du rechtbank (tribunal).

7.4.1 Le rechtbank (tribunal) a jugé que la demande de communication des données relatives au trafic et des données de localisation relevait en l'espèce de la lutte contre la criminalité grave. À cet égard, le rechtbank (tribunal) a estimé que le soupçon visait un vol qualifié en réunion, que cette infraction pénale était punissable d'un emprisonnement de six ans maximum – de sorte qu'il s'agit également d'une infraction visée à l'article 67, paragraphe 1, du code de procédure pénale – et que cette infraction pénale concernait un objet

d'une valeur d'environ 18 000 euros. Le rechtbank (tribunal) a également pris en considération le fait que l'infraction pénale dont était soupçonné le suspect était passible d'une détention provisoire et que, eu égard au risque de récidive, une ordonnance de détention avait été prononcée contre l'utilisateur.

7.4.2 Compte tenu des considérations qui précèdent aux points 6.5.3, 6.6.3 et 6.8, l'appréciation manifeste du rechtbank (tribunal) selon laquelle, compte tenu des exigences imposées par la loi et par le droit de l'Union, une autorisation peut être accordée aux fins d'une demande de données relatives au trafic et de données de localisation, ne procède pas d'une erreur de droit. En effet, d'une manière générale, une infraction au sens de l'article 67, paragraphe 1, du code de procédure pénale – y compris un vol qualifié en réunion – peut être considérée comme une infraction grave. Le rechtbank (tribunal) a en outre pris en considération la gravité de l'infraction concrète dont l'utilisateur est soupçonné. Sur cette base, il a manifestement estimé, de manière compréhensible, que la violation du droit à la protection de la vie privée qui découle de la demande de communication des données visées à l'article 126n, paragraphe 1, du code de procédure pénale, concernant l'utilisateur ainsi que le trafic des communications lié à cet utilisateur et se rapportant à un numéro de téléphone pour une période de quatre jours, était proportionnée à la gravité de l'infraction concrète.

8. Demande de décision préjudicielle

8.1 Ainsi que nous l'avons exposé en détail aux points 6.2 et 6.7, il y a lieu de poser des questions préjudicielles à la Cour sur les points de droit abordés dans le présent arrêt, afin de pouvoir statuer définitivement sur le moyen de cassation.

8.2 La première question préjudicielle s'énonce comme suit :

> Les mesures législatives concernant l'octroi aux autorités publiques d'un accès aux données relatives au trafic et aux données de localisation (y compris les données d'identification), dans le cadre de la prévention, de la recherche, de la détection et de la poursuite des infractions pénales, relèvent-elles du champ d'application de la directive 2002/58 lorsqu'il s'agit d'octroyer un accès à des données qui ne sont pas conservées sur le fondement de mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58, mais qui sont conservées par le fournisseur sur un autre fondement ?

Pour les raisons exposées au point 6.2.4, le Hoge Raad (Cour suprême, Pays-Bas) considère que cette question appelle une réponse affirmative.

8.3 La deuxième question préjudicielle s'énonce comme suit :

a) Les notions d'« infractions pénales graves » et de « criminalité grave » utilisées dans les arrêts de la Cour mentionnés aux points 5.7 et 5.8 sont-elles des notions autonomes du droit de l'Union ou appartient-il aux autorités compétentes des États membres d'en préciser elles-mêmes le contenu ?

b) S'il s'agit de notions autonomes du droit de l'Union, selon quelles modalités convient-il de déterminer s'il est question d'« infractions pénales graves » ou de « criminalité grave » ?

Pour les raisons exposées aux points 6.6.2 et 6.6.3, le Hoge Raad (Cour suprême, Pays-Bas) considère qu'il appartient aux autorités compétentes des États membres de préciser elles-mêmes le contenu des notions précitées.

8.4 La troisième question préjudicielle s'énonce comme suit :

L'accès aux données relatives au trafic et aux données de localisation (autres que les seules données d'identification) aux fins de la prévention, de la recherche, de la détection et de la poursuite des infractions pénales peut-il être accordé aux autorités publiques au titre de la directive 2002/58 en l'absence d'infraction pénale grave ou de criminalité grave, en particulier lorsque l'on peut supposer que, dans le cas concret, l'octroi de l'accès à ces données ne devrait entraîner qu'une ingérence limitée dans, notamment, le droit à la protection de la vie privée de l'utilisateur visé à l'article 2, sous b) [*], de la directive 2002/58 ?

Pour les raisons exposées au point 6.5.3, le Hoge Raad (Cour suprême, Pays-Bas) considère que, compte tenu des considérations relatives au principe de proportionnalité énoncées dans les arrêts de la Cour cités aux points 5.7 et 5.8, cette question appelle une réponse affirmative.

8.5 Avant de statuer, le Hoge Raad (Cour suprême, Pays-Bas) demande à la Cour de se prononcer sur la directive 2002/58 eu égard aux questions précitées. Le Hoge Raad (Cour suprême, Pays-Bas) note que ces questions préjudicielles sont posées dans le cadre d'une procédure en cassation dans l'intérêt de la loi. Le fait que le Hoge Raad (Cour suprême, Pays-Bas) soit également compétent pour poser des questions préjudicielles dans le cadre d'une telle procédure est confirmé par l'arrêt du 21 novembre 2019, Procureur-Generaal bij de Hoge Raad der Nederlanden (C-678/18, EU:C:2019:998) [44].

[OMISSIS]

[*] Ndt : Peut-être faut-il lire « sous a) ».

[44] Arrêt du 21 novembre 2019, Procureur-Generaal bij de Hoge Raad der Nederlanden, C-678/18, EU:C:2019:998, en particulier points 21 à 27.

[OMISSIS] [Formule de clôture et signature]