COUR DE CASSATION

AVIS DE MME LABROUSSE, CONSEILLÈRE

Arrêt n° 771 du 12 juillet 2022 – Chambre criminelle

Pourvoi n° 21-83.820

Décision attaquée : Cour d'appel de Fort-de-France du 8 juin 2021

M. [F] [U]
C/

M. [F] [U] a formé un pourvoi contre l'arrêt de la chambre de l'instruction de la cour d'appel de Fort-de-France, en date du 8 juin 2021, qui, dans l'information suivie contre lui des chefs d'importation et exportation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants, associations de malfaiteurs, a prononcé sur sa demande d'annulation d'actes de la procédure.

1. RAPPEL DES FAITS ET DE LA PROCÉDURE

A la suite de l'interception dans les eaux territoriales du département de la Martinique d'une embarcation dans laquelle étaient découverts 78,5 kilogrammes de cocaïne, une information judiciaire était ouverte le 26 avril 2018 des chefs d'importation et exportation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants, associations de malfaiteurs.

Les nombreuses investigations sur commission rogatoire (interceptions téléphoniques, données de connexion, géolocalisations) mettaient en évidence de nouveaux faits d'importation de stupéfiants et d'association de malfaiteurs qui donnaient lieu à plusieurs réquisitoires supplétifs.

Le 7 février 2019, intervenait notamment une série de perquisitions permettant la saisie d'armes et de produits stupéfiants ainsi que plusieurs interpellations.

M. [V] [U], considéré par les enquêteurs comme l'organisateur du trafic de stupéfiants, était remis par les autorités saint-luciennes aux autorités judiciaires françaises, sur mandat d'arrêt, le 3 avril 2020 et mis en examen.

Le 4 novembre 2020, son frère, M. [F] [U], était interpellé.

Il était mis en examen le 6 novembre 2020 des chefs d'importation et exportations en bande organisée de stupéfiants, infractions à la législation sur les stupéfiants, associations de malfaiteurs en vue des crimes et délits précités, faits commis entre le 7 février 2019 et le 3 avril 2020.

Le 20 avril 2021, M. [F] [U] déposait une requête en nullité :

- de plusieurs actes coercitifs, pris de ce qu'ils auraient été diligentés pour des faits dont le juge d'instruction n'était pas saisi ;
- de ses auditions en garde à vue, prises de ce qu'elles auraient porté sur des faits postérieurs au 17 juin 2019 qui ne lui avaient pas été notifiés ;
- l'ensemble des procès-verbaux d'exploitation de facturations détaillées et de données géolocalisées, et notamment des actes suivants le concernant :

proc s-verbal d'exploitation de facturations détaillées et de données de géolocalisation du 26 novembre 2019 15 heures (D5757-D5758) ;

proc s-verbal d'exploitation de facturations détaillées et de données de géolocalisation du 28 novembre 2019 8 heures (D5767-D5768) ;

proc s-verbal d'exploitation de facturations détaillées et de données de géolocalisation du 28 novembre 2019 15 heures (D5774-D5775) ;

proc s-verbal d'identification de la ligne 17587332918 du 5 février 2019 (D5816-D5819).

Par l'arrêt attaqué, en date du 8 juin 2019, la chambre de l'instruction déclarait la requête en nullité recevable et la rejetait.

Par déclaration par avocat en date du 14 juin 2021, M.[U] s'est régulièrement pourvu en cassation.

Le 24 juin 2021, la SCP Thouvenin, Coudray et Grévy s'est constituée en demande.

Par ordonnance en date du 13 septembre 2021, le président de la chambre criminelle a ordonné l'examen immédiat du pourvoi.

Le 4 octobre 2021, la SCP précitée a déposé un mémoire ampliatif pour le demandeur.

2. ANALYSE SUCCINCTE DES MOYENS

TROIS MOYENS SONT PROPOSES

Le premier moyen, en trois branches, fait grief à l'arrêt d'avoir rejeté sa requête en nullité des actes coercitifs dépassant les limites de la saisine du juge d'instruction alors que :

1. en n'expliquant pas en quoi la mise en évidence des nouvelles infractions l'avait été dans le cadre de la recherche des auteurs des infractions dont le juge d'instruction était saisi et quand il résultait de ses propres constatations que de nouvelles infractions d'importation de stupéfiants avaient été constatées partir du 22 juin 2018 et jusqu'au 7 février 2019, sans faire l'objet d'un réquisitoire supplétif d s la mise en évidence des indices les concernant, la chambre de l'instruction a privé sa décision de base légale, au regard des articles 80 et 152 du code de procédure pénale ;

2. dès lors qu'elle affirmait que le mis en examen aurait repris le trafic qui était visé par les réquisitoires introductifs et supplétifs portant sur les faits commis jusqu'au 7 février 2019, visant ainsi des infractions qui n'étaient pas le simple prolongement de celles dont le magistrat instructeur était saisi, par les réquisitoires établis jusqu'au 7 février 2019, la chambre de l'instruction a violé les articles 80 et 152 du code de procédure pénale ;

3. dès lors que le blanchiment n'était pas visé parmi les faits dont était saisi le magistrat instructeur, avant les écoutes des lignes attribuées au mis en examen et son placement en garde vue, ce qui établissait que ces mesures coercitives portaient sur des faits distincts de ceux dont le magistrat instructeur était saisi, la chambre de l'instruction a encore méconnu les articles 80 et 152 du code de procédure pénale.

Le deuxième moyen, en une branche unique, fait grief à l'arrêt attaqué d'avoir rejeté sa requête en nullité des procès-verbaux de ses auditions en garde à vue alors que l'omission, dans la notification à la personne gardée à vue, prévue à l'article 63-1 du code de procédure pénale, d'une infraction qu'elle est soupçonnée d'avoir commise ou tenté de commettre doit entraîner le prononcé d'une nullité s'il en est résulté pour elle une atteinte effective à ses intérêts ; dès lors, faute d'avoir recherché si le fait de l'avoir interrogé sur les enregistrements téléphoniques, portant sur une ligne téléphonique, dont il niait être le titulaire, pour l'amener à reconnaitre que la voix des enregistrements était la sienne, ce qu'il n'a pas nié, n'impliquait pas qu'ainsi le mis en examen s'incriminait, la chambre de l'instruction a privé sa décision de base légale, en violation des articles 198 et 593 du code de procédure pénale.

Le troisième moyen, en quatre branches, fait grief à l'arrêt attaqué d'avoir rejeté sa requête en nullité portant sur les réquisitions des enquêteurs portant sur les données de trafic et de localisation de la téléphonie et les actes d'exploitation de ces données alors que :

1. l'article 15, paragraphe 1 de la directive 2002/58/CE 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, 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, s'oppose à des mesures législatives prévoyant, aux fins de protection de la sécurité nationale ou de lutte contre les infractions graves, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation des communications par les fournisseurs des services de communication électronique ; en considérant que le trafic de stupéfiants entrait dans la catégorie des infractions graves justifiant un stockage massif et indifférencié des données de trafic et de localisation gérées par les fournisseurs de communication électronique dans les conditions prévues par l'article 15 de la directive 2002/58, quand les articles L. 34-1, II et R. 10-13 du code des postes et des télécommunications n'ont précisé ni quelles infractions graves justifiaient une obligation de conservation, ni les catégories de données à conserver, ni les personnes concernées, ni les autorités habilitées à définir les cas dans lesquels ce stockage s'impose, la chambre de l'instruction a méconnu l'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52 de la Charte des droits fondamentaux de l'Union européenne et 88-1 de la Constitution ;

2. en estimant que la conservation en vue de leur exploitation dans le cadre des enquêtes pénales des données de trafic et de localisation des utilisateurs des moyens de communication électroniques était justifiée pour la recherche des infractions graves, quand le législateur n'a pas défini les catégories d'infractions graves justifiant une telle ingérence, ni l'autorité habilitée à se prononcer sur l'obligation de conserver de telles données, la cour d'appel a violé l'article 8, §2, de la Convention européenne de sauvegarde des droits de l'homme ;

3. en vertu de l'article 15 de la directive 2002/52/CE de la directive 2002/58/CE 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, les données de trafic et de localisation ne peuvent être exploitées que pour la fin qui a autorisé la conservation ; qu'en se référant à l'arrêt du Conseil d'Etat du 21 avril 2021, ayant jugé que l'obligation de conservation des données de connexion et de localisation pendant un an prévue par la législation et la réglementation nationale, était justifiée par les impératifs de protection de la sécurité nationale que constitue la lutte contre le terrorisme, conservation pourtant non subordonnée à une autorisation d'une juridiction ou d'une autorité indépendante, la chambre de l'instruction, qui a jugé que l'accès à ces données par les enquêteurs agissant sur commission rogatoire était justifié dans le cadre de la recherche des auteurs des infractions visées aux poursuites, pourtant sans lien avec le terrorisme, a violé l'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52 de la Charte des droits fondamentaux de l'Union européenne ;

4. en vertu de l'article 15 de la directive 2002/58/CE du 12 juillet 2002, l'accès des autorités nationales compétentes aux données de trafic et de localisation

conservées est subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative, tiers par rapport à l'autorité de poursuite, et à la condition que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de cette autorité de poursuite ; que, par ailleurs, en vertu de l'article 8, paragraphe 2, de la Convention européenne de sauvegarde des droits de l'homme, l'exploitation de données de trafic et de connexion pour les besoins d'une enquête répressive ne peut intervenir que sur décision d'un juge indépendant et impartial ; que, dans son mémoire, le mis en examen contestait l'accès par les enquêteurs, agissant sur commission rogatoire, aux données de trafic et de localisation concernant différentes personnes, conservées par les fournisseurs de communication électronique, en ce que cet accès n'avait pas été autorisé par une juridiction ; que la chambre de l'instruction qui ne s'est pas prononcée sur ce moyen de nullité, a privé sa décision de base légale en violation des articles 198 et 593 du code de procédure pénale.

Dans le corps du mémoire (p.41), il est mentionné que pourrait être posée à la Cour de justice de l'Union européenne la question préjudicielle suivante :

« (...) qu'elle détermine si la France peut continuer à appliquer en matière de recherche des infractions en cause en l'espèce, de leur preuve et de leurs auteurs :
- l'exploitation des données de connexion et de localisation conservées par les opérateurs de téléphonie, dans les conditions prévues par l'article L. 34-1 du code des postes et télécommunication électroniques ;
- la faculté pour les enquêteurs de demander, sans autorisation d'un juge, communication de telles informations (voir infra) ;
Et qu'elle détermine également :
- quelles qualités doit présenter le juge appelé à autoriser les enquêteurs à solliciter l'accès à de telles données ;
- si la législation nationale n'étant pas conforme aux exigences de l'article 15 de la directive n°2002/58/CE, il est possible de reporter les effets de son annulation, lorsqu'un juge peut intervenir a posteriori pour contrôler les conditions dans lesquelles les données de connexion et de localisation ont été exploitées ».

3. DISCUSSION

Sur le premier moyen relatif à la saisine du juge d'instruction : proposition de non-admission

Devant la chambre de l'instruction, M. [U] a fait valoir la nullité de plusieurs actes coercitifs (notamment les interceptions de lignes qui lui étaient attribuées ou l'étaient à des tiers, son interpellation, la perquisition de son domicile et enfin l'intégralité de sa garde à vue) en exposant qu'ils avaient été diligentés hors saisine du juge d'instruction, telle qu'elle était délimitée par les réquisitoires introductif du 26 avril 2018 et supplétifs des 7 et 8 février 2019 et 20 juin 2019.

***

Il résulte de l'article 80, alinéa 1er du code de procédure pénale que « *le juge d'instruction ne peut informer qu'en vertu d'un réquisitoire du procureur de la République* », lequel peut être pris contre personnes dénommées ou non dénommées (alinéa 2 du même texte).

Le troisième alinéa du même article ajoute que « *lorsque des faits, non visés au réquisitoire, sont portés à la connaissance du juge d'instruction, celui-ci doit immédiatement communiquer au procureur de la République les plaintes ou les procès-verbaux qui les constatent* ».

La chambre juge que « *le juge d'instruction peut avant toute communication au Procureur de la République, consigner la substance des faits nouveaux dans un procès-verbal et, le cas échéant, effectuer d'urgence les vérifications sommaires pour en apprécier la vraisemblance, mais il ne peut sans excéder ses pouvoirs, procéder à des actes qui, présentant un caractère coercitif, exigeant la mise en mouvement de l'action publique* » (Crim., 6 février 1996, pourvoi n° 95-84.041, Bull. Crim, 1996, n° 60).

Elle juge également que n'encourt pas la nullité les actes coercitifs, à l'occasion desquels sont progressivement apparus des indices de commission de faits nouveaux, lorsqu'ils ont été mis en oeuvre régulièrement pour établir les délits dont le juge d'instruction était saisi (Crim., 7 janvier 2020, pourvoi n° 19-83.606 - Crim., 21 février 2017, pourvoi n° 16-85.542).

Ainsi, par arrêt en date du 24 juin 2015, dans une affaire de vols aggravés et recels multiples, la chambre a jugé « *que les moyens coercitifs, à l'occasion desquels étaient apparus les indices de la commission de faits nouveaux, avaient été mis en oeuvre régulièrement pour établir le degré de participation des autres personnes soupçonnées des délits dont le juge d'instruction était saisi et dont les faits découverts étaient le prolongement, s'agissant d'un mode opératoire identique qui se traduisait par des infractions successives, étroitement liées aux précédentes* », en sorte que le magistrat instructeur n'avait pas excédé sa saisine (Crim., 24 juin 2015, n°14-86.817).

De même, par arrêt en date du 6 mai 2014, la chambre a approuvé la chambre de l'instruction d'avoir écarté le moyen de nullité pris de la violation des limites de la saisine initiale du juge d'instruction par le recours à une interception téléphonique afin d'établir des faits nouveaux de commerce illicite de produits stupéfiants, dès lors que les interceptions téléphoniques ayant révélé les indices de la commission de faits nouveaux avaient été mis en oeuvre régulièrement pour établir l'existence de délits entrant dans la saisine initiale du juge d'instruction des chefs de direction et d'organisation d'un groupement ayant pour objet une activité illicite liée aux stupéfiants et d'importation de ces produits en bande organisée, dont ils étaient le prolongement (Crim., 6 mai 2014, pourvoi n° 13-88.597).

De même dans une procédure où les requérants soutenaient que les enquêteurs agissant dans le cadre d'une commission rogatoire portant sur un trafic de stupéfiants ne pouvait exploiter les écoutes téléphoniques faisant apparaître d'éventuels faits de corruption, trafic d'influence et violation du secret professionnel, la chambre a énoncé que « *ne saurait constituer un acte coercitif*

irrégulier ni la poursuite des écoutes téléphoniques légalement ordonnées dans l'information initiale ni la transcription des conversations interceptées, même si elle révèlent la commission d'infractions dont le juge d'instruction n'a pas été antérieurement saisi » (Crim., 31 octobre 2012, pourvoi n° 12-84.220).

Ainsi, les actes coercitifs ne sont légaux que pour autant qu'ils ont pour objet de caractériser les faits dont le juge d'instruction est saisi mais, si tel est le cas, peu importe qu'ils révèlent également des faits nouveaux extérieurs à la saisine de celui-ci.

En l'espèce, l'information judiciaire a été ouverte par réquisitoire introductif en date du 26 avril 2018 (D48), des chefs d'importation et exportation de stupéfiants, infractions à la législation sur les stupéfiants, association de malfaiteurs, faits commis entre le 1er janvier 2018 et le 22 avril 2018.

Ce réquisitoire introductif a été suivi de plusieurs réquisitoires supplétifs :

- des 7et 8 février 2019, pour des faits d'infractions à la législation sur les armes, associations de malfaiteurs, commis entre le 23 avril 2018 et le 7 février 2019 (D87, D94) ;
- du 13 mars 2019, des chefs d'infractions à la législation sur les armes, association de malfaiteurs (D1079) ;
- du 20 juin 2019, pour des faits d'association de malfaiteurs, commis entre le 8 février 2019 et le 17 juin 2019 (D1375).

M. [V] [U] a été interpellé le 3 avril 2020 par les autorités saint-luciennes et remis aux autorités françaises le jour même.

Après des interceptions téléphoniques, faisant notamment apparaître qu'il avait été sollicité par son frère [V], qui se trouvait alors en fuite, pour gérer des transactions d'argent et de produits stupéfiants, M.[F] [U] a été interpellé le 4 novembre 2020.

Un réquisitoire supplétif du 6 novembre 2020 (D6077) a été délivré contre M. [F] [U] des chefs d'importation et exportation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants, blanchiment de produits stupéfiants, association de malfaiteurs en vue de la commission des crimes et délits précités, faits commis entre le 7 février 2019 et le 3 avril 2020.

M. [F] [U] a été mis en examen pour les faits visés au réquisitoire supplétif, excepté le blanchiment.

Pour ne pas faire droit à la nullité, la chambre de l'instruction, après avoir rappelé la chronologie précitée de la procédure, énonce :

> « *Cette instruction JIRS a été initiée à la suite de la saisine de plus de 78 kgs de cocaïne jetés d'un bateau provenant de [Localité 1], l'un des occupants étant de nationalité vénézulienne.*
> *Le réquisitoire introductif visant un trafic de stupéfiants, l'importation et l'exportation en bande organisée étant spécifiquement visées, tout comme l'association de malfaiteurs,* ***il appartenait au magistrat instructeur d'investiguer sur tout le trafic, sur l'organisation mise en place, d'en déterminer l'ampleur, d'en***

identifier les auteurs, le rôle de chacun *(commanditaires, fournisseurs, passeurs, logisticiens),* ***les filières d'approvisionnement****.*
Les moyens coercitifs à l'occasion desquels sont apparus les indices de la commission de faits nouveaux ont été mis en oeuvre régulièrement pour établir les infractions criminelles et délictuelles dont le magistrat instructeur était saisi et dont ils étaient strictement le prolongement*.*
Le fait que ces mesures ***aient permis de révéler la poursuite du trafic*** *auquel [V]* [S] *[T] avait participé et* ***conduit à l'identification de [F] [U] qui était impliqué dans le trafic dont le juge d'instruction était saisi*** *ne constitue pas une cause de nullité de ces mesures et ce d'autant plus que le magistrat instructeur a informé à plusieurs reprises le procureur de la République de la poursuite des faits dont il a ensuite été saisi par des réquisitoires supplétifs ».*

Sur la 1er branche, on observera que la chambre de l'instruction a énoncé que les actes coercitifs critiqués visaient à établir les faits d'association de malfaiteurs et de trafic de stupéfiants, dont le juge d'instruction avait été intialement saisi, en recherchant les membres participants, le mode d'organisation de ce trafic, son ampleur, et que c'est lors de la mise en oeuvre de ces moyens coercitifs, destinés à établir la preuve des infractions précitées, que, concomitamment, a été rapportée la preuve des nouveaux délits d'importation de produits stupéfiants. La 1ère branche du moyen parait dès lors ne pouvoir être admise.

S'agissant des 2ième et 3ième branche, le même raisonnement peut être fait s'agissant des infractions de trafic de stupéfiants et blanchiment révélés lors de la poursuite des actes d'investigation relatifs à cette même association de malfaiteurs, pour laquelle la saisine du juge d'instruction avait été étendue par supplétif du 20 juin 2019, étant précisé que M.[F] [U] n'a pas été mis en examen du chef de blanchiment.

En conséquence, les 2ième et 3ième branches du moyen paraissent ne pas pouvoir être admises.

Dès lors, le premier moyen parait ne pas pouvoir être admis, en application de l'article 567-1-1 du code de procédure pénale.

Sur le deuxième moyen relatif aux auditions en garde à vue : proposition de non-admission

En vertu de l'article 6, 3, a) de la Convention européenne de sauvegarde des droits de l'homme, l' « accusé » doit être informé de manière détaillée, de la nature et de la cause de l'accusation portée contre lui. Ce droit s'applique à la notification des faits reprochés à l'occasion d'une garde à vue.

L'article 63-1 2° du code de procédure pénale dispose que toute personne placée en garde à vue doit être informée « *2° de la qualification, de la date et du lieu présumés de l'infraction qu'elle est soupçonnée d'avoir commise ou tenté de commettre ainsi que des motifs mentionnés aux 1° et 6° de l'article 62-2 justifiant son placement en garde à vue* ».

La chambre juge que l'omission, dans la notification à la personne gardée à vue prévue à l'article 63-1 du code de procédure pénale, d'une partie des faits qu'elle est soupçonnée d'avoir commis ou tenté de commettre ne peut entraîner le prononcé d'une nullité que s'il en est résulté pour elle une atteinte effective à ses intérêts. Une telle atteinte ne se trouve pas caractérisée lorsque, en répondant aux questions des enquêteurs, le demandeur n'a tenu aucun propos par lequel il s'est incriminé. Il appartient à la Cour de cassation, qui a le contrôle des pièces de la procédure, de vérifier si tel est le cas (Crim., 2 novembre 2016, pourvoi n° 16-81.716, Bull. crim. 2016, n° 281 ; Crim., 31 octobre 2017, pourvoi n° 17-81.842, Bull. crim. 2017, n° 238 - cf : même solution en cas d'omission du lieu de commission de l'infraction : Crim., 27 mai 2015, pourvoi n° 15-81.142, Bull. crim. 2015, n° 126).

En l'espèce, pour ne pas faire droit au moyen de nullité pris de ce que M. [U] avait été entendu en garde à vue sur des faits qui ne lui avaient pas été notifiés, la chambre de l'instruction, après avoir relevé qu'il avait effectivement été interrogé « *sur une période postérieure à la période de prévention susvisée* » a énoncé que :

- « *les questions ainsi posées dans le cadre de sa garde à vue avaient pour objectif de matérialiser sa participation au trafic initial, à cerner sa participation et à identifier d'autres mis en cause* » ;
- « *au surplus, ce dernier ne s'est pas auto-incriminé en ce qu'il a nié toute participation aux infractions dont est saisi le magistrat instructeur* ».

Le moyen ne parait pas pouvoir être admis, au sens de l'article 567-1-1 du code de procédure pénale, pour les raisons suivantes :

- d'une part, le moyen apparaît inopérant en ce qu'il ne critique qu'une motivation surabondante de l'arrêt et non la motivation énoncée à titre principal, à savoir que les questions posées avaient pour objet de caractériser la participation de l'interessé aux faits d'infractions à la législation sur les stupéfiants et d'associations de malfaiteurs qui lui avaient été préalablement notifiées ;

- d'autre part, il résulte des procès-verbaux d'audition de l'intéressé que, si celui-ci, lors de sa quatrième audition, après avoir écouté deux échantillons de voix captées sur les interceptions judiciaires, a répondu « *c'est bien ma voix* » pour celle interceptée sur la ligne ouverte à son nom, il a précisé, s'agissant de la seconde, correspondant à la ligne pouvant servir au trafic de stupéfiants, « *cela ressemble bien à ma voix, oui* » avant d'ajouter « *je n'ai rien à dire* ». Interrogé sur ces déclarations, lors d'une audition ultérieure, il a ajouté « *non, je n'ai jamais dit que les deux c'étaient moi, je vous ai dit que la seconde voix ressemblait à la mienne mais ce n'est pas ma voix* ». Dès lors, de telles déclarations n'apparaissent pas incriminantes, et ce d'autant que durant ses auditions en garde à vue, l'intéressé a nié toute participation aux faits.

Sur le troisième moyen, relatif aux données de connexion

Le moyen est pris en ses différentes branches de la violation de :

> l'article 15, § 1er de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite directive « vie privée et communications électroniques, lu la lumière des articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, protégeant respectivement le droit au respect de la vie privée et familiale, le droit la protection des données caractère personnel et la liberté d'expression, ainsi que de l'article 52, § 1er relatif la portée et l'interprétation des droits et principes consacrés par ladite Charte ;
>
> l'article 8 de la Convention européenne des droits de l'homme.

Il repose explicitement, en ses 1ère, 3ième et 4ième branches, sur l'interprétation des normes de droit européen précitées par la Cour de justice de l'Union européenne dans les arrêts dits « La Quadrature du Net »[1] du 6 octobre 2020 et « Prokuratuur »[2] du 2 mars 2021 relatifs à la conformité des réglementations adoptées par certains Etats membres, dont la France[3], prévoyant une obligation pour les fournisseurs de services de communications électroniques, d'une part, de conserver de manière généralisée ou indifférenciée les données des utilisateurs à des fins de lutte contre les infractions pénales, d'autre part, de les transmettre, à cette fin, à leur demande, aux autorités compétentes.

La première branche du moyen soutient que droit interne français est contraire aux exigences de l'Union européenne dès lors qu'il n'encadre pas suffisamment la possibilité de conserver les données de trafic et de localisation aux fins de lutte contre la criminalité grave.

La deuxième branche du moyen reprend la même argumentation mais au regard de l'article 8 de la Convention européenne des droits de l'homme.

La troisième branche critique l'arrêt du Conseil d'Etat du 21 avril 2021 « French Data Network », rendu suite à l'arrêt « La Quadrature du Net » de la Cour de justice de l'Union européenne, en ce qu'il a jugé que l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation était justifiée par les impératifs de protection de la sécurité nationale alors même que cette conservation n'a pas fait l'objet d'une autorisation d'une juridiction ou d'une autorité administrative indépendante. Il soutient également que l'exploitation des données ainsi conservées ne peut l'être que pour la fin qui a autorisé leur conservation et donc pas pour la criminalité grave.

---

[1] CJUE,arrêt du 20 octobre 2020, La Quadrature du Net, C-511/18, C-512/18 et C-520/18

[2] [4] CJUE,arrêt du 2 mars 2021, Prokuratuur, C-746/18

[3] la question préjudicielle dans l'affaire C-512/18 a été posée par le Conseil d'Etat français (CE, 26 juillet 2018, n°393099).

La dernière branche reproche à la chambre de l'instruction de ne pas avoir répondu à l'argumentation de la personne mise en examen selon laquelle le juge d'instruction français ne constituait pas « *un juge indépendant et impartial* » pouvant autoriser l'accès aux données de connexion.

Plan du rapport :

1. La conservation des données : 1ère , 2ième et 3ième branches

1.1 : les normes applicables

1.1.1 : les normes de droit interne
l'article L. 34-1 du CPCE
l'article R. 10-13 du CPCE
la déclaration d'inconstitutionnalité de l'article L. 34-1 précité.

1.1.2 : le droit de l'Union
la Charte des droits fondamentaux
la directive 2002/58/CE
le RGPD

1.1.3 : l'article 8 de la Convention européenne des droits de l'homme

1.2 : la jurisprudence de la Cour de justice de l'Union européenne

1.2.1 : les arrêts Quadrature du Net et Prokuratuur
la prohibition de la conservation générale et indifférenciée des données de connexion ;
la conservation des données aux fins de lutte contre la criminalité grave

1.2.2 : la conservation dite « rapide » des données de connexion
un apport de l'arr t « La Quadrature du Net »
le fondement : la Convention de Budapest sur la cybercriminalité

1.2.3 : précisions apportées par l'arrêt Commissioner of the Garda Siochana du 5 avril 2022 (C- 140/20)

1.3 : l'arrêt « French Data Network » du 21 avril 2021 du Conseil d'Etat

1.4 : examen des trois premières branches du moyen

1.4.1 : la motivation de la chambre de l'instruction
1.4.2 : l'argumentation du moyen

1.4.3 : analyse

2. L'accès aux données : 4ième branche

2.1 : les normes de droit interne

2.1.1 : les articles pertinents

2.1.2 : la déclaration d'inconstitutionnalité des articles 77-1-1 et 77-1-2 du code de procédure pénale

2.2 : la jurisprudence de la Cour de justice de l'Union européenne

2.3 : examen de la 4ième branche du moyen

2.3.1 : la motivation de la chambre de l'instruction

2.3.2 : l'argumentation du moyen

2.3.3 : analyse du moyen

3. La sanction de la méconnaissance du droit européen

3.1 : la question du défaut de conformité de la jurisprudence de la Cour de justice de l'Union européenne aux exigences constitutionnelles

3.2 : La prohibition de la limitation dans le temps des effets de la déclaration d'inconventionnalité

3.3 : le principe d'autonomie procédurale et son encadrement

3.3.1 : le principe d'équivalence

3.3.2 : le principe d'effectivité : l'exigence du procès équitable
l'exigence de pouvoir commenter les éléments de preuve obtenus
illustrations par la jurisprudence de la Convention européenne des droits de l'homme

3.4 : analyse de la 4ième branche

3.4.1 : la conformité de la législation au principe d'effectivité

3.4.2 : le principe d'équivalence commande-t-il le prononcé de la nullité ?
l'inopposabilité des données de connexion : une sanction transitoire se substituant au prononcé de la nullité
la prévisibilité des exigences de droit européen : quelle date retenir ?

3.4.3 : les conditions du prononcé de la nullité
nullité d'ordre public ou de droit privé ?
qualité agir
quel grief ?

1. La conservation des données de connexion : 1ère, 2ième et 3ième branches

Rappels terminologiques :

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 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 identifié et d'obtenir la liste des appels ayant borné à la même antenne relais.

> La chambre distingue parmi les géolocalisations mises en oeuvre par la police judiciaire, celles qui, accomplies en temps réel pour suivi dynamique d'un mis en cause, sont régies par les dispositions des articles 230-32 et suivants du code de procédure pénale et celles qui, réalisées en temps différé pour reconstitution ultérieure de son parcours, sont exécutées sur le fondement de réquisitions du procureur de la République ou du juge d'instruction (Crim., 2 novembre 2016, pourvoi n° 16-82.376, Bull. crim. 2016, n° 282). Seules sont en cause dans le présent pourvoi ces derni res.

1.1 : les normes

1.1.1 : les normes de droit interne

Le moyen conteste la conformité au droit de l'Union européenne des articles L. 34-1 et R. 10-13 du CPCE, dans leur version en vigueur à la date des faits.

> l'article L.34-1 du CPCE dans sa version applicable la date des faits, soit du 20 décembre 2013 au 31 juillet 2021[4]

En son paragraphe II, cet article fait obligation aux opérateurs de services de communications électroniques d'effacer ou de rendre anonyme toute donnée relative au trafic, sous réserve des dispositions des paragraphes III à VI du même article.

Les données relatives au trafic au sens de ces dispositions sont définies par le 18° de l'article L. 32 du même code comme « *toutes les données traitées en vue*

4

résultant de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation », ce qui inclut les données d'identité, de localisation et de trafic stricto-sensu, comme précédemment définies.

Deux exceptions sont néanmoins prévues à l'obligation d'effacement ou d'anonymisation :

- d'une part, le paragraphe III prévoit qu'il « *peut être différé* » aux opérations d'effacement ou d'anonymisation de « *certaines catégories de données techniques* », pour une durée maximale d'un an, notamment « *pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales* » ; loin de poser une simple faculté, ce paragraphe crée une **véritable obligation de conservation à la charge des opérateurs**, sanctionnée par le délit de non-conservation des données de connexion[5] ; par ailleurs, le paragraphe IV de cet article précise que les données conservées et traitées dans les conditions définies au III portent excusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées.

- 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 un an ou jusqu'à la fin des poursuites engagées, le cas échéant.

A la suite de l'arrêt précité rendu par la Cour de justice de l'Union européenne dans la procédure « La Quadrature du Net », la rédaction de cet article a été modifiée par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

l'article R. 10-13 du CPCE

Cet article, pris pour l'application de l'article L. 34-1 précité, énumère les données qui doivent être conservées, pour une durée d'un an à compter du jour de leur enregistrement, par les opérateurs de communications électroniques aux fins mentionnées d'une part de la recherche, de la constatation et de la poursuite des infractions, notamment pénales, d'autre part, des missions de défense et promotion des intérêts fondamentaux de la Nation confiées aux services de renseignement.

Sont concernées par cette obligation :

« *a) Les informations permettant d'identifier l'utilisateur ;*

5

Le 2° de l'article L. 39-3 du code des postes et des communications électroniques punit en effet d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents de ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

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 données 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.

Ainsi, il résulte des articles L. 34-1 et R. 10-13 du CPCE, dans leur version à la date des faits, que les opérateurs de services de communications électroniques avaient 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 pénales, dans les conditions et limites fixées par la loi et les dispositions réglementaires prises pour son application.

la déclaration d'inconstitutionnalité de l'article L. 34-1 du CPCE

Le Conseil constitutionnel a été saisi par la Cour de cassation d'une QPC relative à la conformité aux droits et libertés que la Constitution garantit des paragraphes II et III de l'article L. 34-1 du code des postes et des communications électroniques dans leur version antérieure à leur modification par la loi n° 2021-998 du 30 juillet 2021.

Dans sa décision n° 2021-976/977 QPC du 25 février 2022, il a jugé que les dispositions contestées étaient contraires à la Constitution dès lors qu'elles portaient une **atteinte disproportionnée au droit au respect de la vie privée**, au terme du raisonnement suivant.

Le Conseil constitutionnel a constaté que, en adoptant les dispositions contestées, le législateur avait poursuivi les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions.

Néanmoins, il a relevé successivement que :

- compte tenu de leur nature, de leur diversité et des traitements dont elles pouvaient faire l'objet, les données conservées fournissaient sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée ;

- une telle conservation s'appliquait de façon générale à tous les utilisateurs des services de communications électroniques et que l'obligation de conservation portait 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.

Enfin, après avoir relevé que les dispositions déclarées contraires à la Constitution n'étaient plus en vigueur, le Conseil constitutionnel a jugé que la

remise en cause des mesures ayant été prises sur le fondement de ces dispositions 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 pouvaient être contestées sur le fondement de cette inconstitutionnalité.

1.1.2 : le droit de l'Union

la Charte des droits fondamentaux de l'Union européenne

L'article 7 intitulé « Respect de la vie privée et familiale » énonce que :

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

L'article 8, relatif à la protection des données à caractère personnel dispose que :

> *« 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, relatif à la liberté d'expression et d'information, dispose :

> *« 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.*
> *(...)*
> *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 (...)*.

la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002

Il résulte des articles 1er et 2 de cette directive, tel qu'interprétés par la Cour de justice de l'Union européenne, que les opérateurs mentionnés à l'article L. 34-1 du CPCE relèvent du champ d'application de cette directive.

Le considérant 2 énonce que la présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la Charte. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

Aux termes de son article 5 :

> *« 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 ».*

L'article 6 dispose :

> *«* ***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*** *».*

Le paragraphe 1 de l'article 15 est ainsi rédigé :

> *« 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. »*

le réglement 2016/679 (RGPD)

L'article 5 prévoit que :

« *Les données à caractère personnel doivent être :*
b) collectées pour des finalités déterminées, explicites et légitimes, ***et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités*** *(...)* ».

L'article 23 du RGPD prévoit que :

1. Le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :
a) la sécurité nationale ;
b) la défense nationale ;
c) la sécurité publique ;
d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces (...).

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant:
a) aux finalités du traitement ou des catégories de traitement;
b) aux catégories de données à caractère personnel;
c) à l'étendue des limitations introduites;
d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; e) à la détermination du responsable du traitement ou des catégories de responsables du traitement;
f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement;
g) aux risques pour les droits et libertés des personnes concernées; et
h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

1.1.3 : l'article 8 de la Convention européenne des droits de l'homme

Le droit à la protection des données à caractère personnel ne fait pas partie, en tant que droit autonome, des droits et libertés garantis par la Convention. La Cour a néanmoins reconnu que la protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée et familiale, du domicile et de la correspondance garanti par l'article 8 de la Convention (Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande, 27 juin 2017, § 137).

Cet article dispose :

Droit au respect de la vie privée et familiale
« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Le Guide sur la jurisprudence de la Convention européenne des droits de l'homme en matière de protection des données précise que « *Dans la plupart des affaires où un traitement des données à caractère personnel était destiné à permettre aux autorités de conduire une enquête contre leur titulaire ou à recueillir des moyens de preuve dans le cadre d'une procédure judiciaire devant les juridictions nationales, la Cour a estimé qu'un tel traitement entrait dans le champ d'application de l'article 8 et donnait lieu à une ingérence dans la vie privée des personnes concernées ».*

1.2 : la jurisprudence de la Cour de justice de l'Union européenne

1.2.1 : les arrêts Quadrature du Net et Prokuratuur

La jurisprudence de la Cour de justice de l'Union européenne sur la conservation et l'accès aux données de connexion a fait l'objet de **plusieurs arrêts successifs**[6].
Le moyen repose sur le dernier état de cette jurisprudence au jour du dépôt du mémoire ampliatif, à savoir les arrêts :

- « La Quadrature du Net et autres » (C-511/18, C-512/18, C-520/18) du 6 octobre 2020 ;
- « Prokuratuur » du 2 mars 2021 (C- 746/18).

La décision attaquée est postérieure à ces deux arrêts mais concerne des données collectées et communiquées avant qu'ils ne soient rendus.

Postérieurement au dépôt du mémoire ampliatif, dans l'arrêt « Commissioner of the Garda Síochána e.a ». du 5 avril 2022 (C-140/20), la Cour de justice de l'Union européenne a apporté plusieurs précisions quant à l'étendue des pouvoirs que reconnaît la directive « vie privée et communications électroniques » aux États membres en matière de conservation de données de connexion aux fins de lutte contre la criminalité grave.

***

la prohibition de la conservation générale et indifférenciée des données de connexion

---

6

CJUE, 8 avril 2014, Digital Rights Ireland Ldt, C 293/12 et C-594/12 - CJUE, 21 décembre 2016, Télé2 Sverige et Watson, C-203/15 et C-698/15 - CJUE 2 octobre 2018, Ministerio Fiscal, C-207/16 -

Par les arrêts précités, la Cour de justice de l'Union européenne a entendu limiter strictement la possibilité pour les Etats d'imposer aux opérateurs de communications électroniques la conservation des données de connexion de leurs utilisateurs.

En premier lieu, la Cour confirme, ce qu'elle avait précédemment énoncé dans l'arrêt Télé 2, à savoir que la directive « vie privée et communications électroniques » s'applique à des réglementations nationales imposant aux fournisseurs de services de communications électroniques de procéder, aux fins de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, à des traitements de données à caractère personnel.

En deuxième lieu, la Cour reprend le raisonnement, déjà mené dans l'arrêt Tele 2, selon lequel 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**, indépendamment même d'un accès éventuel à ces données. 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.

Elle rappelle que la directive « vie privée et communications électroniques » ne se limite pas à encadrer l'accès à de telles données par des garanties visant à prévenir les abus, mais consacre, en particulier, **le principe de l'interdiction du stockage des données relatives au trafic et à la localisation, en ses articles 5 et 6.** La conservation de ces données constitue ainsi, d'une part, une dérogation à cette interdiction de stockage et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte.

Elle en déduit 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.

En troisième lieu, elle relève que si l'article 52 de la Charte permet aux États membres de limiter les droits aux fins notamment de la lutte contre les infractions pénales, de telles limitations doivent avoir été prévues par la loi, respecter le contenu essentiel de ces droits, être nécessaires et adéquates au regard des objectifs d'intérêt général reconnus par l'Union et respecter le principe de proprotionnalité.

Elle précise que, pour satisfaire à l'exigence de proportionnalité, la réglementation doit respecter les points suivants (point 132 de l'arrêt « La Quadrature du Net ») :

- elle doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées

disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus ;

- elle doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise.

Elle relève qu'en conséquence la possibilité pour un Etat d'imposer une obligation de conservation diffère selon la nature des données en cause et les finalités (ou objectifs) poursuivies, telles qu'elles sont prévues à l'article 15 de la directive (point 133 dudit arrêt).

Elle établit en conséquence une corrélation étroite (ou un « tableau de correspondance ») entre d'une part la nature de la donnée en cause et la gravité de l'ingérence qu'elle implique, d'autre part, la gravité de l'infraction ou de la menace de nature à justifier cette ingérence.

Ainsi, dans l'arrêt « La Quadrature du Net », elle relève, par une interprétation 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 que :

- l'existence d'une menace pour la sécurité nationale, qui s'avère réelle et actuelle ou prévisible est de nature, par elle-même, à établir le rapport nécessaire entre les données de trafic et de localisation à conserver et cet objectif (point 137);

- **une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité, serait-elle même grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique** (point 141) ;

- l'ingérence qu'emporte la conservation générale et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ne saurait, en principe, être qualifiée de grave dès lors que 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 (point 157) ;

- les adresses IP attribuées à la source d'une connexion ne révèlent aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication et peuvent constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Une conservation indifférenciée et généralisée de celles-ci emporte cependant une ingérence grave dans les droits fondamentaux des personnes concernées, de sorte qu'elle ne saurait être justifiée qu'aux fins de lutte contre la criminalité grave, pour la prévention des menaces graves contre la sécurité publique et pour la sauvegarde de la sécurité nationale (point 154).

La Cour de justice en déduit (point 168) que :

> « *1. 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 des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation*** ».
>
> *En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives*
>
> *2-permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;*
>
> *– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;*
>
> *– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;*
>
> *– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques,*
>
> *– permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,*
>
> *dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions*

matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

la conservation des données aux fins de lutte contre la criminalité grave

Il en résulte, s'agissant spécifiquement de la lutte contre la criminalité, 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 que:

1. il s'oppose à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, quelle que soit la gravité de celle-ci.

2. il ne s'oppose pas à des mesures législatives prévoyant, aux fins de la lutte contre la criminalité grave :

- une conservation ciblée des données relatives au trafic et des données de localisation en fonction de catégories de personnes concernées ou au moyen d'un critère géographique ;

- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion ;

- une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

- le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide (« conservation rapide » ou quick freeze) des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

1.2.2 : la conservation rapide des données de trafic et de localisation

un apport de l'arrêt « La Quadrature du Net »

La notion de « conservation rapide » des données a été introduite dans la jurisprudence de la Cour de justice de l'Union européenne par l'arrêt « La Quadrature du Net ».

Compte tenu de l'importance de cette problématique, il convient de citer in extenso le passage de cet arrêt relatif à celle-ci.

« 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, 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.

Il résulte de ce qui précède, qu'au titre de la conservation rapide, un Etat peut enjoindre aux fournisseurs de services de communication de procéder à une conservation des données de connexion aux conditions suivantes :

- 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 que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation de l'infraction ou la prévention de la menace ;

- il doit s'agir d'une **infraction pénale grave** ou d'une atteinte à la sécurité publique ;

- la décision de l'autorité compétente doit être soumise à un **contrôle juridictionnel effectif** ;

- la durée de conservation doit être limitée au **strict nécessaire** ;

- enfin, la conservation rapide **doit être prévue par la loi** et préciser notamment la ou les finalités pour laquelle ou lesquelles elle peut être ordonnée.

le fondement de la conservation rapide : la Convention de Budapest sur la cybercriminalité

La Cour de justice de l'Union européenne a « puisé[7] » cette notion dans l'article 16 de la Convention de Budapest sur la cybercriminalité du 23 novembre 2021.

Aux termes du paragraphe 1 de cet article :

> « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification* ».

Cet article fait donc obligation aux Etats parties à la convention de prévoir dans leur législation les mesures permettant d'ordonner la conservation rapide des données relatives au trafic.

Le rapport explicatif de cette Convention précise que :

- toutes les dispositions dont il est question dans la section 2 «Droit de procédure » visent à permettre l'obtention ou la collecte de données aux fins des enquêtes ou des procédures pénales à mener. Aucun seuil de gravité pour l'accès aux données de connexion n'est fixé ;

- durant la période de conservation, les données ne sont pas automatiquement portées à la connaissance des services répressifs. En effet, pour que les données puissent être divulguées, il faut prendre une mesure supplémentaire de divulgation ou ordonner une perquisition ;

- la « *conservation* » exige que les données qui existent déjà et sont stockées (...) soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient « gelées » (c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes (...)

- 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 États d'appliquer cet article en mettant en oeuvre ces autres moyens (point 160).

1.2.3 : les précisions apportées par l'arrêt Commissioner of the Garda Siochana du 5 avril 2022 sur la conservation des données

[7]Selon l'expression du rapporteur public M.A.Lallet de l'arrêt du Conseil d'Etat « French Data Network et autres ».

Dans cet arrêt, la Cour réitère, en premier lieu, sa jurisprudence 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.

Elle apporte également plusieurs précisions s'agissant de la conservation rapide :

- les autorités compétentes peuvent ordonner une mesure de conservation rapide dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou sur un éventuel acte de criminalité grave (point 91) ;

- elle peut être étendue à des 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 ou au lieu où une personne, potentiellement victime d'un acte de criminalité grave, a disparu, à la condition que cette mesure ainsi que l'accès aux données ainsi conservées respectent les limites du strict nécessaire aux fins de la lutte contre la criminalité grave ou de la sauvegarde de la sécurité nationale (point 90).

1.3 : l'arrêt du Conseil d'Etat 21 avril 2021 « French Data Network E.A » :

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

Le Conseil d'Etat était saisi de moyens tendant à l'annulation pour excès de pouvoir du refus du Premier ministre d'abroger notamment l'article R. 10-13 du CPCE.

Les demandeurs faisaient valoir que ces dispositions étaient contraires au droit de l'Union (article 15 de la directive sur la vie privée, articles 7,8 et 11 de la Charte), tel qu'interprété par la Cour de justice de l'Union européenne.

En défense, le Gouvernement a développé deux arguments afin de faire obstacle à l'annulation du refus du Premier ministre d'abroger l'article précité :

le premier fondé sur « l'ultra vires » ;

le second sur le respect des exigences constitutionnelles qui ne seraient pas garanties de façon équivalente par le droit européen.

S'agissant du premier, le Conseil d'Etat a refusé de rechercher si la Cour de justice de l'Union européenne avait excédé sa propre compétence. Il a énoncé qu' « *il n'appartient pas* ***au juge administratif*** *de s'assurer du respect, par le droit dérivé de l'Union européenne ou par la Cour de justice elle-même, de la répartition des compétences entre l'Union européenne et les Etats membres* » (§8).

En revanche, il a vérifié que l'application du droit européen, tel qu'il avait été interprété par la Cour de justice de l'Union européenne, conduisant à mettre à l'écart le droit national au motif de sa contrariété au droit de l'Union, s'agissant de la conservation généralisée et indifférenciée des données, n'avait pas pour effet

de priver de garanties effectives les objectifs de valeur constitutionnelle de sauvegarde des intérêts fondamentaux de la Nation, de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales et de lutte contre le terrorisme.

Le Conseil d'Etat a jugé que :

1. 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. 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. 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 Cour de justice de l'Union européenne en raison :

- de 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) ;

- sous réserve néanmoins pour le gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace (§46).

4. 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, quelle que soit sa gravité.

Examinant alors le respect des objectifs à valeur constitutionnelle, le Conseil d'Etat constate successivement que :

- l'obligation de conservation généralisée et indifférenciée des données de connexion pour une durée d'un an est une condition déterminante du succès des enquêtes pénales ;

- les alternatives envisagées par la Cour de justice de l'Union européenne 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) ;

- 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) ;

- l'efficacité de la conservation rapide est subordonnée à la condition que les données aient été effectivement conservées par les opérateurs.

Dès lors, le Conseil d'Etat juge que :

> **« *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***[8]***, 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 ».*

Il peut être éclairant de se référer sur ce point aux conclusions du rapporteur public M.A.Lallet :

8

Point 39 : (...) Or, aux termes de l'article préliminaire du code de procédure pénale : " Au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction ". Conformément au principe de proportionnalité consacré par cet article, l'obligation de conservation résultant du III de l'article L. 34-1 du code des postes et des communications électroniques et du II de l'article 6 de la loi du 21 juin 2004 n'est donc imposée aux opérateurs, sous le contrôle des juridictions compétentes, que pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales susceptibles de présenter un degré de gravité suffisant pour justifier l'ingérence dans les droits protégés par les articles 4, 7 et 11 de la Charte des droits fondamentaux de l'Union européenne. Seules de telles infractions pouvant légalement justifier l'accès des services d'enquêtes aux données conservées par les opérateurs, il s'ensuit que la conservation des adresses IP imposée de façon généralisée et indifférenciée aux opérateurs ne saurait être regardée comme méconnaissant les exigences de la directive du 12 juillet 2002.

« A bien y regarder, nous pensons toutefois qu'il y a place pour construire un dispositif viable et aussi respectueux que possible des exigences de la Cour, en combinant les différentes souplesses offertes par l'arrêt, avec l'audace interprétative qui nous caractérise aujourd'hui. Si vous admettez que l'Etat puisse légalement enjoindre aux opérateurs de conserver de manière généralisée et indifférenciée l'ensemble des données de connexion pour les besoins de la sauvegarde de la sécurité nationale, alors les données dont les services d'enquête ont besoin existeront. Cette existence est, bien entendu, la première condition de leur disponibilité. Elle ne se suffit toutefois pas à elle-même. Car, comme on l'a dit, la jurisprudence de la Cour exclut qu'on puisse y accéder directement à des fins de lutte contre la criminalité grave, conformément à la règle de concordance. L'entrepôt de données est là, mais sa porte ne s'ouvre qu'à ceux pour qui il a été constitué. Toutefois, l'arrêt du 6 octobre 2020 n'exclut pas, et même envisage à notre avis, que la conservation rapide à des fins de lutte contre la criminalité grave puisse se greffer sur ce lac de données « sécurité nationale ». ***Elle indique en effet au point 164 de l'arrêt du 6 octobre que la finalité de la conservation rapide doit être précisée dans la loi « dans la mesure où [elle] ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement ». Elle semble ainsi admettre une forme de « déclassement » du motif de conservation, qui apparaît justifié dès l'instant que la conservation rapide n'est pas elle-même généralisée et indifférenciée, mais porte sur des personnes ou des infractions bien identifiées – c'est la logique du bassin de rétention.*** *Ainsi articulée avec le régime de conservation pour les besoins de la sécurité nationale, la conservation rapide pourra porter non seulement sur les données futures, mais aussi sur les données passées, avec la même profondeur d'un an, et avec le champ d'application large admis par la Cour qui permet de geler les données des suspects, des victimes ou des tiers dès l'instant qu'elles peuvent contribuer à l'élucidation de l'infraction, mais aussi de sanctuariser les données se rapportant à telle ou telle zone géographique – par exemple la liste des numéros de téléphone ayant « borné » dans un secteur ».*

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

Il en déduit qu'aussi longtemps que l'existence d'une menace grave sur la sécurité nationale justifie la conservation généralisée et indifférenciée des données de connexion, de nature à permettre une conservation rapide de celles-ci, l'application du droit de l'Union européenne, en conduisant à écarter le droit national, ne prive pas de garanties effectives les objectifs de valeur constitutionnelle précités.

1.4 : examen des trois premières branches du moyen

1.4.1 : motivation de la chambre de l'instruction sur la conservation des données

En substance, la chambre de l'instruction énonce que :

- la Cour de justice de l'Union européenne a jugé que le droit européen ne s'opposait pas à des mesures qui, par exception, prévoiraient, aux fins de lutte contre la criminalité grave, une conservation des données relatives au trafic et des

données de localisation, qui ne soit pas systématique et continue, mais ciblée, à condition que les critères du ciblage soient objectifs et limités à une durée strictement nécessaire au regard de l'objectif poursuivi ;

- la législation française limite à un an la durée de conservation de ces données pour les besoins de la recherche, de la constatation et la poursuite des infractions pénales ;

- il résulte de l'arrêt du Conseil d'Etat que la conservation généralisée des données est aujourd'hui justifiée par la menace existante pour la sécurité nationale; que la possibilité d'accéder à ces données pour la lutte contre la criminalité grave permettait à ce jour, de garantir les exigences constitutionnelles de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales.

La chambre de l'instruction en déduit qu'en l'espèce, l'ingérence dans la vie privée de M. [U], constituée par les réquisitions aux opérateurs téléphoniques et l'exploitation des données d'identité, des données relatives au trafic traçant les dates, heures et destinataires des communications et des données de géolocalisation apparaît tout à la fois nécessaire et proportionnée à la poursuite d'infractions pénales relevant de la criminalité grave, infractions que la chambre de l'instruction a longuement analysées in concreto[9].

1.4.2 : argumentation du moyen

Après avoir rappelé la teneur de l'arrêt « La Quadrature du Net », le moyen développe l'argumentation suivante :

- les articles L. 34-1 et R. 10-13 du code des postes et communications électronique n'ont précisé ni quelles infractions graves justifiaient une obligation de conservation, ni les catégories de données à conserver, ni les personnes concernées, ni les autorités habilitées à définir les cas dans lesquels ce stockage s'impose ;

- il s'ensuit que sont méconnues tant les dispositions de l'article 15 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne que celles de l'article 8 de la Convention européenne des droits de l'homme ;

- les réquisitions aux fins de recherche d'un trafic de stupéfiants sans lien avec la recherche des infractions en matière de terrorisme ne répondent pas aux conditions du droit de l'Union européenne.

9

« Il lui est ainsi reproché d'avoir participé à une organisation criminelle de dimension internationale, dont les membres présentent un comportement aguerri avec l'utilisation de multiples lignes téléphoniques dédiées, de méthodes relevant de la grande criminalité organisée et d'armes de guerre. Cette organisation a ainsi importé et exporté plusieurs centaines de kilogrammes de cocaïne d'une grande pureté en provenance d'Amérique du sud et à destination du continent européen »

1.4.3 : analyse

En premier lieu, on observera que, contrairement à ce que soutient le moyen en sa première branche, la chambre de l'instruction n'a pas énoncé que les infractions de criminalité grave justifiaient une conservation généralisée et indifférenciée des données de connexion mais une « conservation ciblée ».

En second lieu, à supposer que la chambre juge que la conservation rapide permet aux enquêteurs, pour la finalité de la lutte contre la criminalité grave, d'accéder aux données de connexion conservées de façon générale et indifférenciée aux fins de sauvegarde de la sécurité nationale, elle devra dire si cette conservation fait l'objet d'un encadrement suffisant.

A cet égard, les observations suivantes peuvent être faites :

la portée de l'arr t du Conseil d'Etat

Le Conseil d'Etat a jugé (point 58) que :

- l'article L. 34-1 du CPCE doit être écarté, comme contraire au droit de l'Union européenne, uniquement en tant qu'il poursuit une finalité autre que celle de la sauvargarde de la sécurité nationale ;

- le refus d'abroger l'article R. 10-13 doit être annulé en tant que, d'une part, ces dispositions ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation à la sauvegarde de la sécurité nationale, d'autre part, ces dispositions ne prévoient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, s'agissant des données qu'elles mentionnent autres que celles afférentes à l'identité civile, aux comptes et aux paiements des utilisateurs et aux adresses IP.

En outre, constatant 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, il en déduit que le Gouvernement pouvait légalement imposer aux opérateurs de communications léctroniques la conservation générale et indifférenciée de telles données aux fins de sauvegarde de la sécurité nationale (point 96).

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?

Existe-t-il en droit interne une norme permettant la conservation rapide des données qui satisfasse aux exigences de l'Union européenne et de la Convention européenne des droits de l'homme ?

La Cour de justice de l'Union européenne pose une exigence de **qualité de la norme**, propre à satisfaire à l'exigence de proportionnalité. Deux conditions principales sont posées (point 132, arrêt « La Quadrature du Net ») :

- d'une part, la réglementation doit prévoir des **règles claires et précises** régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus ;

- d'autre part,cette réglementation doit être **légalement contraignante** en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire.

S'agissant spécifiquement de la « conservation rapide », la Cour de justice impose en outre que la législation précise la ou les finalités pour laquelle une conservation rapide peut être ordonnée (point 164 de l'arrêt précité).

La Cour européenne des droits de l'homme pose une même exigence.

Le guide relatif à l'article 8 de la Cour européenne des droits de l'homme précise à cet égard :

> «*15. La Cour a affirmé à maintes reprises que toute ingérence d'une autorité publique dans le droit d'une personne au respect de sa vie privée et de sa correspondance doit être « prévue par la loi ». Cette expression impose non seulement le respect du droit interne, mais elle concerne aussi la qualité de la loi, qui doit être compatible avec la prééminence du droit (Halford c. Royaume-Uni, § 49).*
>
> *16. La législation interne doit être claire, prévisible et suffisamment accessible (Silver et autres c. Royaume-Uni, § 87) (...)*
>
> *18.Pour ce qui est de la prévisibilité, l'expression « prévue par la loi » implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention.* »

S'agissant des réquisitions adressées par le procureur de la République, sur le fondement de l'article 77-1-1 du code de procédure pénale, la Cour européenne des droits de l'homme a jugé, dans l'affaire Ben Faiza c.France du 8 février 2018, que :

> « *72. Concernant la qualité de la loi, et plus spécialement sa prévisibilité, il ne saurait être fait reproche à la loi de ne pas dresser une liste exhaustive de l'ensemble des documents susceptibles d'être requis lors d'une enquête, compte tenu du caractère général inhérent à toute règle normative. La Cour relève, par ailleurs, qu'il ressort cette fois de la jurisprudence de la Cour de cassation (paragraphes 35-37 ci-dessus) que l'article 77-1-1 du CPP est couramment utilisé pour requérir auprès des opérateurs téléphoniques des données personnelles ne touchant pas au contenu des communications.*
>
> *73. En outre, la Cour constate que cette loi prévoit également des garanties contre l'arbitraire. D'une part, dans le cadre d'une enquête préliminaire, les réquisitions prises par un officier de police judiciaire sur le fondement de l'article 77-1-1 sont soumises à l'autorisation préalable d'un magistrat du parquet. La Cour note*

d'ailleurs qu'il ne peut être dérogé à cette obligation sous peine de nullité de l'acte (paragraphes 35-36 ci dessus). D'autre part, de telles réquisitions judiciaires sont susceptibles d'un contrôle juridictionnel. Dans la procédure pénale ultérieure menée contre la personne concernée, les juridictions pénales peuvent contrôler la légalité d'une telle mesure et, si celle-ci est jugée illégale, elles ont la faculté d'exclure du procès les éléments ainsi obtenus. Un tel contrôle a d'ailleurs été effectué en l'espèce (paragraphes 17 et 20-21 ci-dessus) ».

Dans l'arrêt tout récent Ekimdzhiev et autre c. Bulgarie du 11 janvier 2022 (uniquement en anglais), la Cour européenne a jugé que la législation bulgare relative à la conservation des données de connexion et à l'accès à ces données ne satisfaisait pas à l'exigence de qualité de la loi découlant de la Convention dès lors que si cette législation était accessible et prévoyait l'instauration de garanties, les demandes n'avaient néanmoins pas à être étayées par des pièces et les décisions elles-mêmes n'avaient pas à être motivées. Dès lors, la législation ne garantissait pas que l'accès ne soit accordé que lorsque cela était véritablement nécessaire et de manière proportionnée dans chaque cas.

Dans l'arrêt « Big Brother Watch et autres c. Royaume-Uni » du 25 mai 2021 (requêtes nos 58170/13, 62322/14 et 24960/15), la Cour européenne des droits de l'homme a énoncé que l'interception en masse de données de communication associées aux communications pouvait revêtir potentiellement un caractère extrêmement intrusif[10]. Elle a néanmoins jugé qu'il n'y avait pas lieu de leur accorder le même niveau de protection que celui défini au paragraphe 361 du présent arrêt pour le contenu des communications dès lors qu' « *il n'est pas nécessaire que les dispositions juridiques régissant le traitement des données de communication associées soient identiques en tous points à celles régissant le traitement du contenu des communications* ».

Selon l'approche globale adoptée par la Cour, le processus d'interception de masse du contenu des communications doit être encadré par « *des garanties de bout en bout* », c'est à dire que la nécessité et la proportionnalité des mesures prises doivent être appréciées à chaque étape à l'échelle nationale.

La Cour contrôle que le cadre juridique national définit clairement :

-les motifs pour lesquels l'interception en masse peut être autorisée ;

10

Il *en va de même pour les données de communication associées. Comme indiqué dans le rapport établi à l'issue du contrôle des activités de surveillance, pour chaque individu, le volume de données de communication actuellement disponible est normalement supérieur au volume de données de contenu, car chaque contenu s'accompagne de multiples données de communication (paragraphe 159 ci-dessus). Si le contenu d'une communication, crypté ou non, peut ne rien révéler d'utile sur son expéditeur ou son destinataire, les données de communication associées, en revanche, peuvent révéler un grand nombre d'informations personnelles telles que l'identité et la localisation de l'expéditeur et du destinataire, ou encore l'équipement par lequel la communication a été acheminée. De plus, toute intrusion occasionnée par l'acquisition de données de communication associées est démultipliée par l'interception en masse, car ces données peuvent désormais faire l'objet d'analyses et de recherches qui permettent de brosser un portrait intime de la personne concernée par le suivi de ses activités sur les réseaux sociaux, de ses déplacements, de ses navigations sur Internet ainsi que de ses habitudes de communication, et par la connaissance de ses contacts*

-les circonstances dans lesquelles les communications d'un individu peuvent être interceptées ;

-la procédure d'octroi d'une autorisation ;

-les procédures à suivre pour la sélection, l'examen et l'utilisation des éléments interceptés ;

-les précautions à prendre pour la communication de ces éléments à d'autres parties ;

-les limites posées à la durée de l'interception et de la conservation des éléments interceptés, et les circonstances dans lesquelles ces éléments doivent être effacés ou détruits ;

- les procédures et modalités de supervision, par une autorité indépendante, du respect des garanties énoncées ci-dessus ;

- les pouvoirs de cette autorité en cas de manquement

- et enfin les procédures de contrôle indépendant a posteriori du respect des garanties et les pouvoirs conférés à l'organe compétent pour traiter les cas de manquement.

***

Par ailleurs, on observera qu'aucune disposition du code de procédure pénale ne prévoyait, de façon explicite, à la date de la conservation des données, objet de l'arrêt frappé de pourvoi, la conservation rapide des données de connexion.

Une procédure de « conservation rapide » a été introduite en droit français par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement . Le III de l'article L. 34-1 du CPCE prévoit désormais que « *Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données* ».

Peut-on déduire de l'introduction en droit positif de cette disposition que la loi ne prévoyait pas antérieurement une telle possibilité ?

Le rapport explicatif de la Convention sur la cybercriminalité retient que l'injonction de « conservation rapide » peut prendre la forme d'une « injonction de produire ».

Peut-on dès lors considérer que les articles 99-3 et 99-4 du code de procédure pénale, qui autorisent le juge d'instruction à requérir l'accès aux données de connexion, lus à la lumière du 6^{ième} alinéa du III de l'article préliminaire valent également injonction de « *conservation rapide* » ? Si le juge d'instruction est compétent pour accéder aux données, ne l'est-il pas *a fortiori* pour exiger leur conservation ? Et, en cas de réponse positive, les dispositions précitées présentent-elles **la qualité de norme** requise par la Cour de justice de l'Union européenne ?

Enfin, quelle définition retenir de la « *criminalité grave* », qui seule permet la « *conservation rapide* », dès lors que la Cour de justice de l'Union européenne ne

parait pas considérer celle-ci comme une **notion autonome** du droit de l'Union mais comme une notion contingente dont les contours doivent être laissés à l'appréciation des Etats membres ?

On relèvera que tirant les conséquences de la décision n° 2021-952 QPC du 3 décembre 2021 par laquelle le Conseil constitutionnel a censuré les dispositions des articles 77-1-1 et 77-1-2 du code de procédure pénale relatives aux réquisitions portant, en enquête préliminaire, sur des informations émanant d'un système informatique ou d'un traitement de données nominatives (cf. point 2.1.2), l'article 12 de la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire a retenu, sauf exceptions[11], un seuil de trois ans en deçà duquel il ne peut plus être recouru à des réquisitions portant sur des données de connexion.

> *est-il permis d'accéder des données conservées pour la sauvegarde de la sécurité nationale puis ayant fait l'objet d'une conservation rapide aux fins de lutte contre la criminalité grave (3i me branche) ?*

La principale difficulté est d'articuler ce raisonnement avec le principe affirmé, de façon constante, par la Cour de justice de l'Union européenne, et rappelé clairement dans l'arrêt « Commissioner of An Garda Siochana » selon lequel les autorités nationales compétentes ne peuvent **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, à titre exceptionnel, conformément à sa jurisprudence, pour faire face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible (points 96 à 100).

En effet, selon la Cour de justice,

> l'accès aux données ne saurait dépendre de circonstances étrang res l'objectif de lutte contre la criminalité grave ;
>
> l'accès aux données ne peut tre justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, savoir la sauvegarde de la sécurité nationale, ce qui irait l'encontre de la hiérarchie des objectifs d'intérêt général dans le cadre de laquelle doit s'apprécier la proportionnalité d'une mesure de conservation ;
>
> autoriser un tel accès risquerait de priver de tout effet utile l'interdiction de procéder une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave (point 97 et suivants).

Doit-on déduire de ce principe qu'à supposer que des données conservées aux fins de la sauvegarde de la sécurité nationale aient été conservées « à titre rapide », les enquêteurs ne pourraient y accéder ?

11

-La procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques et ces réquisitions ont pour seul objet d'identifier l'auteur de l'infraction

--les réquisitions concernent les équipements terminaux de la victime et interviennent à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement

- les réquisitions interviennent dans le cadre d'une procédure tendant à rechercher une personne disparue ou à retracer un parcours criminel

Il convient d'observer que la critique ne porte pas sur le principe même d'une conservation rapide des données, faisant obstacle à leur disparition, mais sur l'accès, aux fins de lutte contre la criminalité grave aux données ainsi conservées.

A cet égard, on peut faire valoir que la Cour de justice de l'Union européenne distingue nettement, dans ses arrêts « La Quadrature du Net » et « Commissioner of An Garda Siochana»,

- la **conservation générale et indifférenciée** des données de trafic et de localisation, **finalité préventive ;**
- de la **conservation dite « *rapide* »**, dont la finalité est **l'élucidation d'infractions pénales graves » déterminées,** qui a pour objet de faire obstacle l'effacement des données et et peut porter que sur **des données de nature contribuer l'élucidation de cette infraction**.

Ces deux modalités de conservation de données se distinguent donc par leur nature, les données sur lesquelles elles peuvent porter et leur finalité.

Dès lors, l'arrêt « Commissioner of An Garda Siochana » pourrait être compris comme :

- permettant aux autorités compétentes l'accès aux données ayant fait préalablement d'une conservation rapide (point 87), de telles données ayant fait l'objet d' « ***une forme de déclassement*** » pour reprendre l'expression du rapporteur public de l'arrêt « French Data Network » du Conseil d'Etat[12] ;

- mais prohibant, hors hypothèse de conservation rapide, l'accès, aux fins de lutte contre la criminalité grave, aux données conservées aux fins de sauvegarde de la sécurité nationale[13] (point 100).

Conclusion sur les trois premières branches

C'est au vu de l'ensemble de ces observations que la chambre criminelle appréciera si, compte tenu de la jurisprudence de la Cour de justice de l'Union européenne :

- le dispositif légal français permettait la date des faits la conservation généralisée et indifférenciée des données de connexion des fins de sauvergarde de la sécurité nationale ;

---

[12] Point 87 : « *Dans la mesure où la finalité d'une telle conservation rapide necorrespond plus à celles pour lesquelles les données ont été collectées et conservées initialement...* »

[13]

« *les données relatives au trafic et les données de localisation ne peuvent pas faire l'objet d'une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave et, partant, un accès à ces données ne saurait être justifié à ces mêmes fins. Or, lorsque ces données ont exceptionnellement été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale contre une menace qui s'avère réelle et actuelle ou prévisible, dans les conditions visées au point 58 du présent arrêt, les autorités nationales compétentes en matière d'enquêtes pénales ne sauraient accéder auxdites données dans le cadre de poursuites pénales, sous peine de priver de tout effet utile l'interdiction de procéder à une telle conservation aux fins de la lutte contre la criminalité grave* »

- en cas de réponse affirmative cette question, si une menace pour la sécurité nationale présentant les caractères définis par la jurisprudence européenne existait cette date ;
- enfin, si le dispositif légal français permettait, toujours la date des faits, la « conservation rapide », aux fins d'élucidation d'une infraction pénale grave déterminée, de données de connexion conservées de façon générale et indifférenciée des fins de sauvegarde de la sécurité nationale ?

2. l'accès aux données : **quatrième branche du moyen unique**

Cette branche soutient que le juge d'instruction ne peut autoriser les enquêteurs agissant sur commission rogatoire à accéder aux données conservées.

2.1 : les normes de droit interne

2.1.1 **:** les dispositions pertinentes

Les articles 99-3 et 99-4 du code de procédure pénale autorisent le juge d'instruction ou l'officier de police judiciaire par lui commis à accéder aux données de connexion détenus par les opérateurs de télécommunications.

Ces dispositions doivent être lues à la lumière de l'alinéa 6 du III de l'article préliminaire aux termes duquel, au cours de la procédure pénale, toute mesure portant atteinte à la vie privée d'une personne doit être, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnée à la gravité de l'infraction.

Par un arrêt en date du 20 avril 2022 (pourvoi n° 22-90.003), la Cour de cassation a transmis au Conseil constitutionnel une question prioritaire de constitutionnalité portant sur les articles 99-3 et 99-4 en ce qu'ils méconnaitraient le droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen. La Cour a retenu que la question présentait « *un caractère sérieux en ce que les articles précités, qui autorisent le juge d'instruction à requérir la communication de données de connexion de nature à permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées, quelle que soit la gravité des infractions poursuivies, sont susceptibles de porter une atteinte excessive aux droits et aux libertés protégés par l'article 2 de la Déclaration des droits de l'homme et du citoyen* ».

Il convient de mettre en perspective cette question avec la déclaration d'inconstitutionnalité des articles 77-1-1 et 77-1-2 du code de procédure pénale.

2.1.2 : la déclaration d'inconstitutionnalité des articles 77-1-1 et 77-1-2 du code de procédure pénale

Dans sa décision n° 2021-952 du 3 décembre 2021 , saisie d'une QPC relative à la conformité aux droits et libertés que la Constitution garantit des articles 77-1-1 et 77-1-2 du code de procédure pénale, le Conseil constitutionnel a jugé que le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une **conciliation équilibrée entre le droit au respect de la vie privée et l'objectif à valeur constitutionnelle de recherche des auteurs d'infractions** et a déclaré en conséquence les dispositions contestées contraires à la Constitution.

> *« 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 censure du Conseil constitutionnel **n'est donc pas fondée sur le statut du ministère public** mais sur **l'insuffisance des garanties** encadrant son action.

Par arrêt en date du 8 mars 2022 (Crim., 8 mars 2022, pourvoi n° 21-90.046), la Cour de cassation a saisi le Conseil constitutionnel d'une QPC relative aux articles 60-1 et 60-2 du code de procédure pénale ainsi rédigée :

> « *Les dispositions des articles 60-1 et 60-2 du code de procédure pénale qui permettent aux enquêteurs de police en flagrance, d'accéder aux données de trafic et de localisation, par le biais de réquisitions faites aux opérateurs de télécommunication, sous le seul contrôle du procureur de la République et sans nulle décision préalable délivrée par une juridiction indépendante sont-elles inconstitutionnelles, en ce qu'elles violent le droit au respect de la vie privée, qui découle de l'article 2 de la Déclaration des droits de l'homme et du citoyen, ainsi que de l'article 16 de ce texte, qui garantit l'ensemble des droits et libertés proclamés par la Constitution ?* ».

La chambre a retenu que :

> « *si les dispositions précitées n'autorisent les officiers de police judiciaire ou, sous leur contrôle, les agents de police judiciaire à requérir la communication de données de connexion de nature à permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées que dans le cadre d'une enquête*

flagrante ouverte pour un crime ou pour un délit puni d'emprisonnement, en raison de l'urgence, pendant la seule durée de cette enquête, qui ne peut excéder huit jours, éventuellement renouvelable une fois, la loi ne soumet néanmoins ces réquisitions ni à l'autorisation préalable d'une juridiction ou du procureur de la République ni même à l'information de celui-ci, de sorte que la question de l'existence 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, parait sérieuse ».

On rappelera à cet égard, que comme précisé antérieurement, l'article 12 de la loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire a encadré et limité les possibilités de recours aux réquisitions portant sur des données de connexion, en introduisant dans le code de procédure pénale un nouvel article 60-1-2 ainsi rédigé :

« À peine de nullité, les réquisitions portant sur les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés mentionnées au 3° du II bis de l'article L. 34-1 du code des postes et des communications électroniques ou sur les données de trafic et de localisation mentionnées au III du même article L. 34-1 ne sont possibles, si les nécessités de la procédure l'exigent, que dans les cas suivants:

« 1° La procédure porte sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement ;

« 2° La procédure porte sur un délit puni d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques et ces réquisitions ont pour seul objet d'identifier l'auteur de l'infraction ;

« 3° Ces réquisitions concernent les équipements terminaux de la victime et interviennent à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement ;

« 4° Ces réquisitions tendent à retrouver une personne disparue dans le cadre des procédures prévues aux articles 74-1 ou 80-4 du présent code ou sont effectuées dans le cadre de la procédure prévue à l'article 706-106-4. »

Par coordination, la loi a complété les articles 60-1, 60-1-11, 60-2, 77-1-1, 77-1-2 et 99-3 du code permettant de telles réquisitions, en flagrance (sur décision du procureur de la République, de l'officier de police judiciaire ou, sous le contrôle de ce dernier, d'un agent de police judiciaire), en préliminaire (sur décision du procureur de la République ou, avec son autorisation, d'un OPJ ou d'un APJ) et au cours de l'instruction (sur décision du juge d'instruction ou de l'OPJ par lui commis), pour préciser que ces articles s'appliquent « sous réserve des dispositions de l'article 60-1-2 ».

2.2 : la jurisprudence de la Cour de justice de l'Union européenne

Dans les arrêts précités « Telé 2 Sverige et Watson », « Prokuratuur »https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/03/c-746-18.pdf et « Commissioner of An Garda Siochana », la Cour de justice de l'Union européenne a précisé les règles que doit satisfaire une législation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées :

- en premier 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 doit 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[14] ;

- en second 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[15] ;

- en troisième lieu, l'accès ne peut être justifié en principe **que par la finalité ou une finalité plus grave** que celle pour laquelle cette conservation a été imposée[16] ;

- en quatrième 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[17] ;

- en cinquième 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[18]

Sur ce point, la Cour de justice de l'Union européenne a répondu ainsi à la question posée par la Cour suprême estonnienne :

> *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***

[14]Rokuratuur (points 48 à 50)

[15]La Quadrature du Net (point 167) - Prokuratuur (point 29)

[16]La Quadrature du Net (point 166) - Prokuratuur (point 31)

[17]Prokuratuur (point 39 et 45)

[18]Tele 2 (point 119) - La Quadrature du Net (point 188) - Prokuratuur (point 50) -

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*. » (*CJUE C-746/18 K / Prokuratuur du 2 mars 2021*).*

Dans cette espèce, le requérant, H. K., avait été déclaré coupable notamment sur la base de procès-verbaux établis à partir de données de communication conservées, que l'autorité chargée de l'enquête avait recueillies auprès d'un fournisseur de services de télécommunications électroniques, en vertu de dispositions de procédure pénale estonienne[19], qui sont très comparables à l'article 77-1-1 du code de procédure pénale français.

La Cour de justice de l'Union européenne a motivé ainsi sa décision :

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 influenceextérieure [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].(...)*

19

Selon lequel « [...] *(2) L'autorité chargée de l'enquête peut, sur autorisation du ministère public au cours d'une procédure d'instruction ou sur autorisation du tribunal au cours d'un procès devant celui-ci, demander à une entreprise de communications électroniques qu'elle fournisse les données énumérées à l'article 111 1 , paragraphes 2 et 3, de la loi relative aux communications électroniques qui ne sont pas citées au paragraphe 1 du présent article. Cette autorisation indique de manière précise les dates relatives à la période au cours de laquelle il est possible d'exiger des données.*
(3) Les demandes de fourniture de données au sens du présent article ne peuvent être faites que si elles sont absolument nécessaires pour atteindre l'objectif de la procédure pénale. »

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 « G.D contre Commissioner of An Garda Siochana » du 5 avril 2022, 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*** ».

Enfin, dernière condition, énoncée dans l'arrêt Tele 2 du 21 décembre 2016, les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, doivent en informer 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[20], lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits.

2.3 : examen de la 4ième branche

2.3.1 : l'absence de motivaiton de la chambre de l'instruction

Dans son mémoire devant la chambre de l'instruction, la personne mise en examen faisait observer que le droit français « *met en oeuvre l'accès des autorités policières 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 européenne* ».

La chambre de l'instruction n'a pas motivé sa décision sur ce point.

2.3.2 : l'argumentation du moyen

Le moyen fait valoir que le magistrat instructeur ne pouvait autoriser les enquêteurs à solliciter lesdites données « *dès lors qu'il n'était pas un tiers par rapport à l'enquête* ».

2.3.3: analyse du moyen

20

Cet article énonce : « Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive. ».

La chambre appréciera la pertinence de cette branche au regard des termes de l'arrêt « G.D contre Commissioner of An Garda Siochana » et du statut du juge d'instruction français, qui, contrairement au ministère public français, bénéficie d'une indépendance statutaire et fonctionnelle : le juge d'instruction est ainsi indépendant du ministère public, des parties mais aussi de la chambre de l'instruction qui ne peut lui donner d'injonction sauf à lui déléguer un supplément d'information.

La qualité de « tiers par rapport à l'enquête », qui exige que l'intéressé « ne soit pas impliqué dans la conduite de l'enquête pénale en cause » est-elle exigée également de « la juridiction » ou de la seule « entité administrative indépendante » ? Le juge d'instruction doit-il être regardé comme « une juridiction », au sens de la jurisprudence de la Cour de justice de l'Union européenne ?

3 : la sanction de la méconnaissance éventuelle du droit européen

Si la chambre estime que le moyen en l'une de ses quatre branches est fondée, elle devra dire quelle est la sanction de l'irrégularité.

3.1 : La question du défaut de conformité de la jurisprudence de la CJUE aux exigences constitutionnelles

Lorsqu'il est saisi d'un grief d'inconstitutionnalité formulé à l'encontre de dispositions qui se bornent à transposer des textes communautaires, le Conseil constitutionnel 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. Cédric L. et autre)*.

Le Conseil d'Etat, dans sa décision précitée French Data Network du 21 avril 2021*, rendue après question préjudicielle, a rappelé que la Constitution française demeure la norme suprême du droit national et 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.*

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 Cour de cassation pourra se demander si le droit de l'Union, tel qu'interprété par la Cour de justice de l'Union européenne, prive de garanties effectives les exigences constitutionnelles précitées, la réponse à cette question pouvant, le cas échéant, dépendre de celle qu'elle apportera sur l'interprétation de la notion de « conservation rapide ».

Dans l'affaire C-430/21 du 22 février 2022*, rendue en grand Chambre, la CJUE 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 la Cour de cassation qui serait alors pareillement tenue de saisir la CJUE d'une question préjudicielle.

3.2 : La prohibition de la limitation dans le temps des effets de la déclaration d'inconventionnalité

Dans son arrêt « La Quadrature du Net et autres, la Cour de justice de l'Union européenne a dit pour droit, en se fondant sur le **principe de primauté**, que :

> ***« 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 Cour a confirmé cette jurisprudence, dans des termes identiques, dans l'arrêt « Commissioner of an Garda Siochana » du 5 avril 2022.

On observera que ces arrêts s'opposent à la limitation dans le temps des effets d'une déclaration d'inconventionnalité d'une loi imposant aux opérateurs **la conservation généralisée et indifférenciée des données de connexion**. Ne doit-il pas en être de même s'agissant de l'accès aux données ?

3.3 : Le principe d'autonomie procédurale et son encadrement

Il résulte de la jurisprudence constante de la Cour de justice de l'Union européenne qu' 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[21], à

[21] CJCE, 16 décembre 1976, Rewe c/LandwirtschaftsKammer Saarland, aff. 33/76 et Comet c/Produktschap voor Siergewassen, aff. 45/76

condition toutefoisqu'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**).

Le principe d'autonomie procédurale est ainsi encadré par les principes d'équivalence et d'effectivité. La Cour de justice de l'Union européenne 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* ».

3.3.1 : Le principe d'équivalence

Ce principe commande que l'ensemble des règles de procédure nationales s'appliquent indifféremment aux recours fondés sur la violation du droit de l'Union et aux recours fondés sur la méconnaissance du droit interne ayant un objet et une cause semblables. Lorsqu'il est impossible d'appliquer à un recours fondé sur la violation du droit de l'Union les règles de procédure interne, la Cour exerce un contrôle de proportionnalité pour vérifier si la différence entre les règles applicables est justifiée.

Le principe d'équivalence ainsi « *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. Cette appréciation s'effectue en tenant compte de « *l'objet, de la cause ainsi que des éléments essentiels de ces recours* ». 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.

3.3.2 : Le principe d'effectivité

Selon la Cour de justice de l'Union européenne, 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 (arrêt Peterbroeck, précité, point 14).

Dans l'arrêt C-746/18 K / Prokuratuur du 2 mars 2021, complétant d'ailleurs la portée de l'arrêt Quadrature du Net en ajoutant une incise (ci-dessous en gras), la Cour de justice de l'Union européenne a explicité le contenu de ce principe s'agissant tant de la l'obligation de conservation généralisée et indifférenciée des données que de leur accès:

« 41. (...) 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 directive2002/58 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.****(...)*

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). »*

Dans l'arrêt Quadrature du Net, la Cour de justice de l'Union européenne motive son argumentation en se référant à l'arrêt du 10 avril 2003, Steffensen, C-276/01,

Dans cet arrêt, la CJUE était saisie d'une question préjudicielle portant sur le point de savoir si une juridiction nationale était tenue d'écarter un élément de preuve obtenu en violation du droit de l'Union, lequel exigeait le droit de solliciter une contre-expertise, recours qui n'existait pas en droit interne. La Cour de justice de l'Union européenne a répondu ainsi :

« *Il appartient à une juridiction nationale, saisie d'un recours tel que celui en cause au principal, d'apprécier, au vu de tous les éléments de fait et de droit à sa disposition, si les résultats des analyses d'échantillons de produits d'un fabricant*

doivent ou non être admis comme moyen de preuve d'une infraction à la réglementation nationale d'un État membre relative aux denrées alimentaires commise par ce fabricant, lorsque ce dernier n'a pas pu exercer son droit à une contre-expertise, prévu à l'article 7, paragraphe 1, second alinéa, de la directive. À cet égard, il incombe à la juridiction nationale de vérifier si les règles nationales en matière d'administration de la preuve applicables dans le cadre d'un tel recours ne sont pas moins favorables que celles concernant des recours de nature interne (principe d'équivalence) et si elles ne rendent pas pratiquement impossible ou excessivement difficile l'exercice des droits conférés par l'ordre juridique communautaire (principe d'effectivité). En outre, la juridiction nationale doit examiner s'il y a lieu d'exclure un tel moyen de preuve afin d'éviter des mesures incompatibles avec le respect des droits fondamentaux, en particulier le principe du droit à un procès équitable devant un tribunal tel que consacré par l'article 6, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

La motivation de la Cour de justice de l'Union européenne est la suivante :

« 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 CEDH et tel qu'interprété par la Cour européenne des droits de l'homme (...)

75 Il y a lieu d'indiquer, ensuite, qu'il découle de la jurisprudence de la Cour européenne des droits de l'homme, 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 Cour européenne des droits de l'homme, en vertu de l'article 6, paragraphe 1, de la CEDH, 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 Cour européenne des droits de l'homme 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 CEDH. 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. [O] jouit encore d'une possibilité véritable de commenter efficacement ce moyen de preuve ».

Il résulte en effet de la jurisprudence de la Cour européenne des droits de l'homme que la violation de la vie privée à l'occasion d'un acte d'investigation dans le cadre d'une procédure pénale n'induit pas nécessairement une violation du droit à un procés équitable. Ainsi, cette juridiction a écarté la violation de l'article 6 de la Convention européenne des droits de l'homme 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) ;

- 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 eut *« 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).

Au contraire, la violation de l'article 6 a été retenue dans une espèce où les deux premiers degrés de juridiction avaient relaxé la personne au motif que la preuve réunie était incertaine mais la Cour suprême avait, au contraire, condamné celle-ci, sans écouter l'enregistrement litigieux, dont l'authenticité et l'intégrité n'avaient pas pu être établies par une mesure d'expertise, et sans entendre la prévenue et son interlocuteur (CEDH, 22 décembre 2015, Nitulescu v. Romania, requête n°16184/06, §§49 à 56).

3.4 : analyse de la quatrième branche

La quatrième branche pose la question de la nature de la sanction des actes d'enquête qui, bien que conformes aux normes de droit interne alors applicable, ne satisfaisont pas aux exigences découlant de la jurisprudence de la Cour de justice de l'Union européenne.

3.4.1 : la conformité de la législation française au 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 très largement, durant l'information judiciaire, le droit de solliciter une expertise et une contre-expertise, sous le contrôle du juge, lorsque que « *se pose une question d'ordre technique* » et qu'il en est de même devant la juridiction de jugement.

Rien ne fait obstacle à ce qu'une personne mise en examen sollicite une expertise sur les données de connexion qui lui sont attribuées, notamment si elle estime que c'est à la suite d'une erreur technique que de telles données ont pu être rattachées à sa personne.

3.4.2 : le principe d'équivalence commande-t-il le prononcé de la nullité?

l'inopposabilité des données de connexion : une sanction transitoire se substituant au prononcé de la nullité

La question est de savoir si le principe d'équivalence exige de prononcer la nullité des réquisitions et des informations obtenues en méconnaissance du droit de l'Union européenne, si, par ailleurs, les conditions du prononcé de la nullité en droit interne sont réunies.

Selon une jurisprudence constante, le principe d'équivalence requiert que l'ensemble des règles applicables aux recours s'applique indifféremment aux recours fondés sur la violation du droit de l'Union et à ceux similaires fondés sur la méconnaissance du droit interne.

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 principe 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 devait pas 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).

Néanmoins, la chambre criminelle a exclu, sur le fondement de la prévisibilité de la loi, et de la bonne administration de la justice que soit prononcée la nullité d'un acte irrégulier au regard des exigences conventionnelles de la France lorsqu'au jour de sa commission, il n'existait pas de jurisprudence établissant cette irrégularité.

Dans un arrêt du 11 décembre 2018, la chambre a ainsi jugé qu'en l'absence, à la date des mesures critiquées, de jurisprudence établie, résultant des arrêts Salduz c/Turquie et Dayanan c/Turquie, rendus les 27 novembre 2008 et 13 octobre 2009, de la Cour européenne des droits de l'homme et ayant déduit de l'article 6, § 1, de la Convention européenne des droits de l'homme le droit pour la personne gardée à vue d'être assistée par un avocat lors de ses auditions et l'obligation de lui notifier le droit de garder le silence, l'exigence de prévisibilité de la loi et l'objectif de bonne administration de la justice faisaient obstacle à ce que les auditions réalisées à cette date, sans que la personne gardée à vue ait été assistée d'un avocat pendant leur déroulement ou sans qu'elle se soit vue notifier le droit de se taire, soient annulées pour ces motifs. Elle a cependant précisé que les déclarations incriminantes faites lors de ces auditions ne pouvaient, sans que soit portée une atteinte irrémédiable aux droits de la défense, fonder une décision de renvoi devant la juridiction de jugement ou une déclaration de culpabilité[22] (Crim., 11 décembre 2018[23], pourvoi n° 18-82.854, Bull. crim. 2018, n° 209).

22

« Attendu que, si c'est à tort que, pour écarter la demande d'annulation des auditions de Mme D. et de M. L., la chambre de l'instruction énonce qu'elles n'étaient pas le support de leur mise en examen, l'arrêt n'encourt pas pour autant la censure dès lors qu'en l'absence, à la date des mesures critiquées, de jurisprudence établie ayant déduit de l'article 6, § 1 de la Convention européenne des droits de l'homme le droit pour la personne gardée à vue d'être assistée par un

En l'espèce, la garde à vue s'était déroulée en juin 1999, soit à une date bien antérieure aux arrêts de la Cour européenne des droits de l'homme affirmant le droit pour la personne gardée à vue d'être assistée par un avocat lors de ses auditions et l'obligation de lui notifier le droit de garder le silence (près de neuf ans séparent la garde à vue de l'arrêt Salduz c/Turquie).

La portée de cette jurisprudence doit être bien comprise : elle n'a pas pour objet de priver de sanction la violation du droit européen mais de moduler dans le temps la nature de la sanction à y apporter.

Les conséquences à tirer de l'irrégularité sont appréciées non pas, durant l'information judiciaire, dans le cadre du contentieux des nullités mais postérieurement soit lors du renvoi, soit devant la juridiction de jugement : l'acte irrégulier ne peut fonder une décision de renvoi devant la juridiction de jugement ou une déclaration de culpabilité.

Le fondement de cette jurisprudence est double :

- assurer la prévisibilité de la règle de procédure, condition de la sécurité juridique : on ne saurait en effet apprécier la validité d'actes de procédure à la lumière de principes consacrés postérieurement et qui n'étaient pas prévisibles au jour de leur commission. Tel est d'ailleurs le sens de l'article 112-4 du code pénal selon lequel l'application immédiate de la loi nouvelle de procédure est sans effet sur la validité des actes accomplis conformément à la loi ancienne. D'une façon plus générale, le principe de sécurité juridique est à la base du système juridictionnel national et du droit de l'Union.

- garantir l'objectif de valeur constitutionnelle de la bonne administration de la justice qui résulte des articles 12, 15 et 16 de la Déclaration de 1789 et impose, notamment, d'assurer la sécurité des procédures pénales, ainsi que l'a jugé le Conseil constitutionnel (Cons. Const. déc. n° 2016-741 DC 8 déc. 2016, Loi relative à la transparence, à la lutte contre la corruption et à la modernisation).

Cette jurisprudence parait aussi propre à assurer le respect des objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, largement utilisés[24] par le Conseil constitutionnel, dans le contentieux

---

avocat lors de ses auditions et l'obligation de lui notifier le droit de garder le silence, l'exigence de prévisibilité de la loi et l'objectif de bonne administration de la justice font obstacle à ce que les auditions réalisées à cette date, sans que la personne gardée à vue ait été assistée d'un avocat pendant leur déroulement ou sans qu'elle se soit vue notifier le droit de se taire, soient annulées pour ces motifs ; qu'il résulte, toutefois, des stipulations de l'article précité de ladite Convention que les déclarations incriminantes faites lors de ces auditions ne peuvent, sans que soit portée une atteinte irrémédiable aux droits de la défense, fonder une décision de renvoi devant la juridiction de jugement ou une déclaration de culpabilité ;

23

24

Cons. const., déc. n°2010-14/22 QPC du 30 juillet 2010 relative au régime général de la garde à vue ; déc.n° 2010-32 QPC du 22 sept. 2010, relative à la retenue douanière ; déc. n° 2013-357 QPC du 29 nov. 2013 relative à la visite des navires par les agents des douanes ; déc.n° 2014-420/421 du 9 oct. 2014 relative à la prolongation exceptionnelle de la garde à vue pour des faits d'escroquerie en bande organisée.

de la QPC, pour moduler dans le temps la portée de ses décisions et écarter l'abrogation immédiate d'une disposition lorsqu'une telle abrogation entrainerait des conséquences manifestement excessives au regard des objectifs précités.

La chambre pourra dès lors se demander si la jurisprudence précitée de 2018 peut être transposée au cas d'espèce, sans méconnaître le principe d'équivalence.

Convient-il de faire une application stricte de ce principe ou de concilier son application avec celui de sécurité juridique, reconnu en droit européen, ou avec les objectifs de valeur constitutionnelle précités ?

la prévisibilité des exigences de droit européen : quelle date retenir ?

Une telle solution conduirait à moduler la nature de la sanction de la méconnaissance des exigences du droit de l'Union européenne en fonction, d'une part, de la date de l'irrégularité - soit la date de la conservation des données et/ ou de leur communication- d'autre part, de la « prévisibilité » des exigences européennes en matière de conservation et d'accès aux données de connexion.

Si l'acte de conservation et/ou d'accès a été accompli à une date où les exigences de l'Union européenne ne paraissaient pas « prévisibles », le principe d'équivalence n'exigerait pas le prononcé de la nullité mais commanderait que les données ainsi collectées ou communiquées irrégulièrement ne fondent pas une décision de renvoi devant la juridiction de jugement ou une déclaration de culpabilité.

En revanche, si cet acte était postérieur, la sanction de l'irrégularité devrait être examinée dans le cadre du contentieux de la nullité, en application des règles procédurales propres à celui-ci.

Une telle approche conduirait la chambre à rechercher précisemment à quelle date les exigences européennes sur la conservation et l'accès peuvent être analysées comme ayant été « prévisibles » pour les acteurs de la procédure pénale.

Cette exigence de « prévisibilité » peut tre comprise d'une double façon :

Elle peut désigner le comportement de celui qui peut anticiper les conséquences juridique de ses actes à partir des **normes et jurisprudence existantes** ; elle peut comprendre aussi le pouvoir de **prévoir les évolutions du droit**. En droit pénal substantiel, lorsqu'est invoquée la violation du principe de non-rétroactivité pénale, la Cour de justice de l'Union européenne, tout comme la Convention européenne des droits de l'homme, intègre cette conception et prohibe les interprétations jurisprudentielles nouvelles « *dont le résultat n'était pas raisonnablement prévisible au moment où l'infraction a été commise, au vu notamment de l'interprétation retenue à cette époque dans la jurisprudence relative à la disposition légale en cause* » (CJUE,28 juin 2005, Dansk Rorindustri et autres c/ Commission, affaires C-189/02, point 218).

- Elle peut également faire l'objet d'une analyse plusieurs niveaux : s'agit-il de la « prévisibilité » de la seule jurisprudence de l'Union européenne ou convient-il d'intégrer l'analyse, le cas échéant, les jurisprudences précitées de la Convention européenne des droits de l'homme et du Conseil constitutionnel si celles-ci sont de nature faire naître l'incertitude sur la portée des arr ts de la Cour de justice de l'Union européenne ?

Comme précisé antérieurement (cf.1.2), les exigences européennes sur la conservation et l'accès aux données de connexion sont le produit d'arrêts successifs de la Cour de justice de l'Union européenne interprétant un droit de l'Union demeuré constant. Elles sont également la concrétisation du **dialogue des juges** qui a conduit de nombreux Etats de l'Union européenne à interroger la Cour de justice de l'Union européenne sur les premiers arrêts rendus sur cette thématique afin de lui en faire préciser la portée, notamment au regard de la lutte contre la criminalité grave.

A cet égard, on peut relever, en substance, que :

- s'agissant de la conservation des données, la Cour de justice de l'Union européenne, dans sa décision Tele 2 Sverige du 21 décembre 2016 (aff. jointes C-203/15 et C- 698/15), a dit pour droit que l'article 15§1 de la directive 2002/58, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52§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 prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électroniques* » (point 112). La chambre a d'ailleurs repris ce point dans son arrêt du 1er avril 2020 par lequel elle a saisi la Cour de justice de l'Union européenne d'une question préjudicielle relative aux pouvoirs des enquêteurs de l'AMF (Crim., 1 avril 2020, pourvoi n° 19-80.908).

- s'agissant des conditions d'accès aux données conservées, dans ce même arrêt, la Cour de justice a énoncé que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux, devait « *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* ».

Sans constituer des revirements jurisprudentiels, les arrêts « La Quadrature du Net » pour la conservation des données, et « Prokuratuur » pour l'accès aux données, ont apporté des précisions importantes[25] :

- le premier a introduit la réserve de la sauvegarde de la sécurité nationale permettant aux Etats d'imposer la conservation généralisée et indifférenciée des données de connexion en cas de menace grave ainsi que celle de la « conservation rapide » ; en outre, cet arrêt a été rendu sur question préjudicielle de la France et donc au regard des normes de droit français.

25

Le résumé de l'arrêt « La Quadrature du Net » par la Cour de justice de l'Union européenne relève que la jurisprudence Tele 2 a suscité les préoccupations de certains Etats craignant d'avoir été privés d'un instrument qu'ils estiment nécessaire à la sauvegarde de la sécurité nationale et de la lutte contre la criminalité (...) En outre, tout en confirmant sa jurisprudence issue de l'arrêt Tele2 Sverige et Watson e.a., sur le caractère disproportionné d'une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, la Cour apporte des précisions, notamment, quant à l'étendue des pouvoirs que reconnaît cette directive aux États membres en matière de conservation de telles données aux fins précitées ».

- le second a précisé la notion d'autorité administrative indépendante et en a conclut que le ministère public estonien ne remplissait pas les conditions d'indépendance.

La jurisprudence de la Cour de justice de l'Union européenne était-elle prévisible dès l'arrêt Tele 2 ou ne l'était-elle qu'à compter des arrêts précités ?

Par ailleurs, selon la Cour de justice de l'Union européenne, l'autorité dont est revêtu un arrêt rendu en matière préjudicielle ne fait pas obstacle à ce que le juge national destinataire de cet arrêt puisse estimer nécessaire de saisir de nouveau la Cour avant de trancher le litige au principal (arrêt du 6 mars 2003, Kaba, C 466/00; point 39). Un tel renvoi s'impose à une juridiction nationale statuant en dernier ressort lorsqu'elle se heurte à des difficultés de compréhension quant à la portée de l'arrêt de la Cour. En revanche, une telle juridiction peut s'abstenir de soumettre à la Cour une question d'interprétation du droit de l'Union et la résoudre sous sa propre responsabilité lorsque l'interprétation correcte du droit de l'Union s'impose avec une telle évidence qu'elle ne laisse place à aucun doute raisonnable. Doit-on en déduire que tant que la Cour de cassation n'a pas statué dans un pourvoi la conduisant à appliquer le droit de l'Union, tel qu'interprété par la Cour de justice de l'Union européenne, l'interprétation du droit européen laisse place à une incertitude de nature à justifier l'application de la jurisprudence de 2018 ?

3.4.3 : les conditions du prononcé de la nullité

Si la chambre juge que le principe d'équivalence doit conduire la chambre de l'instruction à examiner la sanction de la méconnaissance des exigences de l'Union européenne à l'aune des nullités, elle devra s'assurer que cette juridiction a appliqué la méthodologie propre à ce contentieux, telle qu'elle a été conceptualisée dans ses arrêts du 7 septembre 2021 (pourvois n° 21.80-642 et 20.97-191, en cours de publication).

Il résulte de ceux-ci que, hors les cas de nullité d'ordre public, qui touchent à la bonne administration de la justice, 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.

- *nullité d'ordre public ou d'ordre privé*

En premier lieu, la chambre devra dire si la conservation de façon générale et indifférenciée des données de connexion ou l'accès à de telles données, de façon contraire au droit de l'Union, constitue une nullité d'ordre public. La chambre criminelle a récemment énoncé que les nullités d'ordre public « *touchent à la bonne administration de la justice* » (Crim., 7 septembre 2021, n°21-80.642 et 20-87.191 ; cf. aussi Crim., 14 octobre 2003, pourvoi n° 03-84.539, Bull. crim. 2003, n° 187).

Il résulte d'une jurisprudence ancienne de la chambre et confirmée récemment que l'absence d'autorisation du procureur de la République pour requérir des experts, en violation des dispositions de l'article 77-1 du code de procédure pénale, est constitutive d'une nullité à laquelle les dispositions de l'article 802 dudit code sont étrangères dès lors que celles-ci sont édictées en vue de garantir la fiabilité de la

recherche et de l'administration de la preuve (Crim., 14 octobre 2003, pourvoi n° 03-84.539, Bull. crim. 2003, n° 187- (Crim., 18 juin 2019, pourvoi n° 19-80.105, Bull. crim 2019, n° 121).

La chambre a jugé également qu'un officier de police judiciaire, en enquête préliminaire, ne peut présenter les 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, la méconnaissance de ces dispositions étant là encore constitutive d'une nullité d'ordre public (Crim., 1 septembre 2005, pourvoi n° 05-84.061, Bull. crim. 2005, n° 211 - Crim., 6 décembre 2005, pourvoi n° 05-85.076, Bull. crim. 2005, n° 319).

Cette jurisprudence parait néanmoins avoir été abandonnée dans un arrêt récent du 6 février 2018 (pourvoi n° 17-84.380, Bull. crim. 2018, n° 30) dans lequel la chambre a jugé qu'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.

On observera également que, dans de très nombreux arrêts, la chambre a exclu qu'une partie, dont la vie privée n'avait pas été atteinte par l'acte critiquée, soit recevable à agir en nullité (cf. paragraphe suivant sur la qualité à agir).

S'agissant spécifiquement des exigences européennes en matière de conservation, la Cour de justice les justifie par les risques « *d'abus et d'accès illicite* » (point 119 de la « La Quadrature du Net ») ; quant à l'exigence d'un contrôle préalable de l'accès aux données par une autorité administrative indépendante ou une juridiction, la Cour de justice l'explique par la nécessité de garantir le respect des conditions matérielles et procédurales propres à assurer le principe de proportionnalité (point 51 de « Prokuratuur »).

C'est au vu de ces observations que la chambre appréciera si les exigences européennes en matière de conservation de données et d'accès sont d'ordre privé ou d'ordre public.

Si la chambre exclut que l'on soit en présence d'une nullité d'ordre public, elle devra s'interroger sur la qualité à agir du requérant.

qualité agir du requérant

La chambre juge que 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 consultation du LAPI : Crim., 5 octobre 2021, pourvoi n° 21-82.399 ; d'un dispositif de captation d'images : Crim., 13 octobre 2020, pourvoi n° 19-87.959). Tel est le cas également en matière de réquisitions (cf. arrêt du 6 février 2018 précité).

La chambre appréciera dès lors si M. [U] a qualité pour agir en nullité de la totalité des réquisitions délivrées soit en ce qu'elles portent sur des données conservées de façon contraire au droit de l'Union, soit en ce que le juge d'instruction ne pouvait autoriser les officiers de police judiciaire à en demander communication.

existence du grief

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.

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 appréciera quel peut être le grief en cas de conservation illicite des données ainsi qu'en cas d'accès illicite à ces données, qu'elles aient été licitement ou non conservées. On observera à cet égard que la Cour de justice de l'Union européenne, dans son analyse du principe d'effectivité, n'opère pas de distinction selon que la méconnaissance du droit de l'Union résulte de la conservation générale et indifférenciée des données ou de l'accès à ces données par les autorités publiques.

Pour la chambre criminelle, *« l'existence d'un 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).

Il appartient au requérant de justifier du grief.

Trois approches semblent a priori possible :

- la première analyserait le grief au regard de <u>l'atteinte à la vie privée</u> ou/et de l'absence ou de l'insuffisance du contrôle du juge sur l'atteinte ainsi portée à la vie privée :

La chambre tend à juger que l'absence de motivation d'un acte gravement attentatoire à la vie privée fait nécessairement grief à l'intéressé dans la mesure où elle interdit tout contrôle réel et effectif de la mesure (ainsi, de l'absence de motivation d'une mesure de perquisitions hors des heures légales : Crim., 8 juillet 2015, pourvoi n° 15-81.731, Bull. crim. 2015, n° 174 ou de l'ordonnance, prévue par l'article 706-96 du code de procédure pénale, par laquelle le juge d'instruction autorise les officiers de police judiciaire agissant sur commission rogatoire à mettre en place un dispositif technique de captation et d'enregistrement des paroles prononcées à titre privé ou confidentiel : Crim., 9 janvier 2018, pourvoi n° 17-82.946, Bull. crim. 2018, n° 4 ; Crim., 6 janvier 2015, pourvoi n° 14-85.448, Bull. crim. 2015, n° 5).

Il en est de même dans l'hypothèse où un élément essentiel au contrôle du juge, telle la durée de la mesure attentoire à la vie privée, n'a pas été mentionné (Crim., 9 janvier 2018, pourvoi n° 17-82.946, Bull. crim. 2018, n° 4).

- la seconde analyserait le grief au regard du <u>seul principe du procès équitable</u>.

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). La nullité ne serait dès lors prononcée que s'il apparaissait, après expertise, le cas échéant, que les données avaient été attribuées par erreur au requérant.

-la troisième repose sur la définition du grief, telle qu'elle résulte de la jurisprudence récente de la chambre criminelle.

Dans son arrêt précité du 7 septembre 2021, la chambre énonce que l'existence d'un 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**.

Il va de soit qu'un tel grief est exclu lorsque la méconnaissance des règles de conservation est demeurée sans conséquence, de telles données n'ayant pas fait l'objet d'une demande de communication.

Par ailleurs, dans l'arrêt « Prokuratuur » (point 49), la Cour de justice justifie l'exigence d'un contrôle préalable par une juridiction ou une autorité administrative indépendante par la nécessité de garantir le « *plein respect* » des conditions matérielles et procédurales régissant l'utilisation des données :

- l'accès ne peut porter que sur des données régulièrement conservées ;

- l'accès doit respecter les normes procédurales prévues en droit interne ;

- l'accès doit être circonscrit à des procédures visant à la lutte contre la criminalité grave ;

- l'accès ne doit être accordé 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 ;

- un juste équilibre doit être assuré 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.

Ne peut-on pas en déduire que le grief est caractérisé dès lors que la personne mise en examen justifie de la violation de l'une de ces conditions qu'il aurait appartenu à une autorité administrative indépendante ou à une juridiction de vérifier ? Et, inversement, que si la personne mise en examen n'allègue pas la violation de l'une de ces conditions, elle ne peut se prévaloir d'un grief pris de l'absence de contrôle préalable par une de ces autorités ? L'irrégularité de l'absence de contrôle par une juridiction ou une autorité administrative indépendante ne ferait ainsi grief que s'il était établi qu'un accès aux données n'aurait pas dû être autorisé.

Une telle solution ne conduit pas à substituer à l'exigence d'un contrôle préalable un contrôle a-posteriori, ce que prohibe la Cour de justice de l'Union européenne, mais à constater, conformément à la jurisprudence de la chambre, que l'irrégularité - en l'espèce la violation du droit européen - n'a pas causé un grief à l'intéressé, de sorte que les conditions du prononcé de la nullité ne sont pas réunies.

On observera qu'en l'espèce, le requérant allégue comme grief que les lignes qui lui ont été attribuées l'ont été sur la base de données de connexion illicitement conservées.