COUR DE CASSATION

# RAPPORT DE Mme MÉNOTTI, CONSEILLERE

## Arrêt n° 769 du 12 juillet 2022 – Chambre criminelle

## Pourvoi n° 21-83.710

## Décision attaquée : chambre de l'instruction de la cour d'appel de Paris, 7e section, 27 mai 2021

**M. [C] [L] [E]**
***C/***

_____

M. [C] [L] [E] a formé un pourvoi contre l'arrêt n° 3 de la chambre de l'instruction de la cour d'appel de Paris, 7e section, en date du 27 mai 2021, qui, dans l'information suivie contre lui notamment des chefs de meurtre et tentative de meurtre en bande organisée, destruction de biens, recel en bande organisée et association de malfaiteurs, a prononcé sur sa requête aux fins d'annulation de pièces de la procédure.

## RAPPEL DES FAITS ET DE LA PROCÉDURE

La chronologie des faits s'établit comme suit :

- le 24 août 2019, vers 21h35, les policiers étaient requis pour une fusillade qui venait de se produire au [adresse 1] où ils découvraient, au pied de la rampe d'accès au parking souterrain de la résidence, le corps criblé de balles de [D] [P] sur le siège conducteur d'un véhicule […] immatriculé [IMMATRICULATION 1] moteur tournant ;

- l'exploitation de la vidéo-surveillance révélait que la fusillade était le fait de 2 individus arrivés en haut de la rampe du parking à bord d'un véhicule conduit par un troisième, les trois individus ayant ensuite pris la fuite à bord dudit véhicule ressemblant fortement à une […] découverte incendiée vers 22h25 à [LOCALITÉ 1] ;
- diverses investigations étaient effectuées par les enquêteurs dans le cadre de l'enquête de flagrance ;
- le 6 septembre 2019, une information était ouverte des chefs d'assassinat et tentative d'assassinat en bande organisée, destruction d'un bien par un moyen dangereux en bande organisée, recel de vol en bande organisée, association de malfaiteurs (D 577) ;
- le 23 juin 2020, M. [C] [L] [E] était interpellé ;
- mis en examen le 26 juin suivant notamment des chefs sus-visés, il était placé en détention provisoire le 30 juin 2020, puis interrogé le 23 octobre 2020 ;
- le 28 décembre 2020, il déposait une requête en nullité invoquant :
  * la nullité de l'obtention des données de trafic et de localisation afférentes à une ligne téléphonique (XXXXXXXXX 01) dont l'usage lui était attribué (requête p.14), par les enquêteurs agissant en flagrance sur le fondement de l'article 60-1 du code de procédure pénale (requête p.18), du fait que ces données ont été conservées de manière généralisée et indifférenciée en violation de l'article 15 de la directive 2002/58/CE du 12 juillet 2002 et en violation de l'article 8 de la CEDH protégeant la vie privée ;
  * l'inconstitutionnalité de l'article L 34-1 du code des postes et télécommunications ;
- par arrêt n°3 du 27 mai 2021, la chambre de l'instruction de PARIS rejetait les demandes d'annulation de M. [E].

Cette décision donnait lieu :

- le 31 mai 2021, à un pourvoi de M. [E] par déclaration d'un avocat au barreau de PARIS, au greffe de la juridiction ayant rendu la décision attaquée, soit dans les 5 jours francs prévus par l'article 568 alinéa 1 du code de procédure pénale ;
- le 17 juin 2021, à une constitution d'avocat (SCP CELICE) au nom de celui-ci ;
- le 23 septembre 2021, à une ordonnance du président de la chambre criminelle ordonnant l'examen immédiat de l'affaire ;
- le 14 octobre 2021, au dépôt d'un mémoire ampliatif et d'un mémoire spécial posant une question prioritaire de constitutionnalité ;
- par décision du 25 février 2022 (n°2021-976/977 QPC), le Conseil constitutionnel déclarait contraire à la Constitution les mots *«la recherche, de la constatation et de la poursuite des infractions pénales»* et *«de l'autorité judiciaire ou»* figurant à la 1re phrase du paragraphe III de l'article L 34-1 du code des postes et des communications électroniques, dans sa rédaction résultant de la loi n°2013-1168 du 18 décembre 2013, mais précisait que ces mesures ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

## ANALYSE SUCCINCTE DES MOYENS

Le mémoire ampliatif invoque 3 moyens de cassation :
- le 1er moyen invoque l'inconstitutionnalité de l'article L 34-1 du code des postes et communications électroniques, objet de la question prioritaire soumise au Conseil constitutionnel ;
- le 2e moyen :
  1° argue du défaut de réponse aux conclusions invoquant la violation de l'article 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, 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, du fait d'un recueil et d'une conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation ;
  2° critique le fait que la chambre de l'instruction a retenu que l'atteinte portée à la vie privée de l'intéressé était proportionnée à l'objectif poursuivi ;

- le 3e moyen invoque la violation de l'article 8 de la CEDH du fait du recueil et de la conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation, le recueil desdites données ne faisant l'objet ni d'une autorisation en amont ni d'un contrôle en aval par une autorité indépendante.

## MOTIVATION DE LA CHAMBRE DE L'INSTRUCTION

La chambre de l'instruction a statué comme suit :

*S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, un Etat membre peut également prévoir la conservation ciblée desdites données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge ou une autorité administrative indépendante.*
*Il ressort enfin des arrêts de la CJUE que le juge pénal doit 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, 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".*
*En l'espèce, les lignes téléphoniques utilisées par [C] [L] [E] étaient exploitées par les enquêteurs, suite à leur identification dans le cadre de l'exploitation du flux des bornes couvrant les lieux intéressant l'enquête: la scène de crime d'[Localité 2] dans le créneau du meurtre, la scène de l'incendie du véhicule des auteurs à [Localité 1] et le secteur du domicile de [D] [P] à [Localité 3], où était localisé de manière récurrente le véhicule utilisé par les tueurs. L'obtention de ces données et leur exploitation permettait notamment de le localiser à proximité des lieux où se trouvait [D] [P], la victime, et donc qu'il effectuait des surveillances de ce dernier ; qu'il se trouvait encore aux abords de son domicile peu de temps avant son assassinat , qu'il a pu donner le «top départ» à un individu pour venir le rejoindre à cet endroit où la victime était in fini abattue peu de temps après et enfin, qu'il a escorté le véhicule [...] occupé par les tireurs jusqu'à [LOCALITÉ 2].*
*[C] [L] [E] était mis en examen le 26 juin 2020 de sorte qu'il a eu accès à la procédure à partir de cette date et est donc depuis en mesure de commenter efficacement l'ensemble des éléments de la procédure apparaissant comme constituant des indices graves ou concordants rendant vraisemblable son implication comme auteur ou complice des faits pour lesquels i l est mis en examen.*
*Partant, l'ingérence alléguée dans la vie privée de [C] [L] [E], du fait des réquisitions des enquêteurs aux opérateurs téléphoniques, est prévue par la loi; elle a un but légitime qui est celui de la recherche d'infractions pénales relevant de la criminalité grave, en l'espèce : meurtre et tentative de meurtre en bande organisée, destruction par moyen dangereux en bande organisée, association de malfaiteurs en vue de la préparation de crime et délits, recel en bande organisée; cet objectif tendant à la recherche d'infractions pénales est nécessaire dans une société démocratique, et cette ingérence apparaît enfin proportionnée à la poursuite de l'objectif*
*.*

## DISCUSSION

L'articulation des moyens invoqué par l'intéressé conduit à distinguer 4 questions :
- celle de l'inconstitutionnalité de l'article L.34-1 du code des postes et communications électroniques ;
- celle de la conservation des données de connexion ;
- celle de l'accès auxdites données ;
- celle de la sanction de la méconnaissance éventuelle du droit européen en matière de conservation et d'accès aux données de connexion.

**SUR LE 1ER MOYEN RELATIF À L'INCONSTITUTIONNALITÉ DE L'ARTICLE L 34-1 DU CODE DES POSTES ET TÉLÉCOMMUNICATIONS**

Le contentieux concernant la conservation et l'accès aux données de connexion s'est développé à partir de l'article L.34-1 du code des postes et télécommunications, dans sa version applicable du 20 décembre 2013 au 31 juillet 2021.

En son paragraphe II, cet article pose le principe de l'effacement ou de l'anonymisation de toute donnée collectée par les opérateurs de télécommunications.

Deux exceptions sont néanmoins prévues :
- d'une part, le paragraphe III prévoit que, *«pour les besoins de la recherche, de la constatation et de la poursuites des infractions pénales», « il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques»* ;
- d'autre part, le paragraphe IV permet la conservation, par les opérateurs, des données techniques nécessaires à la facturation et au paiement des prestations, pendant la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées.

Ainsi, il résulte de cet article L 34-1 que les opérateurs, les fournisseurs d'accès à internet et les hébergeurs ont l'obligation de conserver de manière générale et indifférenciée les données de connexion notamment pour les besoins de la recherche, de la constatation et de la poursuite des infractions dans les conditions et limites fixées par la loi et les dispositions réglementaires prises pour son application.

Dans sa décision du 25 février 2022 (n°2021-976/977 QPC), le Conseil constitutionnel a déclaré contraire à l'article 2 de la Constitution garantissant le droit au respect de la vie privée, certaines dispositions de cet article L 34-1 du code des postes et communications électroniques résultant de la loi n°2013-1168 du 18 décembre 2013 pour les motifs suivants :

*11. Toutefois, en premier lieu, les données de connexion conservées en application des dispositions contestées portent non seulement sur l'identification des utilisateurs des services de communications électroniques, mais aussi sur la localisation de leurs équipements terminaux de communication, les caractéristiques techniques, la date, l'horaire et la durée des communications ainsi que les données d'identification de leurs destinataires. Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, ces données fournissent sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée.*
*12. En second lieu, d'une part, une telle conservation s'applique de façon générale à tous les utilisateurs des services de communications électroniques. D'autre part, l'obligation de conservation porte indifféremment sur toutes les données de connexion relatives à ces personnes, quelle qu'en soit la sensibilité et sans considération de la nature et de la gravité des infractions susceptibles d'être recherchées.*
*13. Il résulte de ce qui précède qu'en autorisant la conservation générale et indifférenciée des données de connexion, les dispositions contestées portent une atteinte disproportionnée au droit au respect de la vie privée.*

Mais il a également prévu comme suit les conséquences de cette inconstitutionnalité

*17. D'autre part, la remise en cause des mesures ayant été prises sur le fondement des dispositions déclarées contraires à la Constitution méconnaîtrait les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions et aurait ainsi des conséquences manifestement excessives. Par suite, ces mesures ne peuvent être contestées sur le fondement de cette inconstitutionnalité.*

A titre de comparaison et pour une disposition inconstitutionnelle dont l'abrogation a été différée, la chambre criminelle a rendu la décision suivante :

Crim.17/06/2020, n°19-86.535 : *«Si le Conseil constitutionnel, dans sa décision n° 2019-828/829 QPC du 28/02/2020, a déclaré contraires à la Constitution les mots "Du mari ou de la femme" figurant au 5° de l'article 335 du code de procédure pénale, en ce qu'il dispense ces personnes de l'obligation de prêter serment devant la cour d'assises lors des débats au cours desquels est jugé leur conjoint, il a reporté les effets de cette abrogation au 31/12/2020, sans en faire bénéficier aucunement l'auteur de la question prioritaire de constitutionnalité. 8. Il s'en suit que le moyen est devenu sans objet.»*

## SUR LA CONSERVATION DES DONNÉES

### LES DIFFERENTS TYPES DE DONNEES DE CONNEXION

Il existe trois types de données de connexion :
- les données d'identité qui permettent d'identifier l'utilisateur d'un numéro de téléphone, de carte SIM, d'abonné, d'une adresse IP ou d'une adresse mail ;
- les données relatives au trafic qui établissent les contacts qu'une personne a eus par téléphone ou par SMS, la date et l'heure de ce contact, la durée de l'échange : ce sont notamment ce que l'on appelle les «fadettes» ;
- les données de localisation qui permettent de connaître les zones d'émission et de réception d'une communication passée avec un téléphone mobile et d'obtenir la liste des appels ayant borné à la même antenne relais ;

### LES NORMES

#### Les normes de droit interne

L'article L.34-1 du code des postes et communications électroniques

Il convient de se reporter à ce qui a été dit ci-dessus.

L'article R. 10-13 dudit code

Cet article énumère les catégories de données relevant du régime précité et fixe leur durée de conservation à un an à compter de leur enregistrement.

Sont concernées par cette obligation :
*«a) Les informations permettant d'identifier l'utilisateur ;*
*b) les données relatives aux équipements terminaux de communication utilisés ;*
*c) les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;*
*d) les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;*
*e) les donnés permettant d'identifier le ou les destinataires de la communication».*

Cet article prévoit également que, pour les activités de téléphonie, l'opérateur doit conserver les données relatives au trafic et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

#### Les normes de droit européen

Les normes de droit européen en cause sont les suivantes :

- l'article 7 de la Charte précitée, intitulé "Respect de la vie privée et familiale" qui énonce que :

> Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

- l'article 8 de la Charte qui dispose que :

> Protection des données à caractère personnel
> 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

- l'article 11 de la Charte qui prévoit :

> Liberté d'expression et d'information
> 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.
> 2. La liberté des médias et leur pluralisme sont respectés.

- l'article 52, intitulé «Portée des droits garantis», énonce que :

> 1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.
> 2. Les droits reconnus par la présente Charte qui font l'objet de dispositions dans les traités s'exercent dans les conditions et limites définies par ceux-ci.
> 3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.
> 4. Dans la mesure où la présente Charte reconnaît des droits fondamentaux tels qu'ils résultent des traditions constitutionnelles communes aux États membres, ces droits doivent être interprétés en harmonie avec lesdites traditions.
> 5. Les dispositions de la présente Charte qui contiennent des principes peuvent être mises en oeuvre par des actes législatifs et exécutifs pris par les institutions, organes et organismes de l'Union, et par des actes des États membres lorsqu'ils mettent en oeuvre le droit de l'Union, dans l'exercice de leurs compétences respectives. Leur invocation devant le juge n'est admise que pour l'interprétation et le contrôle de la légalité de tels actes.
> 6. Les législations et pratiques nationales doivent être pleinement prises en compte comme précisé dans la présente Charte.
> 7. Les explications élaborées en vue de guider l'interprétation de la présente Charte sont dûment prises en considération par les juridictions de l'Union et des États membres.

La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 dite *"vie privée et communications électroniques"* énonce elle-même, dans son préambule, qu'elle vise à respecter les droits fondamentaux et à garantir le plein respect des droits exposés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne.

L'article 15 §1 de cette directive prévoit que :

> 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]. 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 [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

Les opérateurs mentionnés à l'article L 34-1 du code des postes et communications électroniques relèvent du champ d'application de cette directive.

**La jurisprudence de la Cour de justice de l'Union européenne (CJUE)**

Les arrêts du 6 octobre 2020 relatifs à LAQUADRATURE DU NET

La position de la CJUE sur la conservation et l'accès aux données de connexion s'est construite par touches successives (CJUE, 08/04/2014, DIGITAL RIGHTS IRELAND LDT (C-293/12 et C-594/12) ; CJUE du 21/12/2016, TELE2 SVERIGE ET WATSON (C-203/15 et C-698/15) ; CJUE du 02/10/2018, MINISTERIO FISCAL (C-207/16).

Par trois décisions rendues le 6 octobre 2020 dans LA QUADRATURE DU NET (C-511/18, C-512/18, C520/18), la CJUE a entendu limiter strictement la possibilité d'imposer aux opérateurs de communications électroniques la conservation des données de connexion de leurs utilisateurs.

Le raisonnement de la Cour est fondé sur le fait que les données de connexion d'une personne peuvent permettre de tirer des conclusions très précises concernant sa vie privée, sans même qu'il soit besoin d'accéder au contenu des échanges ou des informations consultées. Elle en déduit l'existence d'une ingérence dans les droits fondamentaux de l'intéressé dès l'obligation faite aux opérateurs de les conserver. Cette ingérence est d'autant plus grave que la conservation est générale et indifférenciée puisqu'elle porte sur l'ensemble des utilisateurs des services et l'ensemble des communications sur le territoire national.

La Cour reconnaît l'importance des objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave, qui contribuent à la protection des droits et libertés d'autrui, mais elle précise que les mesures de restriction prises sur le fondement de l'article 15 de la directive étant dérogatoires aux principes de confidentialité et d'effacement ou d'anonymisation rapides des données posés par le même texte, elles doivent s'interpréter strictement et ne sauraient devenir la règle.

Elle en déduit qu'il convient de distinguer selon le type des données qui doivent, chacune, faire l'objet d'un traitement spécifique :

*1er type de données : les données relatives à l'identité civile des utilisateurs*

Pour la CJUE, la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs est possible aux fins de prévention, de recherche, de détection et de poursuites d'infractions pénales en général. Il n'est pas nécessaire que l'infraction soit grave.

En effet, ces données ne fournissent aucune information sur les communications effectuées, de sorte que l'ingérence qu'emporte la conservation de telles données ne peut être qualifiée de grave. Pour ce type de données, le texte ne prévoit pas de délai particulier.

*2e type de données : les données relatives aux adresses IP attribuées à la source d'une communication*

La CJUE admet que puisse être imposée aux fournisseurs d'accès à internet et aux hébergeurs une conservation généralisée et indifférenciée des adresses IP, pour une période limitée au strict nécessaire (§152 à 156) mais aux seules fins de lutte contre la criminalité grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale.

Bien qu'emportant une ingérence grave dans les droits fondamentaux de la personne concernée, l'adresse ne révèle aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication, de sorte qu'elles ont un degré de sensibilité moindre (§152).

Par ailleurs, la CJUE souligne que l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse a été attribuée dans le cas d'une infraction commise en ligne (§154).

*3e type de données : les données relatives au trafic et les données de localisation autres que les adresses IP*

Une obligation de conservation généralisée et indifférenciée des données de connexion n'est conforme au droit de l'Union qu'aux fins de sauvegarde de la sécurité nationale (§134 à 139). Cette notion inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociale fondamentales d'un pays, telles que les activités terroriste (§135).

Trois conditions sont posées :
- l'existence d'une menace grave, réelle et actuelle ou prévisible ;
- la durée de la mesure doit être limitée au strict minimum mais son renouvellement «ne peut être exclu» en cas de persistance de la menace grave ;
- l'injonction de conservation doit être soumise au contrôle d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant.

En revanche, **la Cour de justice énonce que le droit de l'Union s'oppose à une obligation de conservation généralisée et indifférenciée des données de connexion** (autres que celles précitées) **aux fins de lutte contre la criminalité** et la prévention des menaces pour la sécurité publique, **quel que soit la gravité de cette criminalité** ou de ces menaces.

Néanmoins, **la Cour de justice de l'Union européenne admet la conservation dite «rapide»** des données de connexion : cette conservation trouve son fondement dans l'article 16 de la convention de BUDAPEST sur la cyber-criminalité du 23 novembre 2001, ratifiée ou approuvée par la quasi-totalité des Etats membres, dont la FRANCE :

> *« 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 cyber-criminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – n°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, C 203/15 et C 698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée) ».*

Ainsi, par conservation rapide, il faut comprendre qu'il est possible d'enjoindre aux fournisseurs de services de communication de procéder à une conservation des données de connexion dans les conditions suivantes :

- il faut que cela concerne une infraction pénale grave ou une atteinte à la sécurité publique ;
- la décision de l'autorité compétente doit être soumise à un contrôle juridictionnel effectif ;
- la législation doit préciser la ou les finalités pour la ou lesquelles une conservation rapide peut être ordonnée ;
- la durée de conservation doit être limitée au strict nécessaire ;
- la conservation rapide ne peut porter que sur les données de trafic et de localisation susceptibles de contribuer à la prévention ou à la répression d'une infraction déterminée, sans toutefois être limitée aux données des personnes soupçonnées de vouloir commettre ou d'avoir commis une infraction pénale, pourvu qu'elles puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de l'infraction ou la prévention de la menace.

L'arrêt du 5 avril 2022 «*Commissioner of the Garda Siochana*»

Dans cet arrêt, la Cour, réunie en grande chambre, confirme sa jurisprudence constante selon laquelle le droit de l'Union s'oppose à des mesures législatives nationales prévoyant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques, aux fins de la lutte contre les infractions graves.

Toutefois, elle sème quelque peu le trouble en ce qu'elle rejette l'argumentation selon laquelle les autorités nationales compétentes devraient pouvoir accéder aux fins de la lutte contre la criminalité grave, aux données relatives au trafic et aux données de localisation qui ont été conservées de manière généralisée et indifférenciée, pour faire face à une menace grave pour la sécurité nationale. Elle souligne, en effet, que cette argumentation fait dépendre cet accès de circonstances étrangères à l'objectif de lutte contre la criminalité grave et que, selon cette argumentation, l'accès pourrait être justifié par un objectif d'une moindre importance que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale (§ 96-100).

Pour autant, elle semble valider l'interprétation du Conseil d'Etat ci-dessous examinée concernant la conservation rapide en indiquant :

*86. Dans une telle situation, il est loisible aux Etats membres ... de prévoir ... 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. ...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 ... répondre à des fins déterminées, les Etats 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 Chartre qu'est susceptible de comporter une telle conservation, seules la lutte contre la criminalité grave et, à fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence, à la condition que cette mesure ainsi que l'accès aux données ainsi conservées respectent les limites du strict nécessaire ...*

**L'arrêt du Conseil d'Etat du 21 avril 2021 (FRENCH DATA NETWORK EA)**

À la suite des précisions apportées par la CJUE, le Conseil d'État, statuant en Assemblée du contentieux, a examiné la conformité des règles françaises de conservation des données de connexion au droit européen.

Le Conseil d'Etat était saisi de moyens tendant à l'annulation, pour excès de pouvoir, du refus du Premier ministre d'abroger l'article R. 10-13 du Code des postes et des communications électroniques et du décret du 25 février 2011 permettant d'identifier toute personne ayant contribué à la création d'un contenu en ligne.

Il a jugé :

1) qu'est conforme au droit de l'Union européenne la conservation générale et indifférenciée des données relatives à l'identité civile, aux paiements, aux contrats et aux comptes de l'abonné ;2) qu'est également conforme au droit de l'Union européenne la conservation générale et indifférenciée des adresses IP attribuées à la source d'une connexion, mais uniquement pour la criminalité grave et la prévention des menaces graves à la sécurité publique en application du principe de proportionnalité, prévu à l'article préliminaire du code de procédure pénale, étant observé que **le rattachement d'une infraction pénale à la criminalité grave doit être apprécié par le juge de façon concrète** au regard des faits de l'espèce ;

3) que, **s'agissant de la conservation générale et indifférenciée des données de trafic et de localisation autres que les adresses IP, elle est justifiée aujourd'hui par l'objectif de sauvegarde de la sécurité nationale**, comme l'exige la CJUE :
* elle est justifiée par la menace grave et réelle, actuelle ou prévisible, à la sécurité nationale qu'est le terrorisme, mais aussi, l'espionnage, l'ingérence étrangère et «l'activité de groupes radicaux et extrémistes» (§ 44) ;
* elle impose néanmoins au gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace (§ 46)

4) qu'en revanche, est contraire au droit européen l'obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins autres que ceux de la sécurité nationale, notamment aux fins de lutte contre la criminalité, quel que soit le degré de gravité de cette criminalité.

Pour autant, le Conseil d'Etat constate successivement :
- que l'obligation de conservation est une condition déterminante du succès des enquêtes pénales et que les alternatives envisagées par la CJUE à la conservation généralisée et indifférenciée des données de connexion (conservation volontaire par les opérateurs, conservation ciblée, conservation rapide) ne permettent pas, par elles-mêmes, de garantir le respect des objectifs de valeur constitutionnelle précités (§ 50) ;
- que **la conservation «ciblée» des données n'est ni matériellement possible ni opérationnellement efficace** : en effet, il n'est pas possible de pré-déterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise (§ 53 et 54).

Il précise également que, lorsqu'est en cause une infraction grave, l'autorité judiciaire peut, sans méconnaître le droit européen, enjoindre aux opérateurs de communications électroniques, de procéder à la **conservation rapide** des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale. Autrement dit, lorsque les données ont été conservées de façon générale et indifférenciée pour les besoins de la sécurité nationale, celles qui concernent l'utilisateur en cause peuvent être mises à la disposition des services enquêteurs dans le cadre de la conservation rapide. Ainsi, **la sauvegarde de la**

**sécurité nationale justifie que soit conservées toutes les données, ce qui permet à la conservation rapide d'y pêcher tout ce dont elle a besoin**.

Ce sont là les considérations qui résultent de la motivation du Conseil d'Etat :

> *lorsqu'est en cause une infraction suffisamment grave pour justifier l'ingérence dans la vie privée induite par la conservation des données de connexion, dans le respect du principe de proportionnalité rappelé aux points 38 et 39, l'autorité judiciaire peut, sans méconnaître ni la directive du 12 juillet 2002, ni le RGPD, enjoindre aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de sites internet de procéder à la conservation rapide des données de trafic et de localisation qu'ils détiennent, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.*
> *Il résulte de ce qui précède que ni l'accès aux données de connexion conservées volontairement par les opérateurs, ni la possibilité de leur imposer une obligation de conservation ciblée, ni le recours à la technique de la conservation rapide ne permettent, par eux-mêmes, de garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales. Toutefois, d'une part, à la date de la présente décision, l'état des menaces pesant sur la sécurité nationale rappelées au point 44 justifie légalement que soit imposée aux opérateurs la conservation générale et indifférenciée des données de connexion. D'autre part, la conservation rapide des données susceptibles de contribuer à la recherche, la constatation et la poursuite des infractions pénales, dans le respect du principe de proportionnalité prévu par le code de procédure pénale conformément à ce qui a été rappelé au point 39, est possible dans les conditions prévues par la directive du 12 juillet 2002 et le RGPD, y compris, comme l'a jugé la Cour ainsi qu'il a été rappelé au point 55, lorsque cette conservation rapide porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. L'autorité judiciaire est donc en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie.*

Ainsi, pour le Conseil d'Etat, la conservation rapide peut porter, non seulement sur les données futures, mais aussi sur les données passées conservées de façon générale et indifférenciée pour les besoins de la sécurité nationale.

Si le Conseil d'Etat rappelle que la décision QUADRATURE DU NET interdit expressément au juge national de limiter dans le temps les effets d'une déclaration d'illégalité résultant d'une méconnaissance du cadre européen, il constate que le motif de sécurité nationale, qui permet de justifier la conservation générale des données de trafic et de localisation, était présent sur toute la période couverte par les dispositions critiquées et le demeure aujourd'hui (§ 96). Il ajoute que l'invalidation du texte réglementaire, en tant qu'il prévoit cette conservation pour d'autres finalités et ne comporte pas d'obligation de réexamen, n'implique ni la suppression de données passées ni la cessation de la conservation dans les mois qui viennent.

Au final, le Conseil d'Etat prononce la nullité des décisions du premier ministre refusant d'abroger l'article R 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, en tant que ces dispositions réglementaires, d'une part, ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation autres que les données d'identité civile, les coordonnées de contact et de paiement, les données relatives aux contrats et aux comptes et les adresses IP à la sauvegarde de la sécurité nationale et, d'autre part, ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

**L'application de ces principes au cas d'espèce soumis**

On rappellera qu'en l'espèce, les infractions en cause sont particulièrement graves puisqu'elles concernent un meurtre et une tentative de meurtre en bande organisée.

Si la procédure de conservation rapide permet de conserver régulièrement aux fins d'enquête sur des infractions graves les données de connexion initialement conservées à des fins de sécurité nationale, il reste que l'on peut se demander si la possibilité d'émettre des injonctions de conservation rapide aux fins d'enquête sur les infractions graves peut être fondée sur les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale.

A cet égard, le rapport explicatif de la Convention sur la cybercriminalité précise le point suivant :

> *158. L'article 16 vise à donner aux autorités nationales compétentes la possibilité d'ordonner ou d'obtenir par un moyen similaire la conservation rapide de données électroniques stockées spécifiées dans le cadre d'une enquête ou d'une procédure pénale spécifique. (...)*
> *160. La mention «ordonner ou ... obtenir par un moyen similaire» vise à autoriser la mise en oeuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction (de la police ou du parquet, par exemple). Dans certains états, le droit de procédure ne prévoit pas d'injonctions de conservation ; les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire. L'utilisation du membre de phrase «ou ... obtenir par un moyen similaire» introduit la souplesse voulue pour permettre à ces Etats d'appliquer cet article en mettant en oeuvre ces autres moyens.»*

Par ailleurs, le juge administratif a jugé que l'article R. 10-13 du CPCE était contraire au droit de l'Union en raison du caractère illimité dans le temps de l'injonction de conservation qu'il imposait. Peut-on admettre qu'un contrôle juridictionnel de l'existence de la menace à la sécurité nationale et de sa gravité au jour de la conservation des données permettrait de pallier le caractère pérenne de l'injonction ?

Enfin, la CJUE impose que la législation précise la ou les finalités pour laquelle une conservation rapide peut être ordonnée, et réponde à des critère objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi.

La chambre appréciera.

**SUR L'ACCES AUX DONNEES**

**Les normes de droit interne**

Le ministère public peut requérir la communication des données de trafic ou de localisation conservées par les opérateurs de télécommunications, soit en flagrance en vertu de l'article 60-2 du code de procédure pénale (ce qui est le cas dans notre espèce), soit en préliminaire en application des articles 77-1-1 et 77-1-2 du code de procédure pénale.

Le Conseil constitutionnel, saisi d'une QPC, a, dans une décision du 3 décembre 2021 (n°2021-952 QPC), censuré les articles 77-1-1 et 77-1-2 du code de procédure pénale :

*10. En permettant de requérir des informations issues d'un système informatique ou d'un traitement de données nominatives, les dispositions contestées autorisent ainsi le procureur de la République et les officiers et agents de police judiciaire à se faire communiquer des données de connexion ou à y avoir accès.*

*11. D'une part, les données de connexion comportent notamment les données relatives à l'identification des personnes, à leur localisation et à leurs contacts téléphoniques et numériques ainsi qu'aux services de communication au public en ligne qu'elles consultent. Compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée.*

*12. D'autre part, en application des dispositions contestées, la réquisition de ces données est autorisée dans le cadre d'une enquête préliminaire qui peut porter sur tout type d'infraction et qui n'est pas justifiée par l'urgence ni limitée dans le temps.*

*13. Si ces réquisitions sont soumises à l'autorisation du procureur de la République, magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, le législateur n'a assorti le recours aux réquisitions de données de connexion d'aucune autre garantie. 14. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la recherche des auteurs d'infractions.*

**La jurisprudence de la CJUE**

Les règles précisant les modalités d'accès, par les autorités publiques, aux données de connexion ont été précisées par l'arrêt PROKURATUUR du 2 mars 2021 (C-746/18K) :
- en 1er lieu, la législation nationale autorisant cet accès doit, pour satisfaire à l'exigence de proportionnalité, prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales : en particulier, elle ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette législation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation ; elle 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 en cause. À cet égard, un tel 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 ;
- en 2e lieu, l'accès ne peut être octroyé que pour autant que les données aient été conservées par les fournisseurs de services de communications électroniques de manière conforme au droit de l'Union européenne (§ 29) ;
- en 3e lieu, l'accès ne peut être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée (§ 31) ; l'accès à ces données ne peut en principe être justifié que par cette finalité ou une finalité « plus grave » ;
- en 4e lieu, l'accès aux données de trafic et de localisation présente par nature une ingérence grave, quelle que soit la durée de la période pour laquelle l'accès est sollicité, de la quantité ou de nature des données disponibles de sorte que cet accès doit être 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 (§ 39) ;
- en 5e lieu, l'accès doit être soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dotée d'un pouvoir contraignant ; la décision de cette juridiction ou de cette entité doit intervenir 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 (§ 51).

Dans cet arrêt, la CJUE, saisie de questions préjudicielles posées par la Cour suprême estonnienne, a dit pour droit :

*1) 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, du25 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.*

*2) L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1,de la charte des droits fondamentaux, 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.*

En ce qui concerne l'autorité chargée de délivrer l'autorisation d'accès aux données de trafic et de localisation, il est utile de reproduire ci-dessous les considérants 50 à 58 qui permettent de mieux appréhender la portée de l'arrêt du 2 mars 2021 :

*50. 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 peut être considéré comme étant 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 en cause. À cet égard, un tel 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. 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 (voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15,EU:C:2016:970, point 119, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18,C-512/18 et C-520/18, EU:C:2020:791, point 188).*

*51. 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 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.»*

On observera que dans l'arrêt du 5 avril 2022 «*Commissioner of the Gaarda Siochana* (C-140/20), la formulation est légèrement différente dans la mesure où elle ne paraît exiger la qualité de tiers, par rapport à l'autorité qui demande l'accès aux données, que de l'entité administrative indépendante.

« *108 : 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. Ainsi, l'exigence d'indépendance à laquelle doit satisfaire l'entité chargée d'exercer le contrôle préalable impose que celle-ci ait la qualité de tiers par rapport à l'autorité qui demande l'accès aux données, de sorte que ladite entité soit en mesure d'exercer ce contrôle de manière objective et impartiale, en étant protégée de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique 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 à l'égard des parties à la procédure pénale* ».

**L'application de ces principes au cas d'espèce soumis**

Le requérant met en cause l'accès, par les enquêteurs, à des données de connexion dans le cadre de l'enquête de flagrance au visa de l'article 60-1 du code de procédure pénale (requête en annulation p.18). De fait, les données relatives à l'une des lignes téléphoniques (XXXXXXXX 01; D505-509 selon la requête en nullité p.14) ont bien été recueillies en flagrance, antérieurement à l'intervention du réquisitoire introductif du 6 septembre 2019 (D577).

La chambre aura à se demander si l'arrêt PROKURATUUR, qui concerne le ministère public estonien, est transposable au ministère public français, étant observé que le statut de l'un et de l'autre sont très proches.

**SUR LA SANCTION DE LA MECONNAISSANCE EVENTUELLE DU DROIT EUROPEEN**

**La question du défaut de conformité de la jurisprudence de la CJUE à nos exigences constitutionnelles**

Le Conseil constitutionnel, lorsqu'il est saisi d'un grief d'inconstitutionnalité formulé à l'encontre de dispositions qui se bornent à transposer des textes communautaires, énonce qu'il *« n'est compétent pour contrôler la conformité des dispositions contestées aux droits et libertés que la Constitution garantit que dans la mesure où elles mettent en cause une règle ou un principe qui, ne trouvant pas de protection équivalente dans le droit de l'Union européenne, est inhérent à l'identité constitutionnelle de la France »* (V. Par ex. décision n°2021-966 QPC du 28 janvier 2022 : M. C. L. et autre [Exclusion de plein droit des procédures de passation des marchés publics et des contrats de concession]*)*.

Le Conseil d'Etat, dans sa décision du 21 avril 2021 concernant FRENCH DATA NETWORK rendue après question préjudicielle, a rappelé que la Constitution française demeure la norme suprême du droit national et a énoncé qu'il lui revient de vérifier que l'application du droit européen, tel que précisé par la CJUE, ne compromet pas, en pratique, des exigences constitutionnelles qui ne sont pas garanties de façon équivalente par le droit européen (V. Aussi *CE, 17 décembre 2021, n°437125, publié).*

On remarquera que jusqu'à présent, ni le Conseil d'Etat, ni le Conseil constitutionnel n'ont eu à faire primer des exigences constitutionnelles internes sur le droit de l'Union.

La CJUE, dans l'affaire C-430/21 du 22 février 2022 rendue en grand Chambre, a énoncé que :

> *« (…) Si une cour constitutionnelle d'un État membre estime qu'une disposition de droit dérivé de l'Union, telle qu'interprétée par la Cour, méconnaît l'obligation de respecter l'identité nationale de cet État membre, cette cour constitutionnelle doit surseoir à statuer et saisir la Cour d'une demande de décision préjudicielle, en vertu de l'article 267 TFUE, en vue d'apprécier la validité de cette disposition à la lumière de l'article 4, paragraphe 2, TUE, la Cour étant seule compétente pour constater l'invalidité d'un acte de l'Union (voir, en ce sens, arrêts du 22 octobre 1987, Foto-Frost, 314/85, EU:C:1987:452, point 20, ainsi que du 3 octobre 2013, Inuit Tapiriit Kanatami e.a./Parlement et Conseil, C 583/11 P, EU:C:2013:625, point 96) (…) ».*

Cette jurisprudence parait également s'appliquer à une cour suprême, qui serait alors pareillement tenue de saisir la CJUE d'une question préjudicielle.

**La question du défaut de conformité de notre législation nationale et le report des effets dans le temps**

Dans son arrêt LA QUADRATURE DU NET du 6 octobre 2020 (C 511/18, C 512/18 et C 520/18), la CJUE a expressément exclu une telle possibilité en énonçant :

*« Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux (...)».*

**La question du défaut de conformité de notre législation nationale et les principes du procès équitable**

Il résulte de la jurisprudence constante de la CJUE qu'en l'absence de règles de l'Union, 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 06/10/2020, LA QUADRATURE DU NET, C-511/18, C-512/18 et C-520/18,EU:C:2020:791, point 223).

Le principe d'autonomie procédurale est ainsi limité par les principes d'équivalence et d'effectivité.
Par ailleurs, la CJUE précise que « *le respect de ces deux principes doit être examiné en tenant compte de la place des règles concernées dans l'ensemble de la procédure, du déroulement de celle-ci et des particularités de ces règles devant les diverses instances nationales* ».

Le principe d'équivalence

Il ressort de la jurisprudence de la CJUE que le respect du principe d'équivalence suppose que la règle nationale en cause s'applique indifféremment aux recours fondés sur des droits que les justiciables tirent du droit de l'Union et à ceux fondés sur la méconnaissance du droit interne ayant un objet et une cause semblables. Il appartient au juge national, qui a une connaissance directe des modalités procédurales applicables, de vérifier la similitude des recours concernés sous l'angle de leur objet, de leur cause et de leurs éléments essentiels. Le principe d'équivalence se conçoit comme une obligation de non-discrimination procédurale du droit de l'Union par rapport au droit d'origine étatique.

Pour apprécier la conformité du droit national au principe d'équivalence, le juge doit, dans un premier temps, établir la comparabilité entre le recours destiné à assurer la sauvegarde du droit de l'Union et le recours fondé sur le droit interne. Dans un second temps, le juge doit s'assurer que les modalités qui régissent le recours fondé sur le droit interne ne sont pas plus favorables que celles s'appliquant aux recours fondés sur la violation du droit de l'Union.

Le principe d'effectivité

Selon la CJUE, chaque cas, dans lequel se pose la question de savoir si une disposition procédurale nationale rend impossible ou excessivement difficile l'application du droit communautaire, doit être analysé en tenant compte de la place de cette disposition dans l'ensemble de la procédure, de son déroulement et de ses particularités devant les diverses instances nationales.

Dans l'arrêt du 2 mars 2021 dit PROKURATUUR, qui complète d'ailleurs la portée de l'arrêt QUADRATURE DU NET en ajoutant une incise sur la problématique de l'accès aux données, la

CJUE a explicité le contenu de ce principe s'agissant tant de la conservation généralisée et indifférenciée des données que de leur accès :

*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, 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 etC-520/18, EU:C:2020:791, points 226 et 227).*

Ainsi, la CJUE retient que, dans le cadre d'une procédure pénale au cours de laquelle ont été versés des informations et des éléments de preuve obtenus au moyen d'une conservation généralisée et indifférenciée des données de trafic et de localisation contraire au droit de l'Union, ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, **le principe d'effectivité commande d'examiner le grief en résultant pour les requérants au regard du procès équitable**.

Dans l'arrêt QUADRATURE DU NET, la CJUE motive son argumentation en se référant à l'arrêt du 10 avril 2003, STEFFENSEN (C-276/01). Dans cet arrêt, la CJUE était notamment saisie d'une question préjudicielle portant sur le point de savoir si la juridiction nationale est tenue d'écarter un élément de preuve obtenu en violation du droit de l'Union, lequel imposait le droit d'en solliciter une contre-expertise.

En réponse à cette question, elle a synthétisé les principes posés par la Cour Européenne des droits de l'Homme, décrivant ainsi son mode de raisonnement :

*« 62. (...) il est constant que l'admissibilité des moyens de preuve dans une procédure (....) ne fait pas l'objet d'une réglementation communautaire.*
*63. Il en résulte que cette matière relève en principe du droit national applicable, sous réserve toutefois du respect des principes d'équivalence et d'effectivité au sens de la jurisprudence de la Cour rappelée au point 60 du présent arrêt. (...)*

*71. (...) dès lors que sont en cause le respect du droit à une contre-expertise garanti par le droit communautaire et les conséquences que pourrait avoir une violation de ce droit sur l'admissibilité d'un moyen de preuve dans le cadre d'un recours tel que celui en cause au principal, les règles nationales applicables en matière d'administration de la preuve entrent dans le champ d'application du droit communautaire. Partant, ces règles doivent respecter les exigences découlant des droits fondamentaux.*

*72. Il convient en l'espèce de prendre en considération, plus particulièrement, le droit à un procès équitable devant un tribunal, tel qu'énoncé à l'article 6, paragraphe 1, de la convention européenne des droits de l'homme et tel qu'interprété par la CEDH (...)*

*75. Il y a lieu d'indiquer, ensuite, qu'il découle de la jurisprudence de la CEDH, que l'article 6, paragraphe 1, de la CEDH ne réglemente pas le régime des preuves en tant que tel et que, partant, l'admissibilité d'une preuve recueillie sans respecter les prescriptions du droit national, ne peut pas être exclue par principe et in abstracto. Selon cette jurisprudence, il appartient au juge national d'apprécier les éléments de preuve obtenus par lui ainsi que la pertinence de ceux dont une partie souhaite la production.*

*76. Toutefois, selon cette même jurisprudence, le contrôle qu'exerce la CEDH, en vertu de l'article 6, paragraphe 1, de la convention européenne des droits de l'homme, sur le caractère équitable de la procédure — exigeant pour l'essentiel que les parties puissent participer de manière adéquate à la procédure devant la juridiction — concerne la procédure considérée dans son ensemble, y compris la manière dont la preuve a été administrée.*

*77. Il convient de relever, enfin, que la CEDH a jugé que, lorsque les parties concernées sont en droit de formuler, devant le tribunal, des observations sur un moyen de preuve,* ***il doit s'agir là d'une possibilité véritable de commenter efficacement celui-ci*** *pour que la procédure revête le caractère équitable exigé par l'article 6, paragraphe 1, de la Convention européenne des droits de l'homme. Une vérification de ce point s'impose en particulier lorsque le moyen de preuve ressortit à un domaine technique échappant à la connaissance des juges et est susceptible d'influencer de manière prépondérante l'appréciation des faits par le tribunal (voir arrêt Mantovanelli c. France, précité, § 36).*
*78. Il incombe à la juridiction de renvoi d'apprécier si, au vu de tous les éléments de fait et de droit à sa disposition, l'admission en tant que moyen de preuve des résultats d'analyses en cause au principal risque d'entraîner une violation du respect du contradictoire et, partant, du droit à un procès équitable. Dans le cadre de cette appréciation,* ***la juridiction de renvoi devra vérifier, plus particulièrement, si le moyen de preuve en cause au principal ressortit à un domaine technique échappant à la connaissance des juges et est susceptible d'influencer de manière prépondérante son appréciation des faits*** *et, dans le cas où il en serait ainsi, si M. S.. jouit encore d'une possibilité véritable de commenter efficacement ce moyen de preuve ».*

On constatera que cette décision ne traite pas du grief sous l'angle du respect de la vie privée (l'intéressé a-t-il subi, du fait de la conservation et de l'accès aux données de connexion une atteinte à sa vie privée ?), mais sous celui du procès équitable (la conservation et l'accès aux données de connexion ont-elle privé l'intéressé d'un procès équitable ?).

Notons que la CEDH a écarté la violation de l'article 6, pour l'utilisation, dans une procédure pénale :

- de l'interception à distance et l'enregistrement clandestin de conversations tenues dans un domicile privé par la police, au cours desquelles un individu a reconnu avoir commis un meurtre et son interlocuteur l'a rémunéré pour ce « service », dès lors qu'en l'espèce, aucune pression n'a été exercée sur l'auteur des faits pour reconnaître l'infraction et que l'enregistrement a eu une importance limitée dans l'ensemble complexe des éléments soumis au tribunal (Bykov c. Russie, précité) ;
- d'un enregistrement de conversations obtenu de manière illégale au regard du droit helvétique dès lors que dans l'affaire en cause, les droits de la défense n'ont pas été méconnus, l'intéressé ayant eu la possibilité de contester l'authenticité de la preuve *et « l'enregistrement téléphonique [n'avait] pas constitué le seul moyen de preuve retenu pour motiver la condamnation »* (12 juillet 1988, Schenk c. Suisse, Requête n°10862/84, §46 et suivants) ;
- de l'utilisation d'une bande audio recueillie de manière clandestine, *« seule preuve à la charge du requérant », « [constituant] un élément de preuve solide et ne [prêtant] à aucun doute* », le requérant ayant eu *« largement l'occasion de contester l'authenticité et l'emploi de l'enregistrement »* mais n'ayant combattu que l'utilisation de la preuve à l'audience, sans en contester l'authenticité (CEDH, 4 octobre 2000, Khan c. Royaume-Uni, requête n°35394/97, §§37 et 38).

Elle a décliné le même raisonnement pour écarter l'atteinte au caractère équitable de la procédure, dans une espèce où les juridictions prud'homales ont admis comme moyen de preuve, par l'employeur, des images issues d'une vidéo-surveillance, uniquement orientée vers des salariées suspectées de vol (CEDH, 17 oct. 2019, Lopez Ribalda, no 1874/13 et 8567/13, § 151).

**L'application de ces principes au cas d'espèce soumis**

Sur le principe d'effectivité

Le principe d'effectivité, tel que défini par la Cour de justice de l'Union européenne, peut être compris comme posant une exigence minimale : la personne dont les données personnelles de connexion ont été conservées ou communiquées aux autorités compétentes « *doit avoir été mis 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* ».

La chambre pourra se demander si la législation française n'offre pas une telle possibilité pour toute partie, dès lors que les articles 156 et suivants du code de procédure pénale ouvrent, durant le cours de l'information judiciaire, très largement le droit d'expertise, sous le contrôle du juge d'instruction, dès lors que « se pose une question d'ordre technique ». Rien ne parait faire obstacle à ce qu'une personne mise en examen sollicite une expertise sur les données de connexion qui lui sont attribuées.

Il pourrait en être déduit que le principe d'effectivité ne doit pas conduire à «écarter les informations et éléments de preuve obtenus par une conservation ou un accès contraire au droit de l'Union européenne.

Sur le principe d'équivalence

En application du principe d'équivalence, la question se pose de savoir si ce principe exige de prononcer la nullité des réquisitions et des informations obtenues en méconnaissance du droit de l'Union européenne, dès lors que les conditions du prononcé de la nullité en droit interne sont réunies.

Lorsque la chambre de l'instruction est saisie d'une requête en nullité, prise de la violation d'une disposition de droit interne, elle doit en prononcer la nullité de l'acte irrégulier si les conditions en sont réunies.

La chambre a ainsi censuré, au visa de l'article 6, § 3, de la Convention européenne des droits de l'homme, l'arrêt d'une chambre de l'instruction qui, pour rejeter le moyen pris de l'absence de notification à la personne gardée à vue de son droit au silence et à l'assistance d'un avocat, avait retenu que la nullité de la mise en examen ne pouvait être prononcée dès lors que les déclarations de l'intéressé n'avaient pas été le fondement exclusif ou essentiel de celle-ci. Il appartenait à la chambre de l'instruction d'annuler les auditions dont elle avait constaté l'irrégularité (Crim. 8 juill. 2015, n° 15-81.192).

En revanche, la chambre criminelle a exclu une telle solution, sur le fondement de la prévisibilité de la loi, dans l'hypothèse où l'acte critiqué était conforme au droit interne au jour de sa commission, mais s'est avéré contraire aux exigences conventionnelles de la FRANCE postérieurement à cette date.

Sur la nullité

Si la chambre juge que la nullité doit sanctionner la méconnaissance des exigences du droit de l'Union européenne, elle devra le faire selon la méthodologie propre aux nullités, telle qu'elle a été conceptualisée dans ses arrêts du 7 septembre 2021 (pourvoi n°21-80.642 et 20-97.191).

Il résulte de ceux-ci que, hors les cas de nullité d'ordre public, touchant à la bonne administration de la justice ou à la compétence, la chambre de l'instruction, saisie d'une requête en nullité, doit d'abord rechercher si le requérant a intérêt à demander l'annulation de l'acte, puis, s'il a qualité pour la demander et, enfin, si l'irrégularité alléguée lui a causé un grief.

**La chambre devra donc, avant tout, dire si l'accès à ces données de connexion de façon contraire au droit de l'Union constitue une nullité d'ordre public.**

Il résulte d'une jurisprudence ancienne que l'autorisation du procureur de la République pour requérir des experts en application de l'article 77-1 du code de procédure pénale a été édictée dans l'intérêt d'une bonne administration de la justice et que cette absence d'autorisation est constitutive d'une nullité à laquelle les dispositions de l'article 802 dudit code sont étrangères (Crim.14/10/2003, n°03-84.539, Bull 187). De même, un officier de police judiciaire ne peut, en enquête préliminaire, présenter des réquisitions prévues par l'article 77-1-1 du code de procédure pénale que s'il y est autorisé par le procureur de la République et la méconnaissance de cet impératif est aussi constitutive d'une nullité d'ordre public (Crim.01/09/2005, n°05-84.061, Bull 211 ; Crim.06/12/2005, n°05-85.076, Bull 319).

Mais un arrêt plus récent parait avoir abandonné cette position :

Crim.06/02/2018, n°17-84.380, Bull 30 (sommaire) : *«Un mis en examen n'est pas recevable à invoquer le défaut d'autorisation donnée par le procureur de la République, conformément à l'article 77-1-1 du code de procédure pénale, aux investigations tendant à obtenir le nom des titulaires de lignes téléphoniques, ainsi que ceux des numéros de téléphone ayant eu des échanges avec ladite ligne, dès lors qu'il ne conteste pas être ni le titulaire ni l'utilisateur de la ligne identifiée et ne prétend pas, à partir des pièces de la procédure soumises à l'examen de la chambre de l'instruction, qu'il aurait été porté atteinte, à l'occasion des investigations litigieuses, à sa vie privée. ... Un mis en examen n'est pas recevable à invoquer le défaut d'autorisation donnée par le procureur de la République, conformément à l'article 77-1-1 du code de procédure pénale, aux investigations ayant pour seul objet d'identifier les lignes téléphoniques ayant déclenché des bornes-relais données, dès lors qu'il ne prétend être ni le titulaire ni l'utilisateur de l'une des lignes identifiées et que sa vie privée n'est pas susceptible d'être mise en cause par cette recherche.»*

Il s'ensuit que, dans le dernier état de sa jurisprudence, la chambre a exclu que l'on soit en présence d'une nullité d'ordre public.

Si la chambre exclut que l'on soit en présence d'une nullité d'ordre public, elle devra s'interroger sur plusieurs points.

D'abord, sur la qualité à agir du requérant

Pour déterminer si le requérant a qualité pour agir en nullité, la chambre de l'instruction doit examiner si la formalité substantielle ou prescrite à peine de nullité, dont la méconnaissance est alléguée, a pour objet de préserver un droit ou un intérêt qui lui est propre. De façon désormais constante, la chambre applique cette solution dans des cas où est invoquée la violation du droit à la vie privée (cf. en dernier lieu : en matière de perquisition Crim., 9 novembre 2021, pourvoi n° 21-81.359 ; en matière de géolocalisation : Crim., 5 octobre 2021, pourvoi n° 21-83.219 ; en matière de consultaiton du LAPI : Crim., 5 octobre 2021, pourvoi n° 21-82.399 ; dispositif de captation d'images : Crim., 13 octobre 2020, pourvoi n° 19-87.959).

Ensuite, sur le grief allégué

La chambre juge que la violation d'une disposition de procédure n'est censurée par la nullité de l'acte que lorsque l'irrégularité *«a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne*» (article 171 et 802 du code de procédure pénale). Il en va ainsi tant des nullités

textuelles que des nullités dites substantielles (c'est ainsi que la méconnaissance des règles relatives aux perquisitions et aux saisies n'emporte pas systématiquement l'annulation de l'opération). Ce n'est que par exception que la chambre criminelle a adopté la théorie du grief nécessaire pour les irrégularités qui portent gravement atteinte à l'existence d'une justice équitable. Tel est le cas, par exemple, du dépassement de la durée légale de la garde à vue (voir Traité de procédure pénale de F. Desportes, 4e édition, n°2021).

La chambre devra apprécier le grief résultant de la conservation illicite des données ou d'un accès illicite à ces données, qu'elles aient été licitement ou non conservées.

On rappellera :

- qu'il appartient au requérant de justifier du grief ;
- que l'existence du grief est établie lorsque l'irrégularité elle-même a occasionné un préjudice au requérant, lequel ne peut résulter de la seule mise en cause de celui-ci par l'acte critiqué. (Crim., 7 septembre 2021, n°21-80.642 et 20-87.191, publiés au Bulletin).

Quant à la nature du grief, deux approches paraissent possibles :

- la première consiste à analyser le grief au regard de l'atteinte portée à la vie privée : elle devrait conduire à juger que la violation du droit de l'Union fait nécessairement grief à l'intéressé, ainsi qu'il a déjà été jugé :

> Crim.09/01/2018, n°17-82.946, Bull 4 (sommaire) : *«Dans la décision par laquelle le juge des libertés et de la détention, à la requête du procureur de la République, autorise, en application de l'article 706-95 du code de procédure pénale, l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques, la mention de la durée pour laquelle la mesure est autorisée constitue une garantie essentielle contre le risque d'une atteinte disproportionnée au droit au respect de la vie privée des personnes concernées, aux intérêts desquelles son absence porte nécessairement atteinte. Encourt en conséquence la censure l'arrêt qui, pour écarter le moyen de nullité tiré de l'absence de mention de la durée pour laquelle l'interception était ordonnée, se borne à retenir que le juge des libertés et de la détention a entendu autoriser celle-ci pour la période maximale prévue par la loi et que la mesure n'a pas été mise en oeuvre au-delà de cette durée, de sorte qu'il n'en est résulté aucun grief pour la personne écoutée.»*

- la seconde approche consiste à analyser le grief au seul regard du principe du procès équitable : cela reviendrait à tirer les conséquences des arrêts précités de la CJUE selon laquelle la règle de l'effectivité est respectée dès lors que le requérant est mis en mesure de commenter efficacement les informations et éléments de preuve obtenus en méconnaissance de ce droit (cf ci-dessus les commentaires relatifs au principe d'effectivité).

Ainsi qu'il a déjà été dit, la jurisprudence de la CJUE en matière de données de connexion caractérise le grief au regard du droit à un procès équitable.