COUR DE CASSATION

AVIS DE M. DESPORTES, AVOCAT GÉNÉRAL

Arrêt n° 769 du 12 juillet 2022 – Chambre criminelle

Pourvoi n° 21-83.710

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

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

_____

Faits et procédure

Le 24 août 2019 à [Localité 5], appelés sur les lieux d'un crime commis dans un parking souterrain, les policiers ont découvert, sur le siège conducteur d'un véhicule, le corps criblé de balles de [D] [P]. L'exploitation de la vidéosurveillance a très vite révélé qu'une autre personne, venue à la rencontre de la victime, avait été visée par les coups de feu. Les investigations ont été engagées le jour même des faits, en flagrance, puis, à compter du 6 septembre 2019, dans le cadre d'une information ouverte à cette date. Tant en flagrance, sur le fondement de l'article 60-1 du code de procédure pénale, que sur commission rogatoire du juge d'instruction, sur le fondement de l'article 99-3 du même code, les enquêteurs de la brigade criminelle de la préfecture de police de Paris ont procédé à de très nombreuses réquisitions auprès des opérateurs de téléphonie aux fins d'exploiter les données de trafic et de localisation afférentes à plusieurs lignes téléphoniques.

Le travail considérable, minutieux et complexe, auquel ils se sont livrés ne peut être retracé dans son détail. Les enquêteurs ont d'abord sollicité des opérateurs de téléphonie mobile le détail du trafic des communications passées par les antennes les plus proches de trois lieux distincts : celui du crime, celui de la découverte du véhicule ayant été utilisé pour la commission du crime et celui du domicile de la victime décédée. En croisant les données révélées lors de ce triple "bornage", ils ont découvert un numéro de téléphone commun à partir duquel ils ont pu déterminer le magasin où avait été acheté le téléphone associé, exploiter les vidéosurveillances installées à proximité et identifier d'autres lignes téléphoniques utilisées pour la commission du crime.

Le 26 juin 2020, M. [C][L][E] a été mis en examen des chefs de meurtre en bande organisée, tentative de meurtre en bande organisée, destruction d'un bien appartenant à autrui par un moyen dangereux pour les personnes, recel en bande organisée, participation à une association de malfaiteurs.

Le 28 décembre 2020, il a déposé, sur le fondement de l'article 173 du code de procédure pénale, une requête aux fins d'annulation d'actes de la procédure. En substance, il a soutenu que les réquisitions aux fins de communication de données de connexion relatives aux lignes dont il avait l'usage étaient irrégulières dès lors que, d'une part, elles portaient sur des données conservées en violation du droit de l'Union européenne et que, d'autre part, pendant l'enquête de flagrance, elles avaient été délivrées sans l'autorisation préalable d'un juge en méconnaissance des exigences découlant de la Convention européenne de sauvegarde des droits de l'homme.

Par arrêt n° 3 du 27 mai 2021, la chambre de l'instruction de Paris a rejeté la demande d'annulation.

M.[L][E] a formé contre cet arrêt un pourvoi dont le président de la chambre criminelle a prescrit l'examen immédiat.

A l'occasion de son pourvoi, il a soumis à votre chambre une question prioritaire de constitutionnalité dirigée contre les dispositions de l'article L. 34-1 du code des postes et communications électroniques qui, dans sa rédaction alors applicable, imposait aux opérateurs téléphoniques une conservation généralisée et indifférenciée des données de connexion pendant une durée d'un an pour les besoins de la lutte contre la délinquance. Par arrêt du 7 décembre 2021, votre chambre a renvoyé cette question au Conseil constitutionnel qui, par sa décision n° 2021-976/977 QPC du 25 février 2022, a déclaré contraires à la Constitution les dispositions critiquées et, aménageant l'application dans le temps de sa décision, précisé que les mesures prises en application de ces dispositions ne pourraient être contestées sur le fondement de la déclaration d'inconstitutionnalité.

Moyens de cassation

Les trois moyens de cassation qui vous sont proposés sont dirigés contre les motifs par lesquels la chambre de l'instruction a écarté la demande d'annulation des réquisitions en matière de téléphonie. Ils critiquent, respectivement sur le fondement de la Constitution, du droit de l'Union et de la Convention européenne de sauvegarde des droits de l'homme, les motifs de l'arrêt attaqué relatifs à la régularité de la conservation des données auxquelles les enquêteurs ont eu accès. Dans son troisième moyen, le demandeur critique en outre les motifs de l'arrêt attaqué relatifs à la régularité de l'accès à ces données.

Le présent pourvoi, qui vient devant vous avec plusieurs autres portant sur les mêmes questions, vous donne l'occasion de lever l'incertitude qui, depuis l'arrêt de la Cour de justice de l'Union européenne *Tele 2 Sverige* du 21 décembre 2016, pèse sur la conformité au droit de l'Union des dispositions de procédure pénale encadrant l'accès aux données de connexion et leur conservation. Les moyens du pourvoi vous invitent ainsi à examiner :
- d'une part, si les données de connexion dont les enquêteurs, agissant en flagrance puis sur commission rogatoire, ont obtenu la communication, étaient conservées par les opérateurs dans des conditions conformes au droit de l'Union ;
- d'autre part, si les enquêteurs ont eu accès à ces données sans méconnaître les exigences de ce même droit.

Mais avant d'entrer dans la discussion relative à chacune de ces deux questions quelques observations communes peuvent être faites.

1. OBSERVATIONS COMMUNES AUX QUESTIONS POSEES

1.1.- Principaux éléments du débat

1.1.1.- Dispositif législatif applicable en la cause

La possibilité, au cours de la procédure pénale, de délivrer des réquisitions afin d'accéder aux données de connexion est prévue, pendant l'enquête de flagrance, aux articles 60-1 et 60-2 du code de procédure pénale, pendant l'enquête préliminaire, aux articles 77-1-1 et 77-1-2 du même code et, pendant l'information, à ses articles 99-3 et 99-4. Si ces textes assez généraux relatifs aux réquisitions tendant à l'obtention d'informations ne visent pas spécialement la communication de telles données, votre chambre a admis qu'ils s'y appliquaient[1].

Les articles 60-1, 77-1-1 et 99-3 régissent les réquisitions qu'on pourrait qualifier d'ordinaires tandis que les articles 60-2, 77-1-2 et 99-4 encadrent les réquisitions dites informatiques ou télématiques qui permettent d'accéder aux données de connexion en *"intervenant par voie télématique ou informatique*" auprès des destinataires, notamment les "opérateurs de communications électroniques"[2], le cas échéant par l'intermédiaire de la plate-forme nationale des interceptions judiciaires (PNIJ), désormais passage obligé en la matière[3].

Les modalités procédurales selon lesquelles, ces réquisitions peuvent être délivrées varient selon le stade de la procédure. En flagrance, selon les articles 60-1 et 60-2, les réquisitions peuvent être délivrées sans autorisation préalable d'un magistrat, par un officier de police judiciaire ou, depuis la loi dite LPJ du 23 mars 2019[4], par un agent de police

[1] Crim. 22 nov. 2011, n° 11-84.308

[2] Art. R. 15-33-68 CPP

[3] Art. 230-45 CPP

[4] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice

judiciaire agissant sous son contrôle. Au stade de l'enquête préliminaire, les articles 77-1-1 et 77-1-2 imposent l'autorisation préalable du procureur de la République. Enfin, au cours de l'information, en vertu des articles 99-3 et 99-4, c'est la commission rogatoire du juge d'instruction qui autorise l'officier de police judiciaire délégataire à procéder à des réquisitions[5].

L'accès instantané aux données de connexion aux fins de géolocalisation en temps réel de l'objet - par exemple, un téléphone - qui les émet échappe aux prévisions de cet ensemble de textes. Il est régi spécifiquement et de manière nettement plus élaborée, par les articles 230-32 et suivants du code de procédure pénale.

Par ailleurs, les données de connexion auxquelles pouvaient accéder les magistrats et enquêteurs pour les besoins de la recherche des auteurs d'infraction étaient désignées, à la date des réquisitions litigieuses, à l'article L. 34-1 du code des postes et communications électroniques (CPCE) dans sa rédaction issue de la loi n° 2013-1168 du 18 décembre 2013 et antérieure à la loi n° 2021-998 du 30 juillet 2021[6]. En son paragraphe II, cet article pose en principe que les opérateurs de communications électroniques doivent effacer ou rendre anonyme toute donnée relative au trafic. Ce principe est toutefois assorti de plusieurs exceptions. En particulier, dans sa rédaction, applicable en la cause, issue de la loi du 18 décembre 2013, l'article L.34-1, paragraphe III, prévoit que "*pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales* (...), *il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonyme certaines catégories de données techniques*" désignées par voie réglementaire.

1.1.2.- Remise en cause du dispositif par la Cour de justice de l'Union européenne

Ce dispositif a été ébranlé au cours de ces dernières années par une suite de décisions de la Cour de justice de l'Union européenne introduite par son arrêt précurseur du 8 avril 2014, *Digital Rights Ireland Ldt* (C-293/12 et C-594/12), par lequel elle a annulé la directive 2006/24/CE du 15 mars 2006 sur la conservation des données[7]. Les solutions qui étaient en germe dans cet arrêt ont été consacrées, explicitées et affinées par cinq arrêts des 21 décembre 2016, *Tele 2 Sverige et Watson* (C-203/15 et C-698/15), 2 octobre 2018, *Ministerio Fiscal* (C-207-16), 6 octobre 2020, *La Quadrature du net, French Data Network* et a. (C-511/18, C-512/18, C-520/18), *2* mars 2021*, H.K./Prokuratuur* (C-746/18) et, enfin, 5 avril 2022*, G.D./Commissioner of An Garda Síochána* (C-140/20). Tous ces arrêts ont été rendus en grande chambre.

Saisie de questions préjudicielles, la Cour a été appelée dans ces différentes affaires à apprécier la portée des dispositions de l'article 15, paragraphe 1, de la directive

---

[5] On mentionnera que ces distinctions procédurales s'effacent aujourd'hui lorsque les réquisitions portent sur des données de connexion émises par un avocat. Elles doivent alors êtres "faites par ordonnance motivée du juge des libertés et de la détention" en vertu de l'article 60-1-1 issu de la loi n° 2021 -1729 du 22 décembre 2021, auquel se réfèrent les articles précités.

[6] 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 ; Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement

[7] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE

2002/58/CE du 12 juillet 2002[8] dite vie privée et communication électronique, qui, "*pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'Etat - la défense de la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*", ménagent aux Etats membres la possibilité d'apporter des limitations aux règles tendant à assurer la confidentialité ou l'effacement des données.

Analysant ces dispositions à la lumière de celles de la Charte des droits fondamentaux et considérant l'exigence de proportionnalité, la Cour a retenu, en substance :
- d'une part, qu'elles s'opposent à ce que les Etats imposent aux opérateurs, pour la lutte contre la criminalité, une conservation généralisée et indifférenciée des données de trafic et de localisation ;
- d'autre part, qu'elles imposent que l'accès à ces données soit autorisé par une juridiction ou une autorité administrative indépendante.

Les décisions précitées, qui ont suscité un certain émoi parmi les Etats membres, ont déterminé de nombreuses questions préjudicielles que nous ne passerons pas en revue. Pour ce qui est de la France, une question, posée par le Conseil d'Etat est à l'origine, avec une autre posée par la Cour constitutionnelle belge, de l'arrêt précité de la Cour de Justice du 6 octobre 2020, *La Quadrature du Net*. Vous-mêmes en avez posé une relative à l'accès aux données de connexion pour la lutte contre les abus de marché, invitant la Cour de justice à se prononcer sur l'articulation entre la directive 2002/58/CE et les textes du droit dérivé incitant les Etats à recourir aux données de connexion pour les besoins de cette lutte[9]. Cette question est en cours d'examen.

1.1.3.- Conséquences tirées par le Conseil d'Etat et le législateur

Dans son arrêt du 21 avril 2021, *French Data Network et a*, Le Conseil d'Etat, statuant sur la conformité au droit de l'Union des dispositions réglementaires d'application de l'article L. 34-1 CPCE, a tiré les conséquences des réponses apportées à ses questions préjudicielles par la Cour de justice dans son arrêt précité *La Quadrature du Net*[10]. A la lumière des solutions dégagées par le Conseil d'Etat, le législateur a refondu, par la loi n° 2021-998 du 30 juillet 2021[11], les dispositions de l'article L. 34-1 CPCE qui prévoyaient la conservation généralisée et indifférenciée des données de connexion pendant un an pour les besoins de la lutte contre la criminalité. Rappelons qu'au regard de la norme constitutionnelle, statuant sur une question prioritaire de constitutionnalité soulevée dans la présente procédure, le Conseil constitutionnel, rejoignant la position de la Cour de justice, a retenu, par sa décision déjà citée n° 2021-976/977 QPC du 25 février 2022 que les dispositions de l'article L. 34-1 dans leur rédaction antérieure à la loi précitée portaient une atteinte excessive au droit au respect à la vie privée en tant qu'elles imposaient une conservation trop peu encadrée des données de connexion pour les besoins de la lutte contre la criminalité

---

[8] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

[9] Crim. 1er avr. 2020, n° 19-80.908 ; Crim. 1er avr. 2020, n° 19-82.222 ; Crim. 1er avr. 2020, n° 19-82.223

[10] CE 21 avr. 2021, *French Data Network et a*., n° 393099, 394922,397844, 397851,424717,424718, Rec., sur les conclusions d'Alexandre Lallet

[11] Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement

En revanche, le législateur n'a pas modifié la répartition entre enquêteurs, procureur de la République et juge d'instruction, telle que prévue par les articles précités du code de procédure pénale pour l'accès aux données. Il s'est borné à entourer cet accès de garanties supplémentaires par la loi n° 2022-299 du 2 mars 2022[12] en énumérant à l'article 60-1-2 de ce code, auquel se réfèrent les articles 77-1-1 et 99-3, les cas dans lesquels il est autorisé. Cette modification tend d'ailleurs moins à tirer les conséquences de la jurisprudence européenne que de la censure partielle de l'article 77-1-1 prononcée par le Conseil constitutionnel dans sa décision n° 2021-952 QPC du 3 décembre 2021. Si le législateur a subordonné, par la loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire, l'accès aux données de connexion émises par un avocat à une autorisation du juge des libertés et de la détention, quel que soit le cadre des investigations, cette modification, limitée, répond à d'autres préoccupations que celles tenant à la nécessité de se conformer au droit de l'Union (art. 60-1-1 CPP auquel renvoient les autres textes).

1.1.4.- Enjeux pour la conduite des procédures et éléments de droits comparé

Pour mesurer l'importance des enjeux attachés aux arrêts que vous rendrez, il suffit de rappeler que, selon les indications données par le ministère de la justice, en 2021, 1 726 144 réquisitions ont été délivrées aux fins d'accéder en temps différé à des données de connexion. Ce nombre était de 1 531 918 en 2019 et de 1 577 889 en 2020. En 2021, pour un peu plus de la moitié, ces réquisitions ont été délivrées dans le cadre d'enquêtes préliminaires et donc sur autorisation du procureur de la République et près de 20 % dans le cadre d'enquêtes de flagrance, et donc sur décision d'un officier de police judiciaire, la dernière part, soit environ 30% l'ayant été sur commission rogatoire du juge d'instruction. Le plus souvent les réquisitions portent sur les "fadettes" (factures détaillées) donnant des indications nombreuses sur les communications afférentes à une ligne téléphonique. Comme l'a relevé le Conseil d'Etat, "*l'accès différé aux données de connexion revêt une importance d'autant plus cruciale que l'utilisation des moyens de communications électroniques, notamment cryptées, constitue un instrument qui facilite la commission* [des] *crimes et délits et rend plus difficile la recherche de leurs auteurs*"[13]. Autant dire que l'exploitation des données de connexion, qui manifeste l'adaptation des unités et services de police judiciaire aux modes de communication désormais utilisés pour la préparation et la commission des crimes et délits, est devenue l'un des principaux moyens mis en oeuvre pour la recherche de la vérité dans les procédures pénales. La présente espèce en est d'ailleurs une parfaite illustration.

Selon une étude de droit comparé, les initiatives prises par les législateurs des Etats membres pour tirer les conséquences des arrêts de la Cour de justice sont assez diverses à la fois dans leur ampleur et dans leur nature. En Belgique, un projet de loi a été déposé pour rétablir un cadre juridique conforme à la jurisprudence européenne. Il est notamment prévu d'organiser une conservation ciblée des données de connexion pour la lutte contre la délinquance, dont nous verrons qu'elle est autorisée par la Cour de justice. En Allemagne, le choix a été fait de réduire drastiquement le type de données conservées ainsi que la durée de l'obligation de conservation. L'Autriche a mis en place un dispositif de "conservation rapide" - ou encore *quick freeze* - également autorisé par la Cour. Sur injonction délivrée aux opérateurs, les données peuvent être retenues pour une durée

[12] Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire

[13] CE, 21 avr. 2021, *French Data Network* préc., n° 50

maximale d'un an. Un accès y est ensuite possible pour la lutte contre les infractions graves. Aux Pays-Bas, depuis l'arrêt *Digital Rights* de 2014, le droit néerlandais n'impose plus aux fournisseurs d'un service de télécommunications l'obligation de conserver des données. L'Espagne et l'Italie maintiennent quant à elles un système de conservation généralisée et indifférenciée.

1.2.- Eléments de délimitation du débat

1.2.1- Diversité des données de connexion et fondement du régime de protection

Comme cela est rappelé au rapport, il est possible de distinguer trois catégories de données de connexion : les données d'identification qui permettent de déterminer l'identité de l'utilisateur ou du titulaire d'un numéro de téléphone, d'une carte SIM, d'une adresse IP ou d'une adresse mail ; les données relatives au trafic qui permettent de déterminer les contacts d'une personne, la date, l'heure et la durée de l'échange ; les données de localisation qui permettent de connaître les zones d'émission et de réception d'une communication et d'obtenir la liste des appels ayant "borné" à la même antenne relais. En l'espèce, les réquisitions litigieuses portent sur des données de trafic et de localisation

Les données de connexion, qui s'analysent en des métadonnées, permettent donc de connaître l'auteur ainsi que les circonstances de temps et de lieu d'une communication mais ne livrent aucune indication sur le contenu des échanges. Si néanmoins leur conservation et leur diffusion doivent être entourées de garanties, c'est que les informations qu'elles révèlent permettent de reconstituer la vie privée de ceux dont elles sont issues. Il en est ainsi tout spécialement des données de trafic et de localisation. Pour reprendre les mots de la Cour de justice de l'Union européenne : "*les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé* (...). *Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications*."[14] De manière plus concise, le Conseil constitutionnel a fait la même analyse dans ses décisions n° 2021-952 QPC du 3 décembre 2021 (§ 11) et n° 2021-976/977 QPC du 25 février 2022 (§ 11).

1.2.2.- Notion de criminalité grave déterminant la disponibilité de certaines données

En raison des éléments de la vie privée qu'elles révèlent, la Cour de justice de l'Union européenne, exerçant son contrôle de proportionnalité, juge que la plupart des données de trafic et les données de localisation ne peuvent être conservées et exploitées pour les

[14] CJUE, *Digital Rights*, point 27 ; CJUE, *Tele 2*, point 99 ; CJUE *La Quadrature du Net,* point 117 ; CJUE *Commissioner of An Garda Síochána*, point 45

besoins des procédures pénales qu'aux fins de lutte contre la "*criminalité grave*"[15]. Semblable condition se retrouve dans la décision précitée du Conseil constitutionnel[16]. Dans cette formulation ou une autre, elle n'était pas requise par les textes en vigueur à la date des réquisitions litigieuses. Cependant, quelle que soit la conception que l'on peut en avoir, il n'y a guère de doute qu'elle est satisfaite en l'espèce, les infractions, objet de la poursuite, se situant au sommet de l'échelle de la gravité. Il peut néanmoins apparaître souhaitable que vous précisiez les critères de reconnaissance de la criminalité grave dès lors que la question risque fort de se poser aux juridictions du fond dans des cas de figure moins évidents que dans la présente affaire. Dans ses conclusions devant la Cour de justice dans l'affaire *Ministerio fiscal*, l'avocat général a estimé que la criminalité grave ne constituait pas une notion autonome du droit de l'Union. Il a fait valoir, notamment, qu'en son article 1er, la directive 2006/24/CE sur la conservation de données, invalidée par l'arrêt *Digital Rights Ireland* du 8 avril 2014, renvoyait, pour cette qualification, au droit interne des Etats membres, dont la spécificité était ainsi ménagée. Il a mis également en avant la solution retenue par la Cour pour l'interprétation de la notion de "*sauvegarde de la sécurité publique*"[17]. Vous avez donc une certaine latitude pour la définition des contours de la notion. S'il paraît difficile d'y inclure les infractions qui ne seraient pas passibles d'emprisonnement, la catégorie déborde très largement les atteintes les plus graves aux personnes ou encore la criminalité organisée.

Afin de prendre en compte l'exigence relative à la gravité de l'infraction découlant tant du droit de l'Union que de la Constitution, le législateur, par la loi n° 2022-299 du 2 mars 2022, a introduit à l'article 60-1-2 du code de procédure pénale des dispositions cantonnant la possibilité d'accéder à un certain nombre de données - dont les données de trafic et de localisation - aux procédure portant sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement. Ce seuil correspond à celui retenu pour la mise en oeuvre d'autres mesures attentatoires à la vie privée, pour certaines comparables, comme la géolocalisation qui implique un accès aux données de connexion en temps réel (art. 230-32 CPP) et, pour d'autres, plus intrusives, comme les interceptions de correspondance (art. 100 CP), ou encore les perquisitions (art. 76 CPP) qui permettent d'accéder à des "contenus". Dans un souci de clarté et de cohérence, ce seuil pourrait également être retenu par votre chambre, en quelque sorte par anticipation, lorsque sont contestées des réquisitions aux fins de communication de données de trafic ou de localisation délivrées avant l'entrée en vigueur de la loi du 2 mars 2022 et donc à une période où aucune disposition législative ne fixait le champ de la mesure quant aux infractions.

---

[15] CJUE, *Tele 2, point 102* ; CJUE, *La Quadrature du Net,* point 140 ; CJUE, *Ministerio fiscal*, point 54 *;* CJUE, *Prokuratuur, point 35* ; CJUE *Commissioner of An Garda Síochána* , point 45 ; v. aussi avis 1/15, Accord PNR UE-Canada, 26 juill. 2017, point 149

[16] Déc. n° 2021-976/977 QPC, 25 févr. 2022 (§ 12) pour la conservation ; Déc. 2021-952 QPC, 3 déc. 2021, implicitement pour l'accès

[17] CJUE 22 mai 2012, P.I., C-348/09, points 21 à 23 : «*Le droit de l'Union n'impose pas aux États membres une échelle uniforme de valeurs en ce qui concerne l'appréciation des comportements pouvant être considérés comme contraires à la sécurité publique* » et que « *les États membres restent libres de déterminer, conformément à leurs besoins nationaux pouvant varier d'un État membre à l'autre et d'une époque à l'autre, les exigences de l'ordre public et de la sécurité publique, notamment en tant que justification d'une dérogation au principe fondamental de la libre circulation des personnes* », mais « *ces exigences doivent, toutefois, être entendues strictement, de sorte que leur portée ne saurait être déterminée unilatéralement par chacun des États membres sans contrôle des institutions de l'Union européenne* »

Bien entendu, ce critère abstrait, tiré de la peine encourue, est insuffisant. Comme l'a relevé le rapporteur public du Conseil d'Etat dans l'affaire *la Quadrature du Net*, sa mise en oeuvre ne dispense pas d'une appréciation *in concreto*, portée par le juge au cas par cas, afin d'assurer le respect du principe de proportionnalité. Il ne s'agit là que d'une exigence constante, consacrée au sixième alinéa du III de l'article préliminaire du code de procédure pénale aux termes duquel : "a*u 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"*.

1.2.3.- Délimitation en l'espèce du champ de la contestation quant aux actes

Il importe enfin de délimiter, en l'espèce, le champ de la contestation articulée par le demandeur quant aux actes de la procédure. Si de très nombreuses réquisitions aux fins de communication de données ont été délivrées par les policiers de la brigade criminelle, seules celles portant sur les lignes téléphoniques dont il a reconnu avoir l'usage peuvent être contestées par M.[L][E]. Conformément à la jurisprudence constante de votre chambre, une partie n'est recevable à demander l'annulation d'une mesure attentatoire à la vie privée que si elle justifie d'un intérêt lui donnant qualité pour agir, cet intérêt tenant alors précisément en l'atteinte portée à sa vie privée. La solution appliquée en cas de sonorisation, perquisition ou captation d'image[18], vaut bien entendu en cas de captation de données de connexion[19]. Il n'y a pas à distinguer selon la nature de l'irrégularité invoquée. La solution s'applique dès lors que la formalité méconnue n'a d'autre objet que d'assurer la protection d'un droit propre. Ainsi, le fait que l'irrégularité consiste en l'absence d'autorisation délivrée par l'autorité compétente ne confère pas à la nullité qui pourrait en découler un caractère d'ordre public[20]. Il en résulte qu'au cas présent, les seules réquisitions dont M.[L][E] est recevable à demander l'annulation sont celles portant sur les trois lignes dont il a reconnu avoir l'usage[21]. Il s'agit des réquisitions ayant donné lieu aux procès-verbaux d'exploitation afférents à ces lignes, établis tant au cours de l'enquête de flagrance le 28 août 2019 (cotes D505 à D 508) qu'au cours de l'information, les 11 et 16 septembre 2019 (cotes D776 à D786 et D 791 à D797). Ce sont d'ailleurs ces procès-verbaux qui sont visés dans sa requête en nullité. Bien entendu, même dirigé contre ces réquisitions, un moyen de nullité ne serait pas recevable s'il était porté pour la première fois devant vous.

Sous le bénéfice de ces observations communes à l'ensemble des moyens, nous en venons à la première question posée : celle de la conformité au droit de l'Union des dispositions alors en vigueur relatives à la conservation des données de connexion et des conséquences d'une éventuelle non conformité.

---

[18] v. entre beaucoup d'autres : Crim. 23 janv. 2013, n° 12-85.059, B., n° 29 ; Crim. 14 oct. 2015, n° 15-81.765, P. ; Crim. 13 oct. 2020, n° 19-87.959 ; Crim. 5 oct. 2021, n° 21-82.399 ; Crim. 9 nov. 2021, n° 21-81.359

[19] Crim. 6 févr. 2018, n° 17-84.380, B. n° 30

[20] Crim. 23 nov. 2016, n° 16-81.904, B. n° 306 (défaut d'autorisation d'une perquisition) ; Crim. 6 févr. 2018, n° 17-84.380, B. n° 30 (défaut d'autorisation d'une réquisition téléphonique) ; Crim. 9 mai 2018, n° 17-86.558, B. n° 90 (défaut d'autorisation d'une géolocalisation) ; de la même façon le défaut d'autorisation d'une privation de liberté ne peut être invoqué que par celui a subi l'atteinte à sa liberté individuelle.

[21] xxxxxxxxxx 01, xxxxxxxxxx 02 et xxxxxxxxx 03

2. MOYENS TIRES DE LA NON-CONFORMITE AUX NORMES SUPERIEURES DE LA CONSERVATION DES DONNEES DE CONNEXION, OBJET DES REQUISITIONS LITIGIEUSES

2.1.- Sort des moyens tirés de la violation de la Constitution et de la Convention européenne des droits de l'homme

Comme cela a été indiqué, le demandeur conteste, respectivement dans ses premier, deuxième et troisième moyens, la conformité à la Constitution, au droit de l'Union européenne et à la Convention européenne de sauvegarde des droits de l'homme, des dispositions de l'articles L. 34-1 CPCE qui, dans leur rédaction applicable à la date des réquisitions litigieuses, imposaient aux opérateurs de téléphonie de conserver les données de trafic et de localisation pendant une durée d'un an pour les besoins de la lutte contre la criminalité.

Le premier moyen, tiré de l'inconstitutionnalité des dispositions considérées, apparaît inopérant[22]. Certes par sa décision n° 2021-976/977 QPC du 22 février 2022, rendue sur une QPC présentée par le demandeur dans la présente procédure, le Conseil constitutionnel a déclaré contraires à la Constitution les dispositions critiquées - nous y reviendrons - mais, faisant application des pouvoirs que lui confère l'article 62 de la Constitution, il a décidé que les mesures prises en application de ces dispositions ne pourraient être contestées sur le fondement de cette inconstitutionnalité dès lors que leur remise en cause pour un tel motif "*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 ailleurs, contrairement à ce qui est soutenu par le demandeur à son troisième moyen, si la Cour européenne des droits de l'homme a entendu entourer de garanties "de bout en bout" la collecte, la conservation et l'exploitation massive par l'autorité publique, des données de connexion pour les besoins de la prévention et de la répression des infractions, il n'apparaît pas qu'à ce jour, elle ait jugé contraire à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, la conservation de ces données par les opérateurs de téléphonie, pour ces besoins[23]. Le débat ouvert au regard de la Convention nous paraît absorbé par celui ouvert au deuxième moyen, au regard du droit de l'Union étant rappelé que, conformément au paragraphe 3 de l'article 6 du TUE, "*les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales* (...) *font partie du droit de l'Union en tant que principes généraux*". Ainsi, comme l'a rappelé la Cour de justice, "*il convient de tenir*

---

[22] Ou "sans objet", selon la réponse que vous apportez tant dans le cas où le Conseil a écarté le grief d'inconstitutionnalité que dans celui où, comme en l'espèce, il a admis le grief mais différé les effets de sa décision (Crim. 17 juin 2020, n° 19-86.535)

[23] v. CEDH, 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15 ; CEDH, *Centrum för Rättvisa c. Suède*, n° 35252/08 ; et dès avant : CEDH, 2 août 1984, *Malone c/ Royaume-Uni*, n° 8691/79 ; CEDH, 8 mai 2018, *Ben Faiza c/ France*, n° 31446/12

compte des droits fondamentaux de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimal"[24]*.*

Rappelons à cet égard que la question de la conformité au droit de l'Union des dispositions du CPCE, alors en vigueur, relatives à la conservation des données de connexion pour les besoins de la lutte contre la criminalité, a été examinée par le Conseil d'Etat dans son arrêt du 21 avril 2021, *French Data Network*. Cet arrêt, abondamment commenté[25], et les conclusions d'Alexandre Lallet qui l'éclairent[26], constituent bien évidemment des références majeures.

2.2.- Règles issues du droit de l'Union et leur transposition

2.2.1.- Principe de l'interdiction du stockage des données de connexion

- Le droit de l'Union

Comme l'a souligné la Cour de justice de l'Union européenne, "*la directive 2002/58 ne se limite pas à encadrer l'accès* [aux données de connexion] *par des garanties visant à prévenir les abus, mais consacre aussi, en particulier, le principe de l'interdiction de leur stockage par des tiers*"[27]. Ce principe est énoncé aux articles 5, paragraphe 1[28], et article 6, paragraphe 1[29], de la directive.

L'interdiction de stockage des données trouve bien entendu son fondement dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, garantis respectivement, dans le droit de l'Union, aux articles 7 et 8 de la Charte des droits fondamentaux. En outre, ainsi que l'a relevé la Cour de justice, l'interdiction tend également à préserver le droit à la liberté d'expression proclamé à l'article 11 de la Charte dans la mesure où le stockage est de nature à avoir un *"effet dissuasif sur l'utilisation des moyens de communication*"[30].

---

[24] not. CJUE, 6 oct. 2020, *La Quadrature du Net*, point124

[25] v. not. : Cl. Malverti et C. Beaufils, *L'instinct de conservation*, AJDA 2021, p. 1194 ; J. Roux, *La lucidité d'une fermeté ajustée*, Rec. Dall. 2021, p. 1247 ; M. Bartolucci, JCP Adm., 2021, n° 28 ; T. Douville et H. Gaudin, *Un arrêt sous le signe de l'exceptionnel*, Rec. Dall. 2021, p. 1268 ; RFDA, p. 570, chron. A. Roblot-Troizier ; RTD eur. 2021. 349, étude L. Azoulai et D. Ritleng ; AJ pénal 2021, 309, chron. A. Archambault ; Dalloz IP/IT 2021, 408, obs. B. Bertrand et J. Sirinelli ; Légipresse 2021. 253 et les obs.

[26] RFDA 2021. 421, concl. A. Lallet

[27] CJUE, 5 avr. 2022, C-140/20, § 39

[28] "*Les Etats membres* (...) *interdisent à toute autre personne que les utilisateurs* (...) *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*"

[29] *"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*"

[30] CJUE, 6 oct. 2020, *La Quadrature du Net*, pt 118

- Sa transposition

Le principe d'interdiction du stockage des données trouve sa transposition au paragraphe II, de l'article L. 34-1 CPCE, dans sa version applicable à la date des réquisitions contestées comme dans sa version actuelle. Les dispositions correspondantes, déjà évoquées, imposent aux opérateurs de communications électroniques, d'effacer ou de rendre anonyme toutes les données relatives au trafic. Au sens et pour l'application de ces dispositions, de telles données doivent s'entendre, selon la définition qu'en donne l'article L. 32, de "*toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation*". Cette formule large couvre, non seulement les données relatives aux échanges entre les usagers du réseau - qui correspondent aux données de trafic au sens strict - mais également les données de localisation et, bien entendu, les données d'identité.

2.2.2.- Limitations au principe d'interdiction

L'interdiction de stockage ainsi énoncée n'est pas absolue. Conformément à l'article 52, paragraphe 1er, de la Charte des droits fondamentaux, des limitations peuvent être apportées à ces droits "*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 liberté d'autrui*". Précisément, aussitôt après avoir posé le principe d'interdiction, l'article 6 de la directive réserve un certain nombre de dérogations. Il en est de même de l'article L. 34-1 du CPCE qui en est la transposition.

2.2.2.1.- Conservation des données pour les besoins des opérateurs

- Le droit de l'Union

En premier, lieu, selon les paragraphes 2 et 3 de l'article 6 de la directive, les opérateurs sont autorisés à traiter deux types de données de trafic pour des motifs commerciaux. Il s'agit d'abord des données "*nécessaires pour établir les factures des abonnés et les paiements pour interconnexion*". Selon la directive, un tel traitement n'est autorisé "*que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement*". Par ailleurs, l'opérateur est également autorisé à traiter les données nécessaires pour "*commercialiser ses services de communications électroniques*" ou "*fournir des services à valeur ajoutée*". Mais il ne le peut que "*dans la mesure et pour la durée nécessaire à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement*". Il faut en outre considérer que l'article 4 de la directive qui confie aux opérateurs le soin d'assurer la sécurité du réseau l'autorise à conserver les données nécessaires à cet effet.
- Sa transposition (art. L. 34-1 et R. 10-14 CPCE)

Cette dérogation à l'interdiction de stockage rendue nécessaire par les besoins propres des opérateurs, trouve sa transposition, aujourd'hui comme hier, au paragraphe IV de l'article L. 34-1 CPCE. Les données pouvant être conservées à ce titre sont énumérées à l'article R.10-14, paragraphes I et II, du même code qui doit être pris, en l'espèce, dans sa rédaction issue du décret n° 2012-436 du 30 mars 2012[31]. Cet article réglementaire

[31] Décret n° 2012-436 du 30 mars 2012 portant transposition du nouveau cadre réglementaire européen des communications électroniques

désigne par ailleurs, en son paragraphe IV, les données devant être conservées par les opérateurs pour assurer la sécurité des réseaux. Un grand nombre de données d'identification, de trafic et de localisation peuvent ainsi faire l'objet d'un stockage[32]. Selon les dispositions combinées des articles L. 34-1, III, L. 34-2 et R.10-14, III, la conservation de données pour les besoins de la facturation et du paiement des prestations est autorisée pendant un an, durée de la prescription de l'action en paiement. Selon l'article L. 34-1, IV, celle des données relatives à la sécurité des réseaux peut l'être pour une durée n'excédant pas trois mois.

2.2.2.2.- Conservation des données pour un motif d'intérêt général

- Le droit de l'Union

En second lieu, en son paragraphe 1, l'article 15 de la directive autorise les Etats membres à adopter des mesures législatives visant à limiter la portée de l'obligation d'effacement ou d'anonymisation des données prévue aux articles 5 et 6 "*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'Etat - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales*". En pareil cas, "*les Etats membres peuvent, entre autres adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée*".

- Sa transposition pour les besoins de la lutte contre la criminalité (art. L. 34-1, R. 10-13 CPCE)

Transposant ces dispositions, l'article L 34-1 CPCE, dans sa rédaction applicable à la date des réquisitions litigieuses, énonce en son paragraphe III, déjà cité, que "*pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (...), il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques*". Bien que le texte exprime une simple faculté, c'est une obligation de conservation des données de connexion pour une durée d'un an, pour les besoins de la lutte contre la criminalité, qui est ainsi imposée aux opérateurs. Le fait, pour eux, de méconnaître cette obligation est sanctionnée pénalement par l'article L.39-3, 2° CPCE.

Les données devant être conservées au titre de la lutte contre la criminalité sont énumérées à l'article R. 10-13 CPCE, dans sa rédaction issue du décret précité du 30 mars 2012, alors applicable. Il s'agit des six catégories de données suivantes : informations permettant d'identifier l'utilisateur ; données relatives aux équipements terminaux de communication utilisés ; caractéristiques techniques, date, horaire et durée de chaque communication ; données relatives aux services complémentaires demandés ou utilisés et

[32]Pour les besoins de leurs opérations de facturation et de paiement les données suivantes : les données à caractère technique permettant d'identifier l'utilisateur ; données relatives aux équipements terminaux de communication utilisés ; caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs (I). En outre, pour les activités de téléphonie, les opérateurs peuvent conserver les données suivantes : celles à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et celles permettant d'établir la facturation (II).

Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver les éléments suivants : données permettant d'identifier l'origine de la communication ; caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; données à caractère technique permettant d'identifier le ou les destinataires de la communication ; données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs (IV).

leurs fournisseurs ; données permettant d'identifier le ou les destinataires de la communication et, enfin, pour les activités de téléphonie, données relatives au trafic ainsi que celles permettant d'identifier l'origine et la localisation de la communication.

2.3.- Appréciation de la conformité de la transposition au droit de l'Union

2.3.1.- Contrôle de proportionnalité assuré par la Cour de justice

Après avoir rappelé, dans les termes que nous avons cités (§ 1.2.1), que les données de connexion d'une personne permettent de tirer des conclusions très précises concernant sa vie privée, la Cour de justice a retenu que, par elle-même, indépendamment des modalités d'accès à ces données ménagées aux autorités publiques, leur conservation constituait une ingérence dans les droits fondamentaux de l'intéressé. Elle rejoint sur ce point la Cour européenne des droits de l'homme[33]. Considérant la gravité de cette ingérence et rappelant que la directive 2002/58 érige en principe l'interdiction du stockage des données de trafic et de localisation, la Cour de justice a jugé que les dispositions de l'article 15, paragraphe 1, de cette même directive, qui ouvre aux Etats membres la faculté de déroger à ce principe pour un motif d'intérêt public, devait s'interpréter strictement[34].

Ces prémisses étant posés, la Cour s'est attachée à déterminer les mesures de nature à assurer une conciliation équilibrée entre la préservation des droits fondamentaux proclamés aux articles 7, 8 et 11 de la Charte et les objectifs d'intérêt général pouvant justifier, aux termes de l'article 15, paragraphe 1, de la directive, qu'il leur soit porté atteinte. Autrement dit, elle s'est livrée au contrôle de proportionnalité imposé par l'article 52, paragraphe 1er, de la Charte des droits fondamentaux.

Pour déterminer cet équilibre, la Cour de justice a pris en compte à la fois la gravité de l'ingérence, appréciée à travers la nature de la donnée conservée, et la force de l'intérêt public de nature à justifier cette ingérence. Cette approche l'a conduite à concevoir un dispositif à plusieurs étages reposant sur une proposition simple : la possibilité de conservation doit être d'autant plus restreinte que la donnée protégée est sensible et l'objectif d'intérêt général de moindre importance[35]. Cette mise en balance l'a conduite à considérer que, contrairement à l'objectif de préservation de la sécurité nationale, celui de lutte contre la criminalité ne pouvait justifier une conservation généralisée et indifférenciée de l'ensemble des données de connexion.

2.3.2.- Interdiction d'une conservation généralisée et indifférenciée pour la lutte contre la criminalité

En tant qu'il prévoit une conservation des données de connexion pour les besoins de la lutte contre la criminalité, qualifiée par la Cour de justice de l'Union européenne de "*généralisée et indifférenciée*", le dispositif issu des articles L. 34-1 CPCE et R. 10-13

---

[33] CEDH, 16 févr. 2000, *Amam c/ Suisse*, n° 27798/95 § 69 ; CEDH, 4 mai 2000, *Rotaru c/Roumanie*, 28341/95, § 46 ; CEDH, 4 déc. 2008, *S. et Marper c/ Royaume-Uni*, n° 30566/04, § 67 ; CEDH, 18 avr. 2013, *M. K. c/ France*, n° 19522/09, § 29 ; CEDH, 22 juin 2017, *Aycaguer c/ France*, n° 8886/12, § 33

[34] not. CJUE, *Commissioner of An Garda Síochána,* point 40

[35] v. not. CJUE, 5 avr. 2022, *Commissioner of An Garda Síochána,* point 59

CPCE, dans leur rédaction applicable en l'espèce, n'apparaît pas conforme aux dispositions de l'article 15, paragraphe I, de la directive telles qu'interprétées par la Cour de justice, à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, dans ses arrêts déjà cités des 21 décembre 2016, *Tele 2 Sverige et Watson*, 6 octobre 2020, *La Quadrature du net* et 5 avril 2022*, Commissioner of An Garda Síochána*. Par conservation généralisée et indifférenciée il faut entendre une conservation mise en oeuvre sans aucune limitation quant aux personnes. On s'en tiendra à une présentation globale de ces arrêts qui adoptent la même solution de principe étant précisé toutefois que l'arrêt rendu dans l'affaire *La Quadrature du Net* revêt une importance particulière puisque, statuant sur renvoi préjudiciel du Conseil d'Etat, la Cour de justice y porte une appréciation sur le dispositif issu des articles précités du CPCE. Graduant, dans l'exercice de son contrôle de proportionnalité, la gravité des atteintes à la vie privée en fonction de la nature de la donnée conservée, la Cour de justice a retenu une solution distributive.

2.3.2.1.- Possibilité d'une conservation généralisée et indifférenciée de certaines données

- *Pour la lutte contre toute forme de criminalité : l'identité civile*

Pour la Cour, l'ingérence résultant de la conservation des données relatives à l'identité civile des utilisateurs ne peut être qualifiée de grave dans la mesure où l'information ne révèle rien des habitudes de vie de l'intéressé. Il s'ensuit que la conservation de ces données peut être prévue pour l'un quelconque des objectifs d'intérêt public énumérés à l'article 15, paragraphe I, de la directive, au nombre desquels la lutte contre la criminalité. Elle peut être en outre généralisée et indifférenciée - autrement dit, prévue pour tous les utilisateurs (not. CJUE, *La Quadrature du Net*, points 157 à 159).

- *Pour la lutte contre la criminalité grave : l'adresse IP attribuée à la source*

L'ingérence résultant de la conservation des adresses IP attribuées à la source d'une connexion - et non à ses destinataires - peut en revanche être qualifiée de grave. Certes, il s'agit d'une donnée de trafic moins sensible que d'autres en ce qu'elle ne révèle aucune information sur les relations entretenues par son titulaire. Mais elle peut être utilisée pour le traçage exhaustif du parcours de navigation d'un internaute. La Cour de justice en a déduit que, si elle peut également faire l'objet d'une conservation généralisée et indifférenciée, cette conservation n'est autorisée que pour la lutte contre la "criminalité grave" - et pour prévenir les menaces graves contre la sécurité publique (not. CJUE, *La Quadrature du Net*, points 152 à 156). Nous avons déjà exposé ce que pouvait recouvrir la notion de criminalité grave (§ 1.2.2).

2.3.2.2.- Conservation ciblée des autres données de trafic et des données de localisation

a) *Conception du dispositif de conservation ciblée*

Compte tenu des enseignements sur la vie privée des intéressés pouvant être tirés de l'exploitation des autres données de trafic et des données de localisation, la Cour de justice de l'Union européenne a jugé que, même aux fins de lutte contre la criminalité grave, la conservation généralisée et indifférenciée de ces données s'analysait en une atteinte disproportionnée au droit au respect à la vie privé. L'objectif de "*lutte contre la criminalité grave*" justifie certes une conservation des données de trafic et de localisation mais celle-ci doit être "*ciblée*" (CJUE, *6 oct. 2020, La Quadrature du Net*, points 140 à 151 ; CJUE, 5 avr. 2022, *Commissioner of An Garda Síochána,* points 76 à 84). Nous nous bornerons à rappeler les principaux éléments de cette solution tels qu'ils sont exposés par la Cour de Justice dans son arrêt *Commissioner of An Garda Síochána* du 5 avril 2022, lequel

correspond au dernier état de sa jurisprudence . Deux modes de ciblage sont envisagés par elle.

En premier lieu, la Cour admet la possibilité d'un ciblage en fonction d'un critère personnel qu'elle a quelque peu élargi au fil de ses arrêts. Peuvent être conservées les données afférentes aux communications de personnes dont certains éléments objectifs et non discriminatoires laissent supposer qu'elles sont susceptibles de se livrer à des actes de criminalité grave. A titre d'illustration, la Cour évoque les personnes faisant l'objet d'une enquête ou d'une mesure de surveillance actuelle ou encore celles dont le casier judiciaire porte mention d'une "*condamnation antérieure pour des actes de criminalité grave pouvant impliquer un risque élevé de récidive*" (*Commissioner of An Garda Síochána,* point 78). Telle qu'elle est conçue, la conservation fondée sur un critère personnel nous semble s'apparenter à une mesure de sûreté voire à une peine complémentaire.

En second lieu, pour la Cour, "*une mesure de conservation ciblée des données relatives au trafic et des données de localisation peut, selon le choix du législateur national et dans le respect strict du principe de proportionnalité, également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave*". Selon la Cour, "*ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou encore des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages*" (*ibid*. point 79) . S'agissant de la mise en oeuvre de ce critère géographique, la Cour indique que peut être pris en compte, notamment, le taux moyen de criminalité dans une zone géographique, estimant que cet élément d'appréciation ne présente aucun caractère discriminatoire (*ibid*. point 80). Bien entendu, la définition des zones géographiques pouvant justifier une conservation ciblée est susceptible d'évolution.

De manière générale, conformément à l'exigence de proportionnalité, la Cour pose en principe que "*la durée des mesures de conservation ciblée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation*" (*ibid* point 82).

Les critères personnel et géographique ainsi proposés par la Cour pour la mise en oeuvre d'une conservation ciblée ne sont pas conçus par elle comme limitatifs. C'est aux Etats membres qu'il incombe d'identifier, le cas échéant, d'autres critères permettant d'établir un lien, au moins indirect, entre les personnes dont les données sont conservées et les actes de criminalité grave. Il importe seulement que ces critères n'aboutissent pas à *"réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation*" (*ibid.* point 83).

b) *Interrogations suscitées par ce dispositif*

La conservation ciblée ainsi définie a suscité de nombreuses interrogations et préoccupations. Au-delà des difficultés d'ordre technique que sa mise en oeuvre est susceptible de poser aux opérateurs, il a été relevé qu'elle exposait à un risque constitutionnel en introduisant entre les personnes ou les parties du territoire national une disparité dans la protection des droits qui, pour reprendre la formule du Conseil

constitutionnel, pourrait *"ne pas apparaître en rapport direct avec l'objet de la norme qui l'établit*". Sur le plan opérationnel, la crainte a été exprimée que la conservation ciblée ne compromette gravement l'efficacité des investigations. Pour élucider une affaire, il est nécessaire de pouvoir exploiter les données de téléphonie antérieures, parfois de plusieurs mois, à la commission des faits ou à leur révélation. Or, dans un système de conservation ciblée, cette exploration du passé sera impossible pour peu que les investigations portent sur une zone non couverte par l'obligation de conservation ou sur une personne dont les données de connexion n'auront pas été conservées ou qui aura neutralisé cette conservation, par exemple en utilisant les moyens de communication d'un tiers ou en agissant sous une fausse identité. Il est toutefois inutile de s'appesantir sur ce point. Ces difficultés ou risques constitutionnels et opérationnels ont été exposés, notamment, par le Conseil d'Etat dans son arrêt du 21 avril 2021, *French Data Network* à la suite de son rapporteur public (n°53 et 54), par la Cour suprême d'Irlande dans la question préjudicielle dont elle a saisi la Cour de Justice dans l'affaire *Commissioner of An Garda Síochána* et par nombre d'Etats membres ainsi que la Commission elle-même. Vous les avez évoqués dans les arrêts du 1er avril 2020 par lesquels vous avez saisi la Cour de justice à titre préjudiciel de la question de l'utilisation des données de connexion pour la recherche des auteurs d'abus de marché (supra, 1.1.3).

C'est en prenant pour partie en compte les interrogations et appréhensions exprimées que, moyennant quelques assouplissements, la Cour de justice a réaffirmé en 2021 et 2022 dans ses arrêts *La Quadrature du Net* et *Commissioner of An Garda Síochána* une solution qu'elle avait adoptée dès 2016 dans son arrêt *Tele 2 Sverige*. Mais, en tout état de cause, pour la Cour, "*l'existence éventuelle de difficultés pour définir précisément les hypothèses et les conditions dans lesquelles une conservation ciblée peut être effectuée ne saurait justifier que des Etats membres, en faisant de l'exception une règle, prévoient une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation*" (CJUE, *Commissioner of An Garda Síochána*, point 84). Le débat nous paraît donc clos.

c) *Concordance de la position du Conseil constitutionnel*

A supposer même que les risques et difficultés que nous avons évoqués ne trouvent aucun remède, la question de savoir si elle méconnaîtrait des exigences d'ordre constitutionnel - notamment l'objectif de valeur constitutionnelle de lutte contre la délinquance - ne se pose pas, ou plus, dès lors que le Conseil constitutionnel a rejoint la position de la Cour de justice. Par sa décision déjà citée n° 2021-976/977 QPC du 22 février 2022 rendue sur la question prioritaire de constitutionnalité qui lui a été renvoyée dans la présente affaire, il a lui-même déclaré contraire à la Constitution comme portant une atteinte disproportionnée à la vie privée les dispositions des paragraphes II et III de l'article L. 34-1 CPCE dans leur rédaction issue de la loi du 18 décembre 2013[36]. Certes, le Conseil a jugé que la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions constituait un objectif de valeur constitutionnelle pouvant justifier l'atteinte à la vie privée que constitue, par elle-même, la conservation de données de connexion. Toutefois, suivant un raisonnement proche de celui de la Cour de justice, il a considéré que le dispositif législatif n'assurait pas une conciliation équilibrée entre la poursuite de cet objectif et la protection du droit à la vie privée dès lors que la conservation imposée aux opérateurs s'imposait sans distinguer selon les utilisateurs, la nature des données ou encore la nature et la gravité des infractions susceptibles d'être recherchées. Comme nous l'avons indiqué (supra, 2.1), il a différé l'entrée en vigueur de la déclaration d'inconstitutionnalité, sans quoi le débat sur la conformité des mêmes dispositions au droit de l'Union serait sans objet.

[36] Déc. n° 2021-976/977 QPC, 25 févr. 2022

2.3.2.3.- Nécessité d'écarter les dispositions de l'article L. 34-1 CPCE comme contraires au droit de l'Union

- Non conformité de l'article L. 34-1 CPCE

Il s'agit pour vous d'assurer la primauté du droit de l'Union et donc tirant les conséquences des arrêts de la Cour de justice, d'écarter comme contraires à ce droit les dispositions de l'article L. 34-1 CPCE dans leur rédaction issue de la loi du 18 décembre 2013 en tant qu'elles imposent aux opérateurs de téléphonie la conservation généralisée et indifférenciée des données de trafic et de localisation, - autres que celles mentionnées au 2.3.2.1 -, pendant une durée d'un an pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. La solution rejoint d'ailleurs celle retenue par le Conseil d'Etat dans l'affaire *La Quadrature du Net*. Après avoir constaté l'incompatibilité de l'article L. 34-1 CPCE avec le droit de l'Union, le Conseil d'Etat a annulé la décision du Premier ministre refusant d'abroger l'article R.10-13 CPCE en tant qu'il imposait une telle conservation[37]. Depuis lors, le législateur a tiré les conséquences de la jurisprudence de la Cour de justice en même temps que de la décision précitée du Conseil constitutionnel puisque, en refondant l'article L. 34-1 par la loi n° 2021-998 du 30 juillet 2021, il a supprimé l'obligation de conservation généralisée et indifférenciée en vue de la recherche des auteurs d'infractions.

- Perte de fondement à la conservation pour les besoins de la lutte contre la criminalité

En conséquence, il vous faudra constater qu'en l'absence de dispositions prévoyant par ailleurs une conservation ciblée telle qu'autorisée par la Cour de justice, notre droit ne comportait, à la date des réquisitions litigieuses, aucun dispositif permettant d'imposer aux opérateurs de conserver des données de connexion pour la lutte contre la criminalité, fût-elle grave. Précisons sur ce point qu'il ne nous paraît pas envisageable de tenter de justifier a posteriori la conservation des données de connexion se rapportant au demandeur en recherchant si, dans un dispositif prévoyant une conservation ciblée, les données afférentes à ses communications téléphoniques n'auraient pu être conservées soit en raison du taux de criminalité enregistré dans la zone de commission des faits soit en raison du passé judiciaire de l'intéressé. Il serait à la fois contestable et périlleux que vous définissiez en lieu et place du législateur les critères de nature à justifier une conservation ciblée sans compter qu'une telle solution introduirait une certaine imprévisibilité dans une matière intéressant la protection des droits fondamentaux.

Cela étant, si la non-conformité est certaine, sa portée doit être relativisée dès lors qu'il apparaît qu'à la date des réquisitions litigieuses, la conservation généralisée et indifférenciée des données de trafic et de localisation était justifiée au titre de la sauvegarde de la sécurité nationale.

2.3.3.- Possibilité d'une conservation généralisée et indifférenciée pour la sauvegarde la sécurité nationale

---

[37] Si une décision d'annulation par le juge administratif a effet *erga omnes* et s'impose au juge pénal (Crim. 12 mars 2003, n° 07-84.104, B. n° 63 ; Crim. 16 nov. 2010, n° 10-83.622 et 10-81.740, B. n° 182 et 183 ; Crim. 4 mars 2014, n° 13-82.078, B. n° 64 ; Crim. 12 déc. 2014, n° 12-82.919, B. n° 277), il nous semble que l'autorité de chose jugée attachée à une décision, qui, comme en l'espèce, n'annule pas des dispositions réglementaires mais seulement le refus de les abroger, ne fait pas obstacle à ce que vous appréciez la légalité de ces dispositions pour le passé (sur la différence de portée entre annulation de l'acte et annulation du refus de l'abroger, v. CE, 17 mars 2021, n° 440208)

2.3.3.1.- Une possibilité admise par la Cour de justice

Dans l'exercice de son contrôle de proportionnalité l'ayant conduite à hiérarchiser les objectifs d'intérêt public énumérés à l'article 15, paragraphe 1, de la directive 2002/58, la Cour de justice de l'Union européenne a placé au sommet l'objectif de *"sauvegarde de la sécurité nationale*", définie par elle comme "*la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays et, notamment, à menacer directement la société, la population ou l'Etat en tant que tel*"[38]. On retrouve dans cette formule des éléments de la définition du terrorisme figurant à l'article 3 de la directive 2017/541 du 15 mars 2017[39]. Sont ainsi désignés, pour l'essentiel, outre les actes de terrorisme, les atteintes aux intérêts fondamentaux de la nation. Pour la Cour, la gravité de tels agissements justifie que, pour les prévenir et les réprimer, une conservation généralisée et indifférenciée des données de connexion soit imposée aux opérateurs de téléphonie.

Cependant, une telle solution est subordonnée par elle à la réunion de plusieurs conditions. D'abord, elle suppose *"une menace grave pour la sécurité nationale, réelle et actuelle ou prévisible*". Ensuite, elle ne peut être mise en oeuvre que par une injonction adressée aux fournisseurs de services de communications électroniques pour une période limitée au strict nécessaire, une prolongation n'étant possible qu'en cas de persistance de la menace dûment constatée par une nouvelle injonction. Enfin, doit être ménagée la possibilité d'un contrôle effectif par une juridiction ou une entité administrative indépendante de manière que la réalité et l'actualité ou la prévisibilité de la menace puisse faire l'objet d'une vérification par un organe indépendant et impartial.

2.3.3.2.- Une possibilité mise en oeuvre dans les conditions encadrées par le Conseil d'Etat

Par son arrêt du 21 avril 2021 *French Data Network*, le Conseil d'Etat a constaté que cette possibilité de conservation avait été mise en oeuvre et en a défini le cadre en conformité avec les conditions posées par la Cour de justice[40]. Il était alors saisi de requêtes lui demandant d'annuler pour excès de pouvoir le refus implicite du Premier ministre d'abroger l'article R. 10-13 CPCE dans sa rédaction alors applicable. Il était soutenu par les requérants que les dispositions de cet article n'étaient pas conformes aux exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58/CE, tel qu'interprété dans la même affaire par la Cour de justice dans son arrêt du 6 octobre 2020, *La Quadrature du Net,* sur renvoi préjudiciel, en tant qu'elles énuméraient les données de connexion dont la conservation généralisée et indifférenciée était imposée à la fois pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales, en application de l'article L. 34-1, paragraphe III, CPCE, et pour ceux de la sauvegarde de la sécurité nationale, en application des dispositions combinées de cet article et de l'article L. 851-1 du code de la sécurité intérieure.

Le Conseil d'Etat s'est attaché à examiner si, à ce second titre, la conservation généralisée et indifférenciée était imposée dans des conditions conformes au droit de l'Union.

---

[38] CJUE, *La Quadrature du Net*, point 135 ; CJUE, *Commissioner of An Sochana*, point 61

[39] Directive (UE) 2017/541 du Parlement et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil

[40] CE 21 avr. 2021, *French Data Network*, points 19, 43 à 46

Il a tout d'abord relevé que cette conservation était justifiée dans son principe et mise en oeuvre par des dispositions à caractère réglementaire susceptibles de faire l'objet de recours devant le juge administratif de sorte que l'exigence d'un contrôle juridictionnel était satisfaite.
La principale question était de savoir si, concrètement, l'injonction de conservation résultant de ces dispositions était justifiée par l'existence d'une menace pour la sécurité nationale "*non seulement prévisible mais aussi actuelle*" et revêtant, par son intensité, "*un caractère grave et réel*". Eclairé par les mesures d'instruction auxquelles l'une de ses chambres avait procédé, le Conseil d'Etat a répondu par l'affirmative. Concrètement, il a constaté "*la persistance d'un risque terroriste élevé*" manifesté, notamment, par la commission de six attaques en 2020 ayant causé sept morts et onze blessés, par deux attentats déjoués dans les premiers mois de l'année 2021 ainsi que par l'activation du plan Vigipirate au niveau "*Urgence attentat*" entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau "*Sécurité renforcée - risque attentat*" depuis le 5 mars 2021. Compte tenu de cette menace, il a estimé que l'obligation faite aux opérateurs de conserver pendant un an les données de trafic et de localisation était nécessaire pour la sauvegarde de la sécurité nationale.

Le dispositif législatif et réglementaire était cependant lacunaire puisqu'il ne prévoyait pas le réexamen périodique - exigé par la Cour de justice - de l'existence d'une menace qualifiée dans les conditions indiquées. Dans cette mesure, le Conseil d'Etat l'a jugé contraire au droit de l'Union, précisant qu'un réexamen de l'état de la menace devrait être assuré dans un délai d'un an à compter de sa décision. Dans le même temps, relevant que, par celle-ci, il avait constaté la réalité, l'actualité et la gravité de la menace pesant sur la sécurité nationale de nature à justifier l'obligation de conservation généralisée et indifférenciée de l'ensemble des données de connexion aux fins d'assurer la sauvegarde de celle-ci, il a précisé que "*les opérateurs ne sauraient, avant l'expiration de ce délai, se soustraire à cette obligation* (...) *au motif que la durée de l'injonction qui leur est faite n'a pas été limitée dans le temps par le pouvoir réglementaire"* (point 46).

2.3.3.3.- Une solution suscitant l'adhésion

Nous adhérons sans réserve à cette solution. Certes, l'invocation de la sauvegarde de la sécurité nationale ne doit pas devenir une manière de contourner l'interdiction de principe d'une conservation généralisée et indifférenciée des données de trafic et de localisation. Pour reprendre la formule de la Cour de justice, une telle conservation "*ne saurait présenter un caractère systémique*"[41]. Pour autant, l'obligation de conservation généralisée et indifférenciée ne saurait davantage être épisodique ou, pour reprendre l'expression du rapporteur public du Conseil d'Etat, "stroboscopique". Elle perdrait tout son sens si, déterminée par la commission d'un attentat, elle devait impérativement être levée, en l'absence de répliques, quelques semaines ou quelques mois après. Un attentat terroriste est souvent le point d'émergence d'une menace qui lui est bien antérieure et perdure bien au-delà, ce que la Cour de justice intègre d'ailleurs en envisageant que la menace puisse n'être que "prévisible".

L'appréciation de la réalité et de l'intensité de la menace ne saurait être abandonnée aux juridictions du fond dès lors qu'elle ne détermine pas seulement l'application de la règle de droit dans un cas particulier mais le contenu même de cette règle. Vous pourrez, pour l'établir, vous reporter à l'analyse du Conseil d'Etat qui n'est pas contestée par le demandeur et nous paraît difficilement contestable : la répétition des attentats depuis la déflagration qu'ont constituée ceux de 2015, qui ont fait quelque 150 morts et des

[41] CJUE, *La Quadrature du Net*, points 135, 141, 142 ; CJUE, *Commissioner of An Garda Síochána*, point 65

centaines de blessés, révèle à elle seule la profondeur et la permanence d'un mal qu'on peut qualifier d'endémique. La liste des attentats établie par le procureur général près la cour d'appel de Paris le confirme. Il en résulte que, depuis 2015, le terrorisme d'origine djihadiste s'est manifesté chaque année par des attaques sanglantes[42]. Encore convient-il de souligner que n'apparaît pas dans cette liste l'action préventive des services de renseignement. Pour nous en tenir à l'année 2019, durant laquelle les réquisitions litigieuses ont été délivrées, deux surveillants pénitentiaires ont été blessés lors d'une attaque au couteau au centre pénitentiaire de [Localité 4] le 5 mars, quatorze personnes l'ont été à Lyon le 24 mai par l'explosion d'un colis piégé et, le 3 octobre, quatre personnes ont été tuées et une blessée lors d'une attaque au couteau à la préfecture de police de Paris. La gravité de ces actions ne se mesure pas seulement à leurs conséquences, par elles-mêmes dramatiques, sur la vie et l'intégrité physique des personnes. Le propre du terrorisme est de chercher à atteindre, au-delà des victimes immédiates, la société toute entière, à la déstabiliser en y répandant un sentiment d'insécurité et de peur. C'est le sens de la formule bien connue de Raymond Aron dans *Paix et guerre entre nations*[43] et c'est l'idée exprimée au point 16 du préambule de la directive 2012/29/UE du 25 octobre 2012, dite "victimes"[44], aux termes duquel "*les victimes du terrorisme ont subi des attaques dont le but est en définitive de porter atteinte à la société*". Nous sommes bien dans le champ de l'atteinte à la sécurité nationale telle qu'elle a été définie par la Cour de justice.

2.3.3.4.- Une possibilité désormais inscrite dans la loi

Le législateur a tiré les conséquences de l'arrêt du Conseil d'Etat du 21 avril 2021. Par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, il a modifié l'article L. 34-1 CPCE de manière à prévoir la possibilité, pour le Premier ministre, d'enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic et de localisation en cas de menace grave et actuelle contre la sécurité nationale. Le texte précise que l'injonction du Premier ministre, dont la durée d'application ne peut elle-même excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. En application de ces dispositions nouvelles, le Premier ministre a pris, le 20 octobre 2021, un décret portant injonction de conservation[45]. Bien entendu, cet ensemble de dispositions, postérieur à la date des réquisitions litigieuses, ne peut trouver application en l'espèce mais il faut avoir présent à l'esprit que l'appréciation que vous porterez sur la légalité, à la date de ces réquisitions, de la conservation généralisée et indifférenciée des données de trafic et de localisation au titre de la préservation de la sécurité nationale

---

[42] Selon la liste établie par le procureur général de Paris, ont été commis : en 2016, six attentats, dont celui de Nice, le 14 juillet, lors duquel 86 personnes ont été tuées et des centaines d'autres blessées ; en 2017, une dizaine dont l'un, à Paris le 20 avril, ayant provoqué la mort d'un policier et un autre, à Marseille, le 1er octobre, lors duquel deux jeunes femmes ont été assassinées ; en 2018, quatre attentats, dont celui, à Trèbes et Carcassone, du 23 mars, lors duquel quatre personnes ont été tuées dont un lieutenant-colonel de gendarmerie et celui du marché de Noël de Strasbourg, le 11 décembre, ayant provoqué la mort de cinq personnes.

[43] *"Une action violente est dénommée terroriste lorsque ses effets psychologiques sont hors de proportion avec ses résultats purement physiques*" (R. Aron, *Paix et guerre entre les nations* , Paris, Calmann-Lévy, 1962, p. 176)

[44] Directive 2012/29/UE " victimes " du Parlement et du Conseil du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil, complété par la directive 2017/541 du 15 mars 2017 relative à la lutte contre le terrorisme

[45] Décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion

induira celle que pourriez être appelés à porter sur la légalité de l'injonction prise en application de la loi nouvelle.

Si vous admettez que, pendant la période considérée, une conservation généralisée et indifférenciée des données de connexion énumérées à l'article R.10-13 CPCE était conforme au droit de l'Union en tant qu'elle était nécessaire pour la préservation de la sécurité nationale, se pose la question de savoir si les données conservées à ce titre n'étaient pas disponibles pour la lutte contre la criminalité grave alors même qu'elles n'auraient pu faire l'objet, à cette seule fin, d'une conservation généralisée et indifférenciée.

2.4.- Disponibilité pour la lutte contre la criminalité grave des données conservées pour la sauvegarde de la sécurité nationale

2.4.1.- Principe de spécialité des finalités d'intérêt public, obstacle à la disponibilité

En faveur de la possibilité d'accéder, pour la lutte contre la criminalité grave, aux données conservées au titre de la sauvegarde de la sécurité nationale, on peut mettre en avant qu'en règle générale, le titre en vertu duquel des informations sont conservées voire la régularité de leur conservation ne fait pas obstacle à ce que les magistrats et enquêteurs puissent y accéder pour les besoins de la manifestation de la vérité dans les procédures pénales. Il n'y a guère que le secret professionnel ou le secret de la défense nationale qui soit susceptible d'empêcher un tel accès. En outre, ouvrir la possibilité d'accéder, pour la lutte contre la criminalité grave, à des données faisant l'objet d'une conservation généralisée et indifférenciée au titre de la sauvegarde de la sécurité nationale n'aggrave en rien l'atteinte à la vie privée résultant d'une telle conservation, considérée par elle-même.

Il faut cependant intégrer dans l'analyse le principe qu'on pourrait dire de spécialité qui imprègne l'ensemble du droit de la protection des données et qui est d'ailleurs inscrit à l'article L. 34-1 CPCE[46]. On en trouve l'expression à l'article 8, paragraphe 2, de la Charte des droits fondamentaux, aux termes duquel les données "*doivent être traitées loyalement, à des fins déterminées*" ou encore à l'article 5 du règlement général sur la protection des données (RGPD) du 27 avril 2016[47] qui dispose 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*". Il est vrai que la règle ainsi énoncée s'applique, selon l'article 23 du RGPD, sous réserve, précisément, des limitations tenant à la nécessité de garantir, dans le respect du principe de proportionnalité, un certain nombre d'objectifs d'intérêt général au nombre desquels *"la prévention et la détection d'infractions pénales ainsi que les enquêtes et les poursuites en la matière ou l'exécution des sanctions pénales* (...)". Autrement dit, certaines finalités d'intérêt public, comme celle de lutte contre la criminalité, se présentent comme des dérogations générales à l'exigence de spécialité. Elles justifient un usage des données pour des objectifs différents de ceux ayant déterminé leur conservation.

---

[46] L. 34-1, VI, al. 5 : *Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article.*

[47] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Toutefois, cette dérogation connaît un tempérament important tenant à la hiérarchisation des finalités d'intérêt public. Dans ses arrêts relatifs à la conservation et au traitement des données de connexion, la Cour de justice de l'Union européenne a posé, pour reprendre l'expression d'Alexandre Lallet, une règle de "*concordance des finalités*" selon laquelle lorsqu'une conservation des données, plus large que celle prévue pour les besoins des opérateurs, a été imposée en application de l'article 15, paragraphe 1, de la directive 2002/58 pour une finalité d'intérêt public déterminée, l'accès aux données conservées à ce titre n'est possible que pour la même finalité d'intérêt public ou une finalité d'intérêt public plus élevée. On trouve une expression de cette conception dans l'arrêt *La Quadrature du Net* du 6 octobre 2020. La Cour y énonce qu'un accès à des données de trafic et de localisation "*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*" (point 66). La Cour a été plus explicite encore dans son arrêt *Commissioner of An Garda Síochána* du 5 avril 2022, en réponse à des observations du gouvernement danois qui faisait valoir qu'il devrait être possible d'accéder, pour les besoins de la lutte contre la criminalité grave, aux données conservées de manière généralisée et indifférenciée au titre de la sauvegarde de la sécurité nationale (points 97 à 100). La solution est logique. En retenant un motif de dérogation, le législateur fixe le périmètre de celle-ci. Un bref rappel des motifs de l'arrêt *Commissioner of An Garda Síochána* permet de mesurer l'exacte portée de la réponse.

La Cour y relève "*que le fait d'autoriser l'accès, aux fins de la lutte contre la criminalité grave, à des données relatives au trafic et à des données de localisation qui ont été conservées de manière généralisée et indifférenciée ferait dépendre cet accès de circonstances étrangères à cet objectif, en fonction de l'existence ou non, dans l'État membre concerné, d'une menace grave pour la sécurité nationale* (...)*, alors que, au regard du seul objectif de lutte contre la criminalité grave devant justifier la conservation de ces données et l'accès à celles-ci, rien ne justifierait une différence de traitement, en particulier entre les États membres"* (point 97). La Cour en a déduit que "*l'accès à des données relatives au 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*". Selon la Cour, "*il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation*" (point 98). Dès lors que l'objectif de lutte contre la criminalité grave "*est d'une importance moindre, dans la hiérarchie des objectifs d'intérêt général, que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale*", il n'est pas possible d'autoriser, dans une telle situation, un accès aux données conservées sans aller "*à l'encontre de cette hiérarchie des objectifs d'intérêt général*" (point 99). La Cour conclut ainsi que, lorsque des 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* (...), *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*" (point 100).

Il est difficile d'être plus clair. De ces motifs, il pourrait être déduit qu'il est radicalement exclu d'utiliser, pour la lutte contre la criminalité grave, des données conservées de manière généralisée et indifférenciée au titre de la sauvegarde de la sécurité nationale dans le cas où ces données n'auraient pas été par ailleurs conservées, en vertu d'un dispositif de conservation ciblé tel que nous l'avons évoqué, au titre de la lutte contre la criminalité grave.

2.4.2.- Tempérament par la mise en oeuvre de la conservation rapide

2.4.2.1.- La conservation rapide, mode d'accès à l'ensemble des données conservées

Si cette solution de principe est certaine, il nous semble que la Cour de justice lui apporte un important aménagement en ouvrant, par le mécanisme de "la conservation rapide" dite encore *quick freeze*, la possibilité de puiser, pour la lutte contre la criminalité grave, dans le gisement des données conservées, notamment, au titre de la sauvegarde de la sécurité nationale. Cette voie d'accès, ouverte par la Cour dans son arrêt *La Quadrature du Net* (points 160 à 167) a été, sinon élargie, du moins éclaircie par elle dans son arrêt *Commissioner of An Garda Síochána* (points 85 à 91).

Il résulte des termes mêmes de ces décisions que le procédé dit de conservation rapide s'applique, pour les besoins de la lutte contre la criminalité grave, "*aux données relatives au trafic et aux données de localisation traitées et stockées par les fournisseurs de services de communications électroniques",* non seulement *"sur la base des articles 5, 6 et 9 de la directive 2002/58",* qui, rappelons-le, recouvrent les données conservées, par les opérateurs, pour les besoins de l'acheminement de la communication ainsi que pour leurs besoins commerciaux - mais également *"sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de cette directive"* - et donc, notamment, au titre de la sauvegarde de la sécurité nationale.

La raison d'être et les modalités de la conservation rapide sont exposées par la Cour. Celle-ci part du constat que "*les 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* [la] *directive, leur traitement et leur stockage".* Or, relève-t-elle, il se peut qu*'"aux fins de l'élucidation d'infractions pénales graves",* apparaisse *"la nécessité de conserver"* les données considérées *"au-delà de ces délais",* sans qu'il y ait à distinguer selon que ces infractions *"ont déjà pu être constatées"* ou que leur existence *"peut être raisonnablement soupçonnée"* (*La Quadrature du Net,* points 160 et 161 ; *Commissioner of An Garda Síochána,* point 85).

La conservation rapide doit donc être justifiée par l'utilité qu'elle présente pour l'élucidation d'une infraction déterminée. Cette précision est essentielle. Si notre droit distingue très nettement prévention et répression des infractions, la première relevant de la police administrative tandis que la seconde relève de la police judiciaire, cette distinction n'a rien d'universelle. L'objectif de "*lutte contre la criminalité*" qui peut justifier une conservation ciblée des données de connexion recouvre, selon la formule de l'article 15, paragraphe 1, de la directive 2002/56 "*la prévention, la recherche, la détection et la poursuite d'infractions pénales".* Le champ de la conservation rapide ne coïncide pas avec celui d'un tel objectif. Il est plus restreint dans la mesure où il n'est possible que pour élucider une affaire déterminée. Pour filer la métaphore du rapporteur public du Conseil d'Etat, dans le lac que forment les données conservées pour une autre fin que la lutte contre la criminalité, la pêche au chalut est interdite.

La Cour énonce de la manière la plus claire que *"dans une telle situation, il est loisible aux États membres* (...) *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* (*La Quadrature du Net,* point 163 *; Commissioner of An Garda Síochána,* point

86). L'injonction de conservation rapide pour l'élucidation d'une infraction peut donc porter sans aucun doute sur *toutes* les données stockées par l'opérateur, y compris, le cas échéant, au titre de la sauvegarde de la sécurité nationale.

Certes, comme le constate la Cour, *"la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement".* Mais, pour la Cour cette discordance impose seulement *"que les États membres précisent, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu".* Il s'agit *de r*especter l'article 8, paragraphe 2, de la Charte selon lequel tout traitement de données doit répondre à des fins déterminées. On le voit, si le défaut de concordance des finalités, explicitement relevé, appelle un encadrement, il n'est pas un obstacle à la conservation rapide. Bien entendu, conformément à la règle générale, eu égard au caractère grave de l'ingérence dans les droits fondamentaux qu'ils emportent, la conservation rapide et l'accès aux données qui en sont l'objet doivent *"respecter les limites du strict nécessaire"* (*Commissioner of An Garda Síochána,* point 87).

La conservation rapide ainsi admise se distingue très nettement de celle, ciblée en fonction de critère personnel ou géographique, dont on a vu qu'elle pouvait par ailleurs être prévue pour les besoins de la lutte contre la criminalité grave. Son champ est beaucoup plus large. La Cour précise que la conservation rapide *"ne doit pas être limitée aux données* (...) *des personnes concrètement soupçonnées d'avoir commis un acte de criminalité grave".* Pour la Cour, une telle mesure *"peut, selon le choix du législateur national 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* (...)*, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction* (...)*, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel"* (*La Quadrature du Net,* point 165 ;*Commissioner of An Garda Síochána,* point 88*).* Ainsi, levant toute ambiguïté, la Cour permet explicitement au législateur national de prévoir la possibilité d'enjoindre aux opérateurs de procéder à la conservation rapide des données relatives au trafic et des données de localisation des personnes avec lesquelles, *"antérieurement à la commission d'un acte de criminalité grave"*, une victime a été en contact en utilisant ses moyens de communications électroniques (point 89). Elle permet en outre que la conservation rapide soit *"étendue à des zones géographiques"* distinctes de celles couvertes par une éventuelle conservation ciblée. Il peut s'agir des *"lieux de la commission et de la préparation de l'infraction"* ou encore du *"lieu où une personne, potentiellement victime d'un acte de criminalité grave, a disparu"* (*Commissioner of An Garda Síochána,* point 90).

Quant au stade de la procédure auquel peut intervenir cette injonction de conservation rapide, la Cour précise "*que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à ce que les autorités nationales compétentes ordonnent une mesure de conservation rapide dès le premier stade de l'enquête portant* (...) *sur un éventuel acte de criminalité grave, à savoir à partir du moment auquel ces autorités peuvent, selon les dispositions pertinentes du droit national, ouvrir une telle enquête".* Autrement dit, la conservation rapide peut intervenir à un stade quelconque des investigations, y compris à leur tout début. La rapidité de la conservation ne tient pas à sa précocité.

2.4.2.2.- Notion de conservation rapide

Comme l'a relevé le rapporteur public dans ses conclusions sur l'affaire *La Quadrature du Net*, la Cour de justice "a puisé" la notion de conservation rapide dans la Convention de

Budapest sur la cybercriminalité du 23 novembre 2001. Il résulte des articles 16 et 17 de la Convention et de son rapport explicatif que cette forme de conservation s'analyse en réalité en un maintien de la disponibilité de données stockées en vue de leur éventuelle "divulgation"[48].

De la lecture de cette convention et de son rapport explicatif, il ressort que la conservation rapide présente trois caractéristiques.

La première est d'être une conservation secondaire puisqu'elle tend à la conservation de donnée déjà stockées ou en cours de stockage. Si elle présente une utilité particulière en cas de risque d'effacement imminent de celles-ci, elle peut être mise en oeuvre bien au-delà de ce cas de figure. Le rapport explicatif de la Convention ne laisse planer aucun doute sur ce point. Il y est indiqué que la mesure s'applique "*aux données stockées qui ont déjà été collectées et archivées par les détenteurs de données*" ou encore aux données *"en cours de stockage*" (point 149 - v. aussi point 152). C'est bien également, on l'a vu, l'objet donné à la mesure par la Cour de justice. Ainsi définie, la conservation rapide s'oppose à la collecte de données en temps réel - et donc au fur et à mesure de leur émission - mise en oeuvre pour la géolocalisation prévue aux articles 230-32 et suivants du code de procédure pénale.

La deuxième caractéristique de la conservation rapide est d'être ciblée. Là encore, comme le précise le rapport explicatif, elle ne peut être mise en oeuvre qu'*"aux fins d'enquêtes ou de procédures pénales spécifiques*", ce qui en restreint l'application à *"une enquête concernant une affaire donnée*". Cette restriction correspond au champ que la Cour de justice a entendu donner à cette mesure qui, rappelons-le, ne doit permettre que d'accéder aux données nécessaires à l'élucidation d'une affaire particulière. En revanche selon la Convention comme selon la jurisprudence de la Cour, elle peut intervenir à tous les stades de "l'enquête".

La troisième caractéristique de la conservation rapide est d'être l'antichambre de la "divulgation". La mesure n'est pas une fin en soi. Sa raison d'être est de permettre une éventuelle communication - "divulgation" selon la Convention - aux magistrats ou aux enquêteurs de tout ou partie des données qui en sont l'objet. Elle est donc le premier temps du processus d'accès aux données. Là encore, le rapport explicatif est clair. On peut y lire que la conservation rapide est "*le pouvoir de requérir la conservation de données stockées existantes, en attendant la divulgation des données en application d'autres pouvoirs juridiques, à l'occasion d'enquêtes ou de procédures spécifiques*" (point 152). Dès lors, que la conservation rapide s'entend du maintien de la disponibilité des données en vue d'une éventuelle mise à disposition effective, la permettre c'est potentiellement permettre cette mise à disposition.

2.4.2.3.- Conservation rapide et réquisitions prévues par le code de procédure pénale

Dans notre système procédural, la première étape du processus de mise à disposition n'est pas individualisée. Les article 60-1, 77-1-1 et 99-3 du code de procédure pénale confèrent le pouvoir de requérir "*la remise*" d'informations nécessaires à la manifestation de la vérité.

[48]L'article 16 prévoit l'adoption par chaque partie d'une législation permettant d'imposer par voie d'injonction la conservation rapide de données informatiques stockées, y compris des données relatives au trafic, afin de permettre aux autorités compétentes d'obtenir leur divulgation. L'article 17 instaure des obligations spécifiques concernant la conservation des données relatives au trafic qui peuvent faire l'objet d'une divulgation rapide aux fins d'identification des autres fournisseurs de services ayant participé à la transmission de communications spécifiées.

Cette remise correspond ainsi à la divulgation de l'information sans temps de conservation rapide préalable. De fait la conservation rapide ne présente d'utilité que dans le cas où, à titre conservatoire, les enquêteurs souhaitent maintenir la disponibilité de données susceptibles d'intéresser l'enquête sans être sûrs cependant qu'ils en auront l'usage. Contrairement à ce que l'on pourrait supposer, les bornages téléphoniques, sollicités en l'espèce dès le début de l'enquête ne correspondent pas à une telle nécessité. Les données ainsi recueillies n'ont pas été simplement "gelées". Elles ont été aussitôt communiquées aux enquêteurs pour exploitation.

Il n'y a guère que les dispositions du deuxième alinéa de l'article 60-2 du code de procédure pénale, auxquelles se réfèrent les articles 77-1-2 et 99-4 qui peuvent évoquer la notion de conservation rapide. Mais, par son objet et sa durée, la mesure qu'elles prévoient va bien au-delà de celle définie par la Convention de Budapest. Elle tend "*à assurer la préservation (...) du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs*" et non pas simplement celle des données de connexion des utilisateurs. En outre cette préservation peut être imposée "*pour une durée ne pouvant excéder un an"* - bien supérieure à celle de quatre-vingt dix jours envisagée par la Convention en cas de conservation rapide.

Il faut donc considérer qu'aucune disposition de procédure pénale n'organise spécifiquement la possibilité pour les enquêteurs de prescrire une conservation rapide des données de connexion même si, à notre sens, rien ne s'oppose à ce qu'une telle conservation soit prescrite sur le fondement des dispositions des articles 60-1, 77-1-1 et 99-3 dont les termes sont suffisamment compréhensifs. Pour autant, il serait paradoxal de refuser aux magistrats et aux enquêteurs la possibilité de demander la remise ou la mise à disposition, pour les besoins de l'élucidation d'une affaire grave, de données conservées au titre de la préservation de la sécurité nationale au motif que cette demande n'aurait pas été précédée d'une demande aux fins de conservation rapide. Au regard du droit à la protection de la vie privée et du droit à la protection des données personnelles, on ne voit pas en quoi cette décomposition du processus de remise pourrait constituer une garantie particulière. Nous aurions même tendance à penser que la conservation rapide, qui permet de préserver la disponibilité de données dont l'utilité pour l'enquête est incertaine, est une atteinte plus grave à la vie privée que l'obtention directe des données utiles à celle-ci. Par ailleurs, comme nous l'avons vu, la conservation rapide est possible, selon la Cour de justice, quel que soit le motif pour lequel sont stockées les données auxquelles s'applique la mesure. Dès lors, si vous jugez qu'elle doit nécessairement précéder la communication de données conservées au titre de la sauvegarde de la sécurité nationale, vous devrez appliquer la même solution pour l'accès aux données conservées par les opérateurs pour leurs besoins propres. On ne voit pas les raisons d'une telle complication.

Il nous semble ainsi que les arrêts de la Cour de justice que nous avons cités, autorisant la conservation rapide, pour l'élucidation d'une infraction grave, des données de trafic et de localisation conservées par les opérateurs à quelque titre que ce soit, autorisent nécessairement les magistrats et enquêteurs, sur le fondement des articles 60-1, 77-1-1 et 99-3 du code de procédure pénale à solliciter directement la communication de ces données. Autrement dit, la Cour de justice leur permet de faire précéder leur demande de communication d'une demande de conservation rapide, qui a l'avantage de maintenir la disponibilité de données dont l'utilité pour l'enquête est incertaine, mais elle ne les y contraint pas. Elle lève ainsi l'incertitude que pouvait faire peser sur la possibilité d'une conservation rapide l'interdiction d'une conservation généralité et indifférenciée. Elle précise dans le même temps que la communication des données qui n'ont pas été spécialement conservées pour la lutte contre la criminalité grave ne peut être obtenue dans le cadre de cette lutte que si elles sont de celles qui pourraient faire l'objet d'une

conservation rapide, ce qui implique qu'elles soient nécessaires à l'élucidation d'une affaire déterminée.

La solution est parfaitement conforme aux termes de la Convention de Budapest. Il résulte en effet des développements de son rapport explicatif consacrés à son article16 que, dans les Etats qui n'ont pas prévu de procédure d'injonction rapide, les données ne peuvent être "*conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire*". Ces procédés ne sont pas tenus pour contraires à la Convention. Il est seulement "*recommandé*" aux Etats concernés "*d'envisager d'instaurer des pouvoirs et procédures permettant d'ordonner effectivement au destinataire d'une injonction de conserver les données, car la rapidité de l'intervention de cette personne peut, dans certains cas, permettre d'appliquer plus rapidement les mesures de conservation*". Souplesse et pragmatisme dominent donc la Convention, dont les auteurs ont été guidés par un souci d'efficacité. Satisfait à ses finalités une injonction, telle que celle prévue aux articles précités du code de procédure pénale, qui impose une remise rapide.

Ainsi, à l'instar du Conseil d'Etat[49], nous vous proposons de juger que, pour l'élucidation d'une affaire particulière, les juridictions pénales peuvent, sans méconnaître le droit de l'Union européenne, accéder aux données de connexion conservées au titre de la sauvegarde de la sécurité nationale. Depuis lors, par la loi déjà citée du 30 juillet 2021, le législateur s'est attaché à consacrer cette solution par des dispositions, introduites au paragraphe IIIbis de l'article L. 34-1 CPCE, dont vous aurez peut-être un jour à apprécier la conformité[50].

2.5.- Accès aux données conservées pour les besoins propres des opérateurs

2.5.1.- Coïncidence avec les données conservées pour la sauvegarde de la sécurité nationale

Si toutefois vous jugiez que le principe de spécialité tel qu'énoncé par la Cour de justice dans ses arrêts *La Quadrature du Net* et, plus nettement encore, *Commissioner of An Garda Síochána* fait obstacle, pour les besoins de la résolution des affaires pénales graves, à l'accès aux données conservées au titre de la préservation de la sécurité nationale, demeurerait la possibilité d'accéder aux données conservées par les opérateurs pour les besoins de la sécurité des réseaux et des installations et pour leurs besoins propres, lesquels recouvrent l'acheminement des communications, les opérations de facturation et de paiement et, plus largement, avec le consentement des intéressés, la mise en oeuvre d'opérations commerciales.

Comme nous l'avons indiqué, les données susceptibles d'être conservées par les opérateurs à ces titres sont énumérées à l'article R 10-14 CPCE. Il suffit de comparer cet article avec l'article R 10-13 énumérant les données pouvant être conservées au titre,

---

[49] CE 21 avr. 2021, *French Data Network et a*., n° 55 à 57

[50] Aux termes de l'article III bis de l'article L. 34-1 CPCE issu de la loi du 30 juillet 2021 : "*Les données conservées par les opérateurs en application du présent article* [et donc, y compris celles pouvant être conservées au titre de la préservation de la sécurité nationale] *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*".

notamment, de la préservation de la sécurité nationale, pour constater que leurs champs coïncident largement. Toutefois, si, pour les besoins de la sauvegarde de la sécurité nationale, un délai de conservation d'un an est imposé, les données conservées par les opérateurs pour leurs besoins propres et ceux de la sécurité des réseaux et installations sont plus volatiles. La loi fixe des durées maximales de conservation - un an pour les données nécessaires à la facturation, trois mois pour celles nécessaires à la sécurité des réseaux - mais n'interdit pas aux opérateurs un effacement anticipé. Or, en pratique, ainsi que l'a relevé le Conseil d'Etat dans son arrêt du 21 avril 2021 : "*seule une partie des données couvertes par l'article R. 10-13 est volontairement conservée par les opérateurs* (...) *au titre du seul article R. 10-14. En particulier, les données de connexion relatives aux appels entrants et celles relatives à la géolocalisation, ne font que très rarement l'objet d'une conservation à ce titre de la part des opérateurs*. *De même, les données relatives aux appels sortants dans le cadre de forfaits illimités ne sont pas conservées dès lors qu'elles ne sont pas utiles à la facturation*" (n° 51).

2.5.2.- Interrogations soulevées par la superposition des causes de conservation

Cela étant, la détermination des données conservées pour les besoins propres des opérateurs soulève une difficulté lorsque les mêmes données doivent en tout état de cause être conservées pour les besoins de la sauvegarde de la sécurité nationale. En ce cas, la superposition des causes de conservation rend impossible de déterminer avec certitude les données qui seraient conservées à l'un ou l'autre titre. En réalité, la première cause de conservation se trouve alors comme absorbée par la première et perd donc son autonomie.

Pour autant, il serait incohérent de considérer qu'en raison de cette absorption, les magistrats ou les services d'enquête n'auraient plus la possibilité de demander, pour l'élucidation d'affaires pénales graves, la communication des données conservées par les opérateurs pour leurs besoins propres et ceux de la sécurité des réseaux. Une telle solution reposerait sur le constat que, d'une part, ces données se trouveraient en quelque sorte fondues dans la masse de celles conservées au titre de la sauvegarde de la sécurité nationale et que, d'autre part, en vertu de la règle de la spécialité - dont on postule ici l'application - les données conservées à ce titre ne pourraient être utilisées pour la résolution d'affaires pénales. Mais on voit l'incohérence à laquelle aboutit un tel raisonnement. Il en découlerait en effet que les magistrats et enquêteurs disposeraient de moins de prérogatives dans le cas où, en raison de l'existence d'une menace grave pour la sécurité nationale, serait prévue, à ce titre, une conservation généralisée et indifférenciée des données. Loin de produire un effet d'aubaine, cette conservation deviendrait calamiteuse pour l'efficacité de la lutte contre la délinquance grave.

2.5.3.- Solutions envisageables

Il faut donc admettre qu'en tout état de cause, une conservation généralisée et indifférenciée des données pour la sauvegarde de la sécurité nationale ne saurait priver les magistrats et enquêteurs de demander aux opérateurs, pour les besoins de l'élucidation d'une affaire pénale grave, la communication des données conservées au titre de leurs besoins propres ou de la sécurité des réseaux. Toute la question est de savoir comment identifier alors ces données. Il paraît difficile de supputer les initiatives qui auraient été prises par les opérateurs quant au sort des données considérées s'ils n'avaient pas été tenus de les conserver pour la préservation de la sécurité nationale. Cette manière de raisonner supposerait de procéder au cas par cas à une sorte de reconstitution hypothétique qui nous paraît lourde et pleine d'aléas. Une solution simple mais également discutable serait de raisonner par présomption. Dès lors que la loi fixe un délai maximal de

conservation, d'un an ou de trois mois des données entrant dans les prévisions de l'article R. 10-14 CPCE, celles-ci pourraient être réputées disponibles pendant toute la durée de ce délai. A tout le moins, il conviendrait à notre sens de présumer que les données en cours de stockage ou stockées depuis peu sont de celles que les opérateurs sont réputés avoir conservées pour leurs besoins propres et sont donc disponibles pour les besoins de la résolution des affaires pénales.
Mais nous n'envisageons cette solution qu'à titre subsidiaire, dans le cas où vous n'admettriez pas la possibilité d'accéder, pour les besoins de la résolution des affaires pénales graves, aux données de trafic et de localisation conservées au titre de la sécurité nationale.

2.6.- Appréciation du moyen

2.6.1.- Motifs de l'arrêt attaqué

En l'espèce, pour écarter l'argumentation de M.[L][E] tirée de ce que les données de trafic et de localisation afférentes à ses communications téléphoniques, obtenues et exploitées par les enquêteurs, avaient été conservées de manière généralisée et indifférenciée en violation du droit de l'Union, la chambre de l'instruction après avoir rappelé succinctement les motifs de l'arrêt de la Cour de justice du 6 octobre 2020, *La Quadrature du Net*, a retenu en substance, que, mis en examen le 26 juin 2020, l'intéressé avait eu accès à la procédure et qu'il avait donc été "*mis en mesure de commenter efficacement l'ensemble des éléments de la procédure apparaissant comme constituant des indices graves ou concordants rendant vraisemblable son implication comme auteur ou complice des faits pour lesquels il est mis en examen*".

Il semble qu'elle ait entendu ainsi se conformer aux motifs, qu'elle cite, de l'arrêt de la Cour de justice *La Quadrature du Net* dont il résulte que le juge pénal national n'est pas tenu 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 si les personnes soupçonnées d'actes de criminalité *"sont 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 Quadrature du Net*, point 227).

2.6.2.- Proposition de rejet par substitution de motifs

Ces motifs ne sont pas critiqués par le demandeur qui se borne à reprocher à la chambre de l'instruction d'avoir affirmé par ailleurs que l'ingérence dans sa vie privée résultant des réquisitions litigieuses était proportionnée à l'objectif de répression d'infractions graves.

Il nous semble cependant que vous pourrez tenir les motifs de l'arrêt attaqué pour surabondants et le moyen qui les critique pour inopérant si, comme nous vous le proposons, vous retenez à la suite du Conseil d'Etat :
- en premier lieu, que la conservation généralisée et indifférenciée des données de trafic et de localisation était justifiée, au regard des dispositions de l'article L. 34-1 CPCE, par la nécessité d'assurer la sauvegarde de la sécurité nationale en raison de l'existence d'une menace terroriste réelle et actuelle ;
- en deuxième lieu, que les juridictions pénales disposaient, pour l'élucidation d'une affaire particulière, du pouvoir d'accéder à ces données par le biais de la conservation rapide conformément à la jurisprudence de la Cour de justice ;

- enfin, que les réquisitions mis en oeuvre en l'espèce en application des articles 60-1 et 99-3 du code de procédure pénale, répondent à l'objectif poursuivi par la mesure de conservation rapide.

Si vous ne reteniez pas cette solution, vous pourriez retenir que les données exploitées en l'espèce doivent être réputées comme étant de celles qui eussent été conservées par les opérateurs pour leurs besoins propres, indépendamment de toute obligation de conservation généralisée et indifférenciée.

2.6.3.- Proposition subsidiaire de question préjudicielle

Si l'interprétation du droit de l'Union sous-tendant ces solutions ne vous parait pas s'imposer avec une telle évidence qu'elle ne "laisse place à aucun doute raisonnable"[51], la même appréciation devrait être portée sur la solution inverse excluant toute possibilité d'accès, pour l'élucidation d'une affaire particulière, aux données conservées au titre de la sauvegarde de la sécurité nationale. En ce cas, il y aurait lieu de saisir la Cour de justice à titre préjudiciel afin que soient précisées :

- d'une part, l'articulation entre les motifs de l'arrêt *Commissioner of An Garda Síochána* énonçant le principe qu'on pourrait dire de spécialité des finalités d'intérêt public (points 97 à 100) et ceux de ce même arrêt (points 85 à 91), repris de l'arrêt *La Quadrature du Net* (points 160 à 167), ménageant la possibilité d'accéder, par le biais de la conservation rapide, aux fins d'élucidation d'une affaire pénale, à l'ensemble des données conservées par les opérateurs à quelque titre que ce soit ;

- d'autre part, la notion même de conservation rapide de manière à déterminer si elle peut inclure un mode d'accès sans phase de conservation préalable.

3. MOYEN TIRE DE L'ABSENCE D'AUTORISATION PREALABLE PAR UNE AUTORITE INDEPENDANTE

Il reste à examiner, avec le troisième moyen, la conformité au droit de l'Union des textes qui, à la date des réquisitions litigieuses, permettaient cet accès - soit, pendant l'enquête, les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale. Dans ce moyen de cassation, le demandeur critique les motifs par lesquels la chambre de l'instruction a rejeté son moyen de nullité tiré de ce qu'en violation, selon lui, de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, l'accès à ses données de connexion n'avait pas été précédé d'un contrôle effectif de l'autorité judiciaire ou, plus exactement, selon la formulation du moyen, "*d'une autorisation en amont* [et] *d'un contrôle en aval par une autorité indépendante*".

3.1.- Observations liminaires

3.1.1.- Irrecevabilité partielle du moyen

[51] CJCE, 6 oct. 1982, *Cilfit,* 283/81, point 11

Il résulte des termes de la requête en nullité présentée devant la chambre de l'instruction ainsi que du mémoire qui la complète que la contestation tirée de l'absence d'autorisation judiciaire préalable était dirigée exclusivement contre les réquisitions délivrées au cours de l'enquête de flagrance, qu'elles aient été exploitées au cours de cette enquête ou ultérieurement. En effet, après avoir rappelé, dans sa requête, les termes de l'article 60-1 du code de procédure pénale régissant la délivrance, au cours de l'enquête de flagrance, des réquisitions aux fins de communication des données de connexion, l'intéressé relève que "*les enquêteurs agissant sous le régime des articles 56* [en réalité 53] *et suivants du code de procédure pénale ont la possibilité d'obtenir les données de trafic et de localisation de n'importe quel utilisateur d'une ligne téléphonique, d'office, sans y avoir été habilité par l'autorité judiciaire, et sans décision écrite et motivée d'un membre de celle-ci*". Il constate que, dans la présente procédure, faisant application des dispositions de l'article 60-1, "*les enquêteurs se* [sont vu] *communiquer par les opérateurs téléphoniques, dans le cadre de l'enquête de flagrance, l'intégralité des données de trafic et de localisation de lignes téléphoniques*" qui lui étaient "*attribuées*". Il demande en conséquence l'annulation des actes afférents à ces investigations en raison de l'absence d'autorisation judiciaire (requête, p. 18 et 19). A aucun moment, il n'est donc question des réquisitions délivrées durant l'information, en application de l'article 99-3 du code de procédure pénale, sur commission rogatoire du juge d'instruction.

Dans les mémoires qu'il a déposés à la suite de sa requête, le demandeur ne dirige pas davantage sa contestation contre ces réquisitions. D'abord, la question prioritaire de constitutionnalité qu'il a soumise à la chambre de l'instruction aux fins de transmission portait exclusivement sur les articles L. 34-1 CPCE , 60-1 et 60-2 du code de procédure pénale. Elle laissait donc hors du champ de la critique les articles 99-3 et 99-4 de ce code. Par ailleurs, dans son mémoire complémentaire à sa requête en nullité, le requérant souligne que le contrôle de l'autorité judiciaire était assuré de manière lointaine par le ministère public (p. 10), confirmant ainsi que seules étaient contestées par lui les réquisitions délivrées dans la phase d'enquête, placée sous l'autorité du magistrat du parquet et non celles délivrées au cours de l'information, conduite par le juge d'instruction.

Nous vous proposons ainsi de retenir qu'en tant qu'il reproche à la chambre de l'instruction d'avoir méconnu l'article 8 de la Convention européenne de sauvegarde des droits de l'homme en écartant la demande d'annulation des réquisitions aux fins de communication des données de connexion tirée de ce qu'elles n'auraient pas été précédées de l'autorisation d'une autorité indépendante, le moyen porte exclusivement sur les réquisitions délivrées au cours de l'enquête de flagrance qu'elles aient donné lieu à exploitation au cours de cette enquête ou ultérieurement.

Nous avons vu par ailleurs que M.[L][E] est irrecevable à critiquer d'autres réquisitions que celles qui portaient sur les lignes téléphoniques dont il a reconnu l'usage (v supra 1.2.3).

3.1.2.- Portée du moyen

Devant la chambre de l'instruction, M.[L][E] a soutenu en substance que les réquisitions tendant à obtenir les données de connexion afférentes aux téléphones utilisés par lui afin, notamment, d'identifier ses correspondants et de suivre ses déplacements le jour des faits, constituaient une atteinte grave à sa vie privée qui aurait dû faire l'objet d'une "autorisation" motivée de "l'autorité judiciaire". Il a soutenu qu'à défaut d'une telle autorisation, les réquisitions litigieuses devaient être annulées comme ayant été délivrées en violation de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme.

Bien que l'argumentation qu'il a développée devant la chambre de l'instruction ne soit pas d'une parfaite clarté, il semble qu'il ait entendu contester l'absence de "*contrôle de nature juridictionnelle préalablement à l'intervention de l'ensemble des opérations*" (mémoire, p. 10, § 1er).

Curieusement, la critique a été articulée exclusivement sur le fondement de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme alors même que l'intéressé soutenait par ailleurs, comme on l'a vu, que la conservation générale et indifférenciée des données de connexion était contraire au droit de l'Union. Devant vous, le demandeur n'a pas modifié le fondement de sa critique.

Néanmoins, nous vous proposons d'en examiner d'abord le bien-fondé au regard du droit de l'Union. Il ne s'agit pas de soulever un moyen d'office mais d'apprécier la valeur du moyen au regard de la règle de droit considérée dans toutes ses dimensions. L'élargissement du champ du débat n'implique, bien entendu, aucune appréciation factuelle qui échapperait à votre office. Il nous paraît d'autant plus nécessaire que la question de la conformité au droit de l'Union des dispositions de notre code de procédure pénale est aujourd'hui, au sein des juridictions, un sujet de préoccupation majeur. En l'absence d'intervention législative, une clarification apparaît indispensable.

3.2.- Question de la conformité au droit de l'Union des dispositions relatives à l'accès aux données de connexion

3.2.1.- Rôle essentiel du ministère public au cours de l'enquête

Rappelons que les réquisitions aux fins d'obtention des données de connexion peuvent être délivrées, tant au cours de l'enquête de flagrance, en vertu des articles 60-1 et 60-2 du code de procédure pénale, qu'au cours de l'enquête préliminaire, en vertu des articles 77-1-1 et 77-1-2 du même code, par un officier de police judiciaire ou, sous son contrôle, par un agent de police judiciaire (v. supra, 1.1.1). Dans les deux cas, le procureur de la République tient une place essentielle.

Dans le cadre de l'enquête préliminaire, la réquisition doit être délivrée sur son autorisation s'il ne décide pas de la délivrer lui-même.

Si, dans le cadre de l'enquête de flagrance, son autorisation n'est pas nécessaire, cette enquête se déroule néanmoins sous son contrôle étroit ainsi que l'énonce l'article 53 du code de procédure pénale. Deux dispositions tendent à assurer l'effectivité de ce contrôle pour y soumettre les initiatives des enquêteurs de manière immédiate et constante. En premier lieu, l'article 54 fait obligation à l'officier de police judiciaire avisé de la commission d'un crime flagrant d'en informer "immédiatement" le procureur de la République. En second lieu, en vertu des deuxième et troisième alinéas de l'article 53, la durée de l'enquête de flagrance est limitée à huit jours et ne peut être prolongée qu'une fois pour la même durée, sur décision du procureur de la République, dans les conditions prévues par les dispositions considérées.

En l'espèce, bien que, agissant en flagrance, les policiers de la brigade criminelle ne fussent pas tenus de demander l'autorisation du parquet avant de délivrer leurs réquisitions en matière de téléphonie, il résulte des pièces de la procédure dont vous avez le contrôle qu'ils l'ont systématiquement sollicitée (D 567, D 568, D 569 et D 573). Autrement dit, ils ont agi en flagrance en respectant les formes de l'enquête préliminaire.

Il est ainsi essentiel, pour la réponse au moyen, de savoir si l'autorisation du procureur de la République, pendant l'enquête préliminaire, ou le contrôle exercé par lui, au cours de l'enquête de flagrance, peut être regardé comme suffisant au regard des exigences du droit de l'Union.

3.2.2.- Droit de l'Union

3.2.2.1.- Subordination de l'accès à l'autorisation d'un juge ou d'une "entité administrative indépendante"

a) *Principe : exigence d'une autorisation préalable*

Dans son arrêt du 8 avril 2014 *Digital Rights*, par lequel elle a invalidé la directive 2006/24/CE du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques[52], la Cour de justice de l'Union européenne a relevé, au nombre des insuffisances de la directive, que l'accès aux données conservées par les autorités nationales compétentes dans le cadre "*de procédures de prévention, de détection ou de poursuites pénales*" n'était "*pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante*" (point 62). Dans le prolongement de cette solution, la Cour de justice a dit pour droit dans son arrêt *Tele 2* du 21 décembre 2016 : "*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 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 (...)".* Sur le fondement des mêmes dispositions, l'exigence d'un *"contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante"* a été rappelée par la Cour dans son arrêt du 6 octobre 2020, *La Quadrature du Net*, pour le recueil en temps réel des données relatives au trafic et des données de localisation - recueil auquel notre législation réserve la dénomination de géolocalisation - (point 189), puis, à nouveau, dans ses arrêts *Prokuratuur* du 2 mars 2021 (point 51) et *Commissioner of An Garda Síochána* du 5 avril 2022 (point 106) pour le recueil des données en temps différé.

b) *Tempérament en cas d'urgence : autorisation à bref délai*

La Cour de justice a toutefois réservé "*les cas d'urgence dûment justifiés*". Il n'y a pas lieu en ces cas à autorisation préalable mais "*le contrôle doit intervenir dans de brefs délai*s" (*La Quadrature du Net*, point 189 ; *Prokuratuur*, point 51 ; *Commissioner of An Garda Síochána*, point 110). La Cour ne précise pas ce qu'il convient d'entendre par "*brefs délais*". Les dispositions internes relatives à la géolocalisation en temps réel qui, instituant un dispositif comparable, permettent à l'officier de police judiciaire, *"en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens*", de mettre en place la mesure sans l'autorisation judiciaire normalement nécessaire, impose que le contrôle de l'autorité judiciaire compétente - alors procureur de

[52] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE

la République ou juge d'instruction selon le cas - intervienne dans les vingt-quatre heures. Il prend alors la forme d'une autorisation, par l'autorité judiciaire compétente, de poursuivre la mesure (art. 230-35 CPP). La notion de "brefs délais" utilisée par la Cour, qui implique que l'autorisation intervienne dès que possible, ne semble pas ouvrir un délai beaucoup plus long, même s'il n'est pas aisé de fixer une limite[53].

3.2.2.2.- Autorité administrative indépendante et ministère public

a) *Critères dégagés par l'arrêt* Prokuratuur

L'arrêt *Prokuratuur* par lequel la Cour de justice a eu à statuer à l'égard des magistrats du parquet estonien fournit des éléments de réponse très précis (points 46 à 52).

Dans cet arrêt, la Cour pose en principe que, pour être en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête pénale et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, l'entité administrative "*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"* (points 52 et 53).

La Cour en déduit que l'exigence d'indépendance impose que l'entité ou l'autorité "*ait la qualité de tiers par rapport à celle qui demande l'accès aux données*". Pour la Cour, ce positionnement est le seul de nature à assurer l'exercice du contrôle "*de manière objective et impartiale à l'abri de toute influence extérieure*". Envisageant le cas où le contrôle préalable s'inscrit dans le cadre d'une enquête pénale, la Cour précise que l'exigence implique que l'autorité qui en est chargée, "*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*" (point 54).

Elle en tire la conséquence que ne satisfait pas à l'exigence d'indépendance ainsi définie "*un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique*", retenant que "*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*". Autrement dit, à ses yeux, le magistrat du ministère public, qui n'est pas un juge, n'est pas non plus dans une position de juge (point 55).

Le fait que le ministère public jouisse d'un statut garantissant son indépendance ou son autonomie à l'égard de l'autorité publique de même que les dispositions lui confiant une fonction de contrôleur impartial de la procédure ne suffisent donc pas à faire de lui une "entité administrative indépendante" dès lors que, fonctionnellement, il est lui-même impliqué dans l'enquête et en charge de la poursuite. La Cour de justice, achevant de

---

[53] On rappellera que la Cour européenne des droits de l'homme, a tenu pour régulière au regard des stipulations de l'article 5, § 3, de la Convention faisant obligation de présenter "*aussitôt*" devant un juge la personne privée de liberté, une présentation intervenue dans les quatre jours de l'arrestation (CEDH 3 oct. 2006, *Mc Kay c/ Royaume-Uni*, n° 543/03).

Le Conseil constitutionnel s'est montré plus exigeant s'agissant de l'obligation qui était alors faite à l'officier de police judiciaire d'aviser le procureur de la République "*dans les meilleurs délais*" en cas de placement en garde à vue. Pour lui, elle devait "*s'entendre comme prescrivant une information qui, si elle ne peut être immédiate pour des raisons objectives tenant aux nécessités de l'enquête, doit s'effectuer dans le plus bref délai possible de manière à assurer la sauvegarde des droits reconnus par la loi à la personne gardée à vue*" (Déc. 93-326 DC,11 août 1993, § 3).

Il ne s'agit pas de transposer ces solutions mais de mettre en évidence la relative flexibilité de la notion de brièveté.

fermer la porte, énonce que "*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*" (point 56).

Sans surprise, la Cour conclut que "*le ministère public n'est pas en mesure d'effectuer le contrôle préalable qu'exige la protection du droit à la vie privée et à la protection des données personnelles*" (point 57). Elle a donc dit pour droit que "*l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale*".

b) *Complément apporté par l'arrêt Commissioner of An Garda Síochána*

Dans son arrêt *Commissioner of An Garda Síochána,* la Cour de justice a réaffirmé fermement cette solution. Elle a rappelé qu'un *"ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique ne peut se voir reconnaître la qualité de tiers par rapport aux intérêts légitimes en cause"* et relevé à nouveau que la mission d'un tel ministère public est "*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"* (point 109)*.*

En outre, dans ce même arrêt, la Cour de justice a eu à se prononcer sur le point de savoir s'il était possible de considérer comme étant assuré par une entité administrative indépendante, le contrôle préalable des demandes d'accès aux données de connexion confié à un fonctionnaire de police d'un rang assez élevé - extérieur à l'enquête. Après avoir rappelé, dans les termes de l'arrêt *Prokuratuur*, les conditions auxquelles devait satisfaire une telle entité, elle a répondu par la négative. Elle a estimé que ce fonctionnaire ne revêtait pas la qualité de tiers par rapport aux services de police demandeurs de sorte qu'il ne remplissait pas les exigences d'indépendance et d'impartialité (point 111). Bien qu'il ne concerne pas sur ce point le ministère public, l'arrêt éclaire la conception étroite qu'a la Cour du tiers à la procédure d'enquête. Il ne suffit pas que l'agent ne concoure pas lui-même à l'enquête. Il faut qu'il soit détaché de ceux qui y concourent.

3.2.3.- Non conformité des dispositions nationales

3.2.3.1.- Position de la question

Il reste à apprécier la conformité à l'article 15, paragraphe 1, de la directive 2002/58 tel qu'interprété par la Cour de justice de l'Union européenne, des dispositions précitées de notre code de procédure pénale permettant aux enquêteurs de requérir auprès des fournisseurs de services de communications électroniques l'accès aux données de connexion. La question est de savoir si le ministère public peut être regardé comme une autorité administrative indépendante de sorte que son autorisation ou, à tout le moins, son contrôle immédiat, pourrait assurer la conformité des dispositions nationales précitées avec

le droit de l'Union. Ainsi posée, la question peut surprendre voire heurter car, par essence, s'ils peuvent être considérés comme indépendants, les magistrats du ministère public ne sont pas des autorités administratives - et, accessoirement, pourraient avoir quelque réticence à se voir désigner comme des "entités". Bien plus, l'appellation contredit leur appartenance à l'autorité judiciaire. Appliquée à eux, elle fait figure d'oxymore constitutionnel. Mais, bien entendu, dans le présent débat, la notion d'autorité administrative indépendante doit être vue comme une notion autonome du droit de l'Union ayant sa définition propre, étrangère aux catégories nationales. En tout état de cause, la Cour ne laisse guère le choix. Au regard de sa jurisprudence, le ministère public n'étant pas une juridiction, il ne peut valablement autoriser ou contrôler l'accès aux données de connexion que s'il est considéré comme une autorité administrative indépendante.

3.2.3.2.- Constat de non conformité

A la lumière de la jurisprudence de la Cour de justice que nous avons rappelée, il ne fait guère de doute que cette solution ne peut être retenue. Pour reprendre les mots d'Alexandre Lallet dans ses conclusions devant le Conseil d'Etat dans l'affaire *French Data Network*, le procureur estonien "*ressemble furieusement à son homologue français*", sa mission étant très exactement, pour reprendre cette fois les mots de la Cour*, "de diriger la procédure d'instruction pénale*" [autrement dit l'enquête] *et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure"* - deux attributions incompatibles, selon la Cour, avec la position de tiers indépendant*.*

S'agissant de la direction des enquêtes, les pouvoirs du procureur de la République résultent des dispositions générales des articles 12, 39-3 et 41 du code de procédure pénale ainsi que de celles de l'article 75 applicables à l'enquête préliminaire[54]. Aux termes des deux premiers alinéas de l'article 41 qui font un peu la synthèse de l'ensemble : "*Le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale.*/*A cette fin, il dirige l'activité des officiers et agents de la police judiciaire".* En son quatrième alinéa, l'article 41 confère en outre au procureur de la République *"tous les pouvoirs et prérogatives attachés à la qualité d'officier de police judiciaire",* encore qu'il n'ait pas lui-même cette qualité. L'article 68 prévoit d'ailleurs qu'en cas d'infraction flagrante, *"s'il se transporte sur les lieux, son arrivée dessaisit l'officier de police judiciaire*" et qu'il "*a alors la possibilité d'accomplir lui-même la totalité des actes de police judiciaire*".

Par ailleurs, sans qu'il soit nécessaire de s'y appesantir, "*l'exercice de l'action publique est l'attribution essentielle du ministère public*"[55]. Elle lui est confiée par l'article 31 du code de procédure pénale, qui prolonge l'article 1er du même code[56]. C'est à lui qu'il revient

---

[54] Art. 12 *La police judiciaire est exercée, sous la direction du procureur de la République, par les officiers, fonctionnaires et agents désignés au présent titre.*

Art. 39-5 *Dans le cadre de ses attributions de direction de la police judiciaire, le procureur de la République peut adresser des instructions générales ou particulières aux enquêteurs* (...)

Art. 75 *Les officiers de police judiciaire et, sous le contrôle de ceux-ci, les agents de police judiciaire désignés à l'article 20 procèdent à des enquêtes préliminaires soit sur les instructions du procureur de la République, soit d'office.*

[55] F. Molins, *Le ministère public*, Rép. Dall., n° 88

[56] Art. 1er *L'action publique pour l'application des peines est mise en mouvement et exercée par les magistrats ou par les fonctionnaires auxquels elle est confiée par la loi* (...)

Art. 31 *Le ministère public exerce l'action publique et requiert l'application de la loi, dans le respect du principe d'impartialité auquel il est tenu.*

d'apprécier, dans le cadre tracé par l'article 40-1, s'il y a lieu d'exercer les poursuites devant la juridiction d'instruction ou de jugement, le cas échéant à l'issue des investigations qu'il aura lui-même dirigées[57]. Une fois l'action publique mise en mouvement, c'est à lui qu'il appartient de l'exercer auprès de la juridiction saisie en soutenant l'accusation et en présentant les demandes ou en formant les recours qu'il estime utiles.

Certes, plusieurs dispositions du code de procédure pénale placent les magistrats du ministère public dans la position d'une autorité de contrôle objective et impartiale, jouissant, dans la conduite des enquêtes, d'une indépendance à l'égard du pouvoir exécutif. Il en est ainsi de l'article 30, aux termes duquel le garde des Sceaux *"ne peut leur adresser aucune instruction dans des affaires individuelles*", de l'article 31, qui leur impose "*le respect du principe d'impartialité"* et de l'article 39-3 qui leur confie la mission, d'une part, "*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*" et, d'autre part, de veiller à ce que les investigations soient accomplies "*à charge et à décharge, dans le respect des droits de la victime, du plaignant et de la personne suspectée*". Ce rôle de garant a été encore renforcé par la loi du n° 2021-1729 du 22 décembre 2021[58] qui, modifiant l'article 77-2 du code de procédure pénale, confie au procureur de la République d'importantes prérogatives pour l'encadrement de l'accès au dossier pendant l'enquête.

Toutefois, bien que le ministère public estonien fût investi d'une semblable mission de garant et d'une indépendance comparable, la Cour de justice n'en a pas moins jugé qu'il ne pouvait être qualifié d'entité administrative indépendante en raison de son implication dans la conduite des investigations et l'exercice de l'action publique. Il nous paraît que la même solution s'impose s'agissant du ministère public français. L'indépendance dont il jouit à l'égard du pouvoir exécutif permet certes que lui soit reconnue, pour l'application des dispositions relatives au mandat d'arrêt européen, la qualité d'autorité judiciaire d'émission[59], mais elle ne fait pas de lui un tiers à la procédure habilité à autoriser l'accès à des données de connexion.

Au cours de l'enquête de flagrance, il pourrait être soutenu que cette conclusion est de peu de conséquence dans la mesure où, nous l'avons vu, la Cour de justice admet qu'en cas d'urgence, l'enquêteur peut requérir la communication de données de connexion sans l'autorisation préalable d'une autorité indépendante. On observera cependant que, s'il y a souvent urgence en cas de flagrance, les deux notions ne coïncident pas. Elles sont d'ailleurs dissociées dans plusieurs dispositions du code de procédure pénale qui, y compris dans le cadre de l'enquête de flagrance, ne permettent aux officiers de police judiciaire d'agir sans autorisation judiciaire préalable qu'en cas d'urgence. Il en est ainsi, notamment, pour la mise en oeuvre de mesure de géolocalisation en temps réel (v. art. 230-33 et 230-35 CPP). En outre, si l'urgence justifie l'absence d'autorisation préalable, la Cour impose, on l'a vu, qu'un contrôle intervienne *dans de brefs délai*s". Or les dispositions des articles 60-1 et 60-2 du code de procédure pénale n'organisent pas un tel contrôle

---

[57] *Lorsqu'il estime que les faits qui ont été portés à sa connaissance en application des dispositions de l'article 40 constituent une infraction commise par une personne dont l'identité et le domicile sont connus et pour laquelle aucune disposition légale ne fait obstacle à la mise en mouvement de l'action publique, le procureur de la République territorialement compétent décide s'il est opportun : /1° Soit d'engager des poursuites ; / 2° Soit de mettre en oeuvre une procédure alternative aux poursuites en application des dispositions des articles 41-1, 41-1-2 ou 41-2 ; / 3° Soit de classer sans suite la procédure dès lors que les circonstances particulières liées à la commission des faits le justifient.*

[58] Loi du n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire

[59] CJUE, 12 déc. 2019, *cour d'appel du Luxembourg et tribunal d'Amsterdam*, C-566/19 PPU et C-626/19, points 54 et 55

auquel ne peut être assimilé celui exercé par la chambre de l'instruction ou la juridiction de jugement, sur contestation de l'intéressé, plusieurs mois voire plusieurs années après la délivrance des réquisitions, sur le fondement des articles 173, 206 ou 385 du code de procédure pénale.

3.2.3.3.- Inopposabilité de l'obstacle constitutionnel

a) Une solution en discordance avec la jurisprudence constitutionnelle

Suivant une approche comparable à celle de la Cour de justice de l'Union européenne, le Conseil constitutionnel veille à ce que les dispositions autorisant l'accès de l'autorité publique à des données de connexion pour la prévention des atteintes à l'ordre public ou la recherche des auteurs d'infractions assurent une conciliation équilibrée entre la poursuite de cet objectif de valeur constitutionnelle et le droit au respect de la vie privée. Comme la Cour de justice, il juge que cette conciliation impose le contrôle préalable d'une autorité indépendante. Il l'a d'abord affirmé dans plusieurs décisions rendues au cours des années 2015 à 2019 relatives aux textes qui accordaient le droit d'obtenir la communication de données de connexion aux agents de l'Autorité de la concurrence[60], de l'Autorité des marchés financiers[61], de la Haute autorité pour la transparence de la vie politique[62] ou encore aux agents des douanes[63]. Le Conseil constitutionnel a prononcé autant de censures à la suite desquelles le législateur a modifié les textes considérés pour subordonner l'accès aux données de connexion, selon le cas, à l'autorisation d'une autorité administrative indépendante ou à celle de l'autorité judiciaire en la personne du procureur de la République[64].

La question de la conformité à la Constitution des dispositions organisant l'accès aux données de connexion au cours de la procédure pénale n'a été soumise que plus récemment au Conseil constitutionnel. Votre chambre l'a saisi de plusieurs questions prioritaires de constitutionnalité portant sur les articles 60-1 et 60-2 applicables au cours de l'enquête de flagrance[65], 77-1-1 et 77-1-2 applicables au cours de l'enquête préliminaire[66] et 99-3 et 99-4 applicables au cours de l'information[67]. Toutefois, à ce jour, le Conseil n'a statué que sur la question portant sur les articles 77-1-1 et 77-1-2, les autres questions, très récemment transmises, étant pendantes devant lui.

---

[60] Déc. 2015-715 DC du 5 août 2015

[61] Déc. n° 2017-646/647 QPC, 21 juill. 2017

[62] Déc. 2017-752,753 DC, 8 sept. 2017

[63] Déc. 2018-764 QPC, 15 févr. 2019

[64] Procureur de la République en matière fiscale et douanière (v. art. 65 quinquies C. douanes et L.96G LPF issus de L. n° 2018-898, 23 oct. 2018) ; AAI pour l'AMF (art. L.612-10-2 CMF issu de la même loi) et l'AC (art . L.450-3-3 C. com. issu de L. n° 2019-486, 22 mai 2019)

[65] Crim. 8 mars 2022, n° 21-90.046

[66] Crim. 21 sept. 2021, n° 21-90.032

[67] Crim. 20 avr. 2022, n° 22-90.003

Dans sa décision n° 2021-952 QPC du 3 décembre 2021, le Conseil constitutionnel a jugé que la communication ou l'accès aux données de connexion organisé par les articles 77-1-1 et 77-1-2 n'était pas entouré 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*". Il a souligné, d'une part, le caractère attentatoire à la vie privée d'un tel accès et, d'autre part, le champ très large de l'enquête préliminaire qui, contrairement à l'enquête de flagrance, "*peut porter sur tout type d'infraction et qui n'est pas justifiée par l'urgence ni limitée dans le temps*". Cependant, le Conseil constitutionnel n'a pas remis en cause, dans son principe, la constitutionnalité des dispositions confiant au procureur de la République le pouvoir de requérir la communication de données de connexion ou d'autoriser les réquisitions délivrées à cette fin. Il a rappelé que le procureur de la République est un "*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*".

Si le magistrat du parquet, dont la mission est de représenter les intérêts de la société, se voit reconnaître ainsi, dans l'ordre constitutionnel, une mission de protection des droits fondamentaux c'est que, dans un Etat de droit, les deux missions sont, pour lui, indissociables en raison de son appartenance à l'autorité judiciaire. Pour reprendre la formule du Conseil, "*l'autorité judiciaire qui, en vertu de l'article 66 de la Constitution, assure le respect de la liberté individuelle, comprend à la fois les magistrats du siège et ceux du parquet*"[68]. En raison précisément de la mission que lui confère l'article 66, elle doit assurer la direction et le contrôle de la police judiciaire[69]. La direction de la police judiciaire par un magistrat du parquet trouve ainsi son fondement constitutionnel dans l'appartenance de ce magistrat à l'autorité judiciaire qui lui fait obligation de veiller à la garantie des droits. C'est précisément après l'avoir rappelé que le Conseil a censuré des dispositions qui avaient ouvert aux officiers ou agents de police judiciaire la possibilité de requérir auprès de tout organisme public des informations intéressant l'enquête, sans avoir à y être autorisés par le procureur de la République[70].

En outre, se fondant sur les dispositions des articles 16 de la Déclaration de 1789, 20, 64 et 65 de la Constitution, le Conseil constitutionnel a posé en principe que "*la Constitution consacre l'indépendance des magistrats du parquet, dont découle le libre exercice de leur action devant les juridictions"*, même si, selon le Conseil, "*cette indépendance doit être conciliée avec les prérogatives du Gouvernement et qu'elle n'est pas assurée par les mêmes garanties que celles applicables aux magistrats du siège*"[71]. Votre chambre a également relevé cette indépendance, en réponse à une question prioritaire de constitutionnalité[72].

---

[68] v. not. Déc. n° 93-326 DC, 11 août 1993 ; Déc. n° 97-389 DC, 22 avr. 1997, cdt 61; Déc. 2002-461 DC, 29 août 2002 cdt 74 ; Déc. 2003-484 DC, 20 nov. 2003, cdt 75 ; Déc. 2019-778 DC, 21 mars 2019, § 179

[69] Déc. n° 2011-625 DC, 10 mars 2011, cdt 59 ; Déc. 2014-693 DC, 25 mars 2014, cdt 11 ; Déc. n° 2019-778, 21 mars 2019, § 141 ; Déc. n° 2021-817 DC, 20 mai 2021, § 6

[70] Déc. n° 2019-778 DC, 21 mars 2019, § 175

[71] Déc. n° 2017-680 QPC, 8 déc. 2017, § 9

[72] Crim. 17 janv. 2017, n° 16-86.077

Certes, l'intervention du magistrat du parquet ne constitue pas, pour le Conseil constitutionnel, *"une garantie équivalente à celle d'un magistrat du siège*"[73] mais la garantie qu'elle assure est suffisante dès lors que l'atteinte aux droits de la personne portée par la mesure placée sous son contrôle n'excède pas un certain seuil. Le Conseil constitutionnel en a jugé ainsi en matière d'atteinte à la liberté individuelle[74] comme en matière d'atteinte à la vie privée. En cette matière, le seuil est dépassé s'il s'agit d'interception de correspondances permettant d'accéder au contenu de celles-ci[75]. En revanche, il ne l'est pas s'il s'agit de requérir ou autoriser la mise en oeuvre de mesures de géolocalisation en temps réel pour une durée de quinze jours compte tenu de l'ensemble des garanties prévues par ailleurs[76]. La décision précitée du Conseil constitutionnel du 3 décembre 2021, admettant au moins implicitement la compétence du procureur de la République pour l'obtention des données de connexion en temps différé se situe dans la droite ligne de ce précédent. De la même façon, au regard de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, vous établissez une gradation en fonction de l'atteinte à la vie privée. Ainsi, tout en subordonnant à une autorisation judiciaire préalable la mise en place d'un système de vidéosurveillance de la voie publique à des fins de police judiciaire, vous avez admis que cette autorisation puisse être délivrée, pendant l'enquête, par le procureur de la République[77].

b) *Une discordance ne faisant pas obstacle à l'application du droit de l'Union*

Il est ainsi possible d'affirmer que, dans l'ordre constitutionnel, le magistrat du ministère public, membre de l'autorité judiciaire, est une autorité indépendante habilitée, comme telle, à autoriser, dans certaines limites, les mesures portant atteinte à la vie privée, solution d'ailleurs inscrite au sixième alinéa du II de l'article préliminaire du code de procédure pénale.

---

[73] v. Commentaire aux Cahiers de Déc. n° 2019-778 DC, 21 mars 2019, préc.

[74] Déc. n° 2010-80 QPC, 17 déc. 2010, cdt 11: si l'autorité judiciaire comprend à la fois les magistrats du siège et du parquet, l'intervention d'un magistrat du siège est requise pour la prolongation de la garde à vue au-delà de quarante-huit heures" , le magistrat du parquet étant compétent pour prolonger la mesure au-delà de vingt-quatre heures

[75] Déc. 2019-778 DC - 21 mars 2019, § 137 à 148 : le seuil est dépassé lorsqu'il s'agit d'intercepter le contenu des correspondances, même en cas d'urgence,

[76] Déc. 2021-930 QPC - 23 sept. 2021, § 15 ; Déc. n° 2014-693 DC du 25 mars 2014

[77] Crim. 18 mai 2021, n° 20-86.266 ; Crim. 8 déc. 2020, n° 20-83.885

Pour autant, cette circonstance ne vous permet pas de refuser d'appliquer le droit de l'Union. Dans un arrêt récent, rendu sur une question préjudicielle émanant d'une juridiction d'appel roumaine[78], la Cour de justice de l'Union européenne a rappelé avec fermeté que le droit de l'Union s'opposait à une règle nationale en vertu de laquelle les juridictions nationales ne seraient pas habilitées à examiner la conformité avec ce droit d'une législation nationale qui aurait été jugée constitutionnelle par un arrêt de la Cour constitutionnelle de l'Etat membre considéré. En particulier, elle a retenu qu'une cour constitutionnelle ne pouvait, au mépris des obligations qui lui incombent en vertu du droit de l'Union, s'autoriser à écarter l'application d'une norme de ce droit, au motif qu'elle méconnaîtrait l'identité nationale de l'Etat membre concerné telle que définie par la cour constitutionnelle nationale. Pour la Cour, si la cour constitutionnelle d'un État membre estime qu'une disposition de droit dérivé de l'Union, telle qu'interprétée par elle, méconnaît l'obligation de respecter l'identité nationale de l'État, elle doit la saisir d'une demande de décision préjudicielle, en vue d'apprécier la validité de cette disposition à la lumière de l'article 4, paragraphe 2, TUE[79], la Cour étant seule compétente pour constater l'invalidité d'un acte de l'Union.

La voie d'une conciliation de cette solution avec celle du Conseil constitutionnel selon laquelle "*la transposition d'une directive ne saurait aller à l'encontre d'une règle ou d'un principe inhérent à l'identité constitutionnelle de la France*"[80] paraît assez étroite. Au cas présent, vous pourriez envisager d'examiner si l'existence d'un ministère public, partie intégrante de l'autorité judiciaire instituée par la Constitution, jouissant d'un statut d'indépendance et concourant à la protection des droits fondamentaux au cours de la procédure pénale, constitue un élément inhérent à l'identité constitutionnelle de la France[81], point sur lequel vous exercez votre contrôle[82].

Cependant, par ses arrêts précités, la Cour de justice de l'Union européenne ne remet pas en cause l'institution du ministère public. Elle délimite de manière plus étroite le champ de son intervention en matière d'accès aux données de connexion en raison de la gravité de l'atteinte à la vie privée qui, selon son analyse, en résulte. Même si la solution peut prêter à discussion, il nous paraît difficile de soutenir qu'en renforçant les garanties protectrices de

---

[78] CJUE, 22 févr. 2022, *RS, Cour d'appel de Craiova* (Roumanie), n° C-430/21

[79] *L'Union respecte l'égalité des États membres devant les traités ainsi que leur identité nationale, inhérente à leurs structures fondamentales politiques et constitutionnelles, y compris en ce qui concerne l'autonomie locale et régionale. Elle respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauve-garder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.*

[80] Déc. n° 2006-540 DC, 27 juill. 2006 ; Déc. n° 2010-79 QPC, 17 déc. 2010 ; Déc. n° 2021-940 QPC, 15 oct. 2021

[81] Au même titre que l'interdiction de déléguer à des personnes privées des compétences de police administrative générale inhérentes à l'exercice de la « force publique » nécessaire à la garantie des droits, reconnue comme un principe inhérent à l'identité constitutionnelle de la France par le Conseil constitutionnel dans sa décision précitée n° 2021-940 QPC, du 15 octobre 2021.

[82] v. Crim. 22 févr. 2012, n° 11-90.122, B. n° 54 ; Crim. 10 août 2016, n° 16-90.016

la vie privée, la Cour de justice aurait porté atteinte à l'identité constitutionnelle de la France. Rappelons que, naguère, votre chambre a jugé, sur le fondement de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, qu'en raison de la gravité de l'atteinte à la vie privée résultant de la géolocalisation en temps réel, celle-ci devait être autorisée par un juge du siège[83].

En tout état de cause, si vous aviez un doute sur ce point, à défaut de pouvoir saisir le Conseil constitutionnel d'une question préjudicielle qui permettrait de le lever - ce qui est d'ailleurs dommage car la réponse à la question de la conformité de la norme de droit dérivé au noyau dur de l'ordre constitutionnel devrait lui revenir - il vous faudrait, sans détour par le Conseil, saisir la Cour de justice de l'Union européenne d'une telle question, conformément à ses prescriptions.

3.2.3.4.- Portée de la non conformité

a) Dispositions applicables pendant l'enquête

La non-conformité au droit de l'Union des dispositions permettant, pendant l'enquête, de requérir la communication de données de connexion, implique que, sans attendre l'intervention du législateur, l'accès à des données, à ce stade de la procédure, soit autorisé par un juge[84].

Une modulation selon la quantité des données de trafic et de localisation sollicitée nous paraît exclue par la Cour de justice pour laquelle "*même l'accès à une quantité limitée de données relatives au trafic ou de données de localisation ou l'accès à des données pour une courte période peut être susceptible de fournir des informations précises sur la vie privée d'un utilisateur d'un moyen de communication électronique*". En outre, la Cour estime que "*l'appréciation de la gravité de l'ingérence que constitue l'accès s'effectue nécessairement en fonction du risque généralement afférent à la catégorie de données sollicitées pour la vie privée des personnes concernées, sans qu'il importe, par ailleurs, de savoir si les informations relatives à la vie privée en découlant présentent ou non, concrètement, un caractère sensible*" (*Prokuraturr*, point 40).

Toutefois, la Cour de justice n'évoque que les données relatives au trafic et les données de localisation. Il s'ensuit que l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante n'apparaît pas nécessaire lorsqu'il s'agit d'accéder à des données relatives à l'identité civile des utilisateurs. La solution est logique dès lors que, par ailleurs, comme nous l'avons vu, en raison du caractère limité de l'atteinte à la vie privée que constituent la conservation et l'accès à de telles données, l'une et l'autre sont possibles sans restriction pour la lutte contre la criminalité en général (CJUE *Ministério fiscal*, pour

---

83 Crim., 22 oct. 2013, n° 13-81.945, B, n° 196

84 Rappelons que depuis loi n° 2021 -1729 du 22 décembre 2021,les réquisitions portant sur des données de connexion émises par un avocat. doivent alors êtres "faites par ordonnance motivée du juge des libertés et de la détention" en vertu de l'article 60-1-1 du CPP auquel se réfèrent les articles 77-1-1 et 99-3 (v. supra 1.1.4).

l'identification du titulaire d'une carte SIM ; CJUE*, La Quadrature du Net*, points 157 à 159 ; CJUE, *Commissioner of An Garda Síochána*, point 72).

C'est l'occasion de rappeler que la Cour de justice impose que l'accès aux données relatives au trafic et aux données de connexion dans le cadre des procédure pénales ne soit ouvert que pour la lutte contre la criminalité grave. Bien que, dans leur rédaction antérieure à la loi n° 2022-299 du 2 mars 2022, les dispositions des articles 60-1, 60-2, 77-1-1 et 77-1-2 n'aient comporté aucune limite tenant à la gravité de l'infraction, l'exigence de la Cour de justice doit être prise en compte pour les réquisitions délivrées avant l'entrée en vigueur de cette loi. Ce point a déjà été abordé (v. supra 1.2.2).

Enfin, si, pour l'essentiel, la solution retenue par la Cour de justice accroît les contraintes procédurales, il convient de relever qu'à certains égards, elle les allège. La Cour permet en effet qu'en cas d'urgence, l'officier de police judiciaire puisse, sans autorisation préalable, requérir la communication de données de connexion. Or, les dispositions de l'article 77-1-1 du code de procédure pénale applicables au cours de l'enquête préliminaire n'ouvrent pas une telle possibilité.

Il reste que, selon une étude d'impact établie par le ministère de la justice, en retenant l'hypothèse, favorable, où il ne porterait pas sur les réquisitions aux fins d'identification de l'abonné, le transfert de compétence impliquerait la création d'environ 536 ETP de juge des libertés et de la détention - 256 étant actuellement localisés au sein des tribunaux judiciaires - et 218 ETP de fonctionnaires de greffe. S'agissant des magistrats du parquet, ce transfert impliquerait également un renforcement substantiel des effectifs ou permettrait au contraire un gain, selon que le juge des libertés et de la détention interviendrait sur la saisine du ministère public ou non.

b) Maintien de la compétence du juge d'instruction pendant l'information

En l'absence de demande d'annulation des réquisitions délivrées pendant l'instruction, le moyen est irrecevable en tant qu'il reproche à la chambre de l'instruction de n'avoir pas fait droit à une telle demande. Nous avons donc laissé hors du champ de la réflexion la question de savoir si, au regard du droit de l'Union, le juge d'instruction, sur la délégation duquel, pendant l'information, les officiers de police judiciaire peuvent, en application des articles 99-3 et 99-4 du code de procédure pénale, requérir la communication des données de connexion, doit être regardé comme étant habilité à autoriser de telles réquisitions. Nous livrerons néanmoins quelques éléments d'analyse sur ce point, ne serait-ce que pour bien circonscrire la solution retenue pour la durée de l'enquête.

Si l'on considère les deux critères retenus par la Cour de justice pour juger que le ministère public n'est pas un tiers à la procédure - participation aux investigations et exercice de l'action publique - on peut avoir quelque doute sur la position du juge d'instruction. Il pourrait être soutenu - et l'a d'ailleurs été - que la solution appliquée au ministère public lui serait transposable, dès lors que, d'une part, il "*dirige la procédure d'instruction*" et que, d'autre part, au terme de l'information, il décide s'il y a lieu de renvoyer la personne mise en examen devant la juridiction de jugement.

Toutefois, la Cour de justice prend soin de préciser que ces critères ne s'appliquent que "*lorsque* [le] *contrôle est effectué non par une juridiction, mais par une entité administrative*

indépendante" (*Prokuratuur,* point 53 ; *Commisioner of An Garda Síochána*, point 108). La distinction se conçoit aisément dès lors que la mission et la raison d'être d'une juridiction est de trancher des contestations de manière indépendante et impartiale. La Cour le met d'ailleurs clairement en évidence en énonçant que la mission du ministre public n'est pas "*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".* Le juge d'instruction étant une juridiction et non une partie à la procédure ou une autorité exclusivement chargée des investigations, il échappe à la grille d'analyse que nous avons développée plus haut. Salomon autant que Maigret pour reprendre une formule fameuse, il est appelé à trancher des contestations au cours de l'information. Lorsqu'au terme de la procédure, il rend une ordonnance de règlement, il n'exerce pas l'action publique mais, ce qui est différent, statue sur le sort de l'action publique mise en mouvement par le ministère public - ou, le cas échéant, la partie civile. Il tranche donc une contestation en arbitrant entre l'accusation et la défense. Bien évidemment, il n'exerce l'action publique à aucun stade ultérieur de la procédure. Le contrôle constant qu'il exerce sur les actes des officiers de police judiciaire délégué nous paraît, en l'état, assurer une garantie répondant aux exigences de la Cour de justice[85].

3.2.4.- Conséquences de la non-conformité au droit de l'Union

3.2.4.1.- Constat préalable : atteinte à la sécurité juridique découlant de l'incertitude entourant la règle applicable

Aux termes de l'article 112-4 du code pénal, "*l'application immédiate de la loi nouvelle est sans effet sur la validité des actes accomplis conformément à la loi ancienne*". La règle a pour objet d'assurer la sécurité juridique en empêchant que la validité d'un acte ne soit appréciée au regard d'une loi qui n'était pas en vigueur à la date à laquelle il a été accompli. Cependant le texte est sans application lorsque la loi en vigueur à cette date se trouve modifiée par l'effet d'une déclaration d'incompatibilité avec la norme supérieure comme c'est le cas en l'espèce. C'est que, juridiquement, la déclaration de non conformité a un effet rétroactif. Elle ne fait que révéler un état du droit préexistant. Pour autant, une révélation étant, par nature, rarement anticipée, elle produit sur la sécurité des procédures les mêmes effets qu'une modification. L'anticipation est particulièrement difficile en cas de conflits entre les normes supérieures telles qu'interprétées par les juridictions en charge d'en assurer la prééminence. A cet égard, malgré les enjeux considérables pour les droits des personnes et la sécurité publique, rarement, le juge national se sera trouvé dans une situation de confusion et d'incertitude semblable à celle qui s'est créée autour de la question des conditions d'accès aux données de connexion[86].

---

[85] v. pour la géolocalisation en temps réel avant la loi de 2014 : Crim. 22 nov. 2011, n° 11-84.308, B. n° 234 ; Crim. 22 oct. 2013, n° 13-81.945, B. n° 196 ; Crim. 6 janv. 2015, n° 14-85.528 (*ne méconnaît pas les dispositions des articles 6 de la Convention européenne des droits de l'homme, 81 et 151 du code de procédure pénale, la géolocalisation mise en oeuvre, antérieurement à la loi n° 2014-372 du 28 mars 2014, sur le fondement d'une commission rogatoire générale, dès lors que, obéissant aux principes de nécessité et de proportionnalité, elle l'a été sous le contrôle effectif du juge d'instruction mandant*)

[86] Cela est également vrai, sinon plus, s'agissant de la question de la conservation des données.

Jusqu'à ce jour votre Cour a toujours affirmé que l'attribution au procureur de la République du pouvoir de délivrer des réquisitions aux fins d'obtenir la communication de données de connexion ne s'analysait pas en une atteinte à la vie privée heurtant l'article 8 de la Convention européenne de sauvegarde des droits de l'homme[87], prenant soin de distinguer cette mesure de la géolocalisation en temps réel soumise à un régime plus strict[88].

Cette solution est conforme à celle pouvant être déduite des arrêts *Uzun* et *Ben Faiza* rendus par la Cour européenne des droits de l'homme, respectivement en 2010 et 2018, en matière d'accès aux données de connexion, en temps réel ou différé, pour l'élucidation d'une affaire pénale[89]. Certes, dans l'affaire, *Big Brother Watch et autres* ayant donné lieu à un premier arrêt en 2018 puis à un second, en grande chambre, en 2021[90],la Cour de Strasbourg a imposé, dans le prolongement du rapport de la Commission de Venise, l'autorisation préalable d'une autorité indépendante pouvant être un organe judiciaire ou, à tout le moins, un "*organe indépendant du pouvoir exécutif*". Mais, outre que la formule n'exclut pas formellement le ministère public en tant que tel dont, au demeurant, l'indépendance à l'égard du pouvoir exécutif a été reconnue par la Cour de justice[91], l'exigence s'applique aux "*activités d'interception en masse*", non ciblées, mises en oeuvre dans le cadre du renseignement, étrangères, en principe, au recueil de données effectué pour l'élucidation d'une affaire pénale déterminée[92]. Contrairement à ce qui est soutenu par le demandeur, ne constitue pas une activité d'interception de masse de la nature de celles ayant fait l'objet d'un strict encadrement par la Cour de Strasbourg, le recueil du "*flux des bornes téléphoniques couvrant les lieux intéressant l'enquête*", tel qu'il a été demandé en l'espèce.

Par ailleurs, dans la jurisprudence de la Cour de justice de l'Union européenne, la réponse à la question de savoir si le ministère public pouvait être regardé comme une autorité - ou une entité - administrative indépendante habilitée à autoriser l'accès aux données de connexion, n'a été apportée que par l'arrêt *Prokuratuur* du 2 mars 2021. Si les arrêts antérieurs ont clairement posé l'exigence d'une autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, ils n'ont pas donné d'indications sur les

---

87 Crim. 22 nov. 2011, n° 11-84.308, B. n° 324 ; Crim. 8 juill. 2015, n° 15-81.781, B. n° 174 ; Crim. 29 juin 2016, n° 15-82.747 ; Crim. 2 nov. 2016, n° 16-82.376, B. n° 282

88 Crim. 2 nov. 2016, n° 16-82.376, B. n° 282

89 CEDH, 8 févr. 2018, *Ben Faiza c/ France*, n° 31446/12, § 69-75 **;** CEDH, 2 sept.2010, *Uzun c. Allemagne*, n° 35623/05

90 CEDH 13 sept. 2018, *Big Brother Watch et autres c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15 ; CEDH, GC, 25 mai 2021,*ibid*, § 350

91 CJUE, 12 déc. 2019, *cour d'appel du Luxembourg et tribunal d'Amsterdam*, C-566/19 PPU et C-626/19, points 54 et 55

92 Etait en cause l'interception d'énormes volumes de données par le service britannique du renseignement électronique - « le GCHQ » (Government Communications Headquarters)

conditions que devait remplir celle-ci[93]. Bien plus, appelée à apprécier si les magistrats du ministère public français jouissaient d'un statut d'indépendance permettant de leur reconnaître la qualité d'autorité judiciaire habilitée à émettre un mandat d'arrêt européen, la Cour de justice avait répondu par l'affirmative par un arrêt du 12 décembre 2019[94]. Elle avait alors relevé "*que l'article 64 de la Constitution garantit l'indépendance de l'autorité judiciaire qui est composée des magistrats du siège et des magistrats du parquet et que, en vertu de l'article 30 du CPP, le ministère public exerce ses fonctions de manière objective à l'abri de toute instruction individuelle émanant du pouvoir exécutif, le ministre de la Justice pouvant seulement adresser aux magistrats du parquet des instructions générales de politique pénale afin d'assurer la cohérence de cette politique sur l'ensemble du territoire*", de telles instruction ne pouvant "*en aucun cas avoir pour effet d'empêcher un magistrat du parquet d'exercer son pouvoir d'appréciation quant au caractère proportionné de l'émission d'un mandat d'arrêt européen*". Elle avait en outre pris acte des déclarations du Gouvernement français selon lesquelles, "*conformément à l'article 31 du CPP, le ministère public exercerait l'action publique et requerrait l'application de la loi dans le respect du principe d'impartialité*". De ces éléments, elle avait conclu que "*les magistrats du parquet disposent du pouvoir d'apprécier de manière indépendante, notamment par rapport au pouvoir exécutif, la nécessité et le caractère proportionné de l'émission d'un mandat d'arrêt européen et exercent ce pouvoir de manière objective, en prenant en compte tous les éléments à charge et à décharge*."

Enfin, comme nous l'avons vu, le Conseil constitutionnel, a jugé à deux reprises que les dispositions attribuant au procureur de la République le pouvoir d'autoriser, pour une durée de quinze jours, une mesure de géolocalisation en temps réel assuraient une conciliation équilibrée entre l'objectif de valeur constitutionnelle de recherche des auteurs d'infractions et la protection du droit au respect de la vie privée, fondé sur l'article 2 de la Déclaration de 1789[95]. De même, lorsqu'il a eu à apprécier la conformité à cet article des dispositions de l'article 77-1-1 du code de procédure pénale, le Conseil constitutionnel, tout en prononçant une censure, n'a pas remis en cause, dans son principe, l'attribution au procureur de la République du pouvoir de requérir la communication de données de connexion ou d'autoriser les réquisitions à cette fin[96]. Il a jugé insuffisantes les garanties entourant l'exercice de ce pouvoir.

Dans un tel contexte, il nous semble que l'incertitude entourant la règle applicable a persisté au-delà de l'arrêt *Prokuratuur* du 2 mars 2021. En réalité, elle ne sera véritablement levée que par votre arrêt. Au point de convergence des normes, votre Cour est en effet seule en mesure de lever les incertitudes nées de leur conflit et d'apporter les

---

[93] Nous songeons bien sûr aux arrêts des 8 avril 2014, *Digital Rights Ireland Ldt*, 21 décembre 2016, *Tele 2 Sverige et Watson* et 6 octobre 2020, *La Quadrature du net, French Data Network*.

[94] CJUE, 12 déc. 2019, *cour d'appel du Luxembourg et tribunal d'Amsterdam*, C-566/19 PPU et C-626/19, points 54 et 55

[95] Déc. 2014-693 DC, 25 mars 2014 ; Déc. 2021-930 QPC, 23 sept. 2021

[96] Déc. n° 2021-952 QPC du 3 déc. 2021

clarifications nécessaires. Il reste à examiner de quelle manière peut être prise en compte l'exigence de sécurité juridique. S'il est exclu de différer l'application du droit de l'Union, vous pouvez envisager de moduler la sanction imposée par sa violation.

3.2.4.2.- Impossibilité de différer les effets de la non conformité

Après avoir constaté, par sa décision n° 2021-952 QPC du 3 décembre 2021, l'inconstitutionnalité partielle de l'article 77-1-1 du code de procédure pénale, pour des motifs tenant à l'insuffisance des garanties entourant la réquisition aux fins de données de connexion - sans pour autant, on l'a vu, remettre en cause le pouvoir du procureur de la République d'en autoriser la délivrance - le Conseil constitutionnel a constaté que l'abrogation immédiate des dispositions contestées entraînerait "*des conséquences manifestement excessives*". Par suite, il a reporté au 31 décembre 2022 la date de l'abrogation de ces dispositions et précisé que les mesures prises avant cette date ne pourraient être contestées sur le fondement de cette inconstitutionnalité. Nous avons vu que, de la même façon, après avoir censuré les dispositions de l'article L. 34-1 CPCE prévoyant une conservation généralisée et indifférenciée des données de trafic et de localisation pour la lutte contre la criminalité, le Conseil constitutionnel a exclu que cette censure puisse être invoquée à l'encontre des mesures prises sur le fondement des dispositions censurées, retenant que la remise en cause de ces mesures "*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".* Cette appréciation se comprend aisément lorsque l'on considère le très large recours aux réquisitions aux fins d'accéder aux données de connexion (supra, 1.1.4).

Vous pourriez ainsi envisager de différer les conséquences de la non conformité au droit de l'Union des dispositions du code de procédure pénale relatives aux réquisitions aux fins d'accès aux données de connexion pendant l'enquête, en écartant toute possibilité de censurer, à raison de cette non-conformité, les mesures qui, comme en l'espèce, auraient été prises sur le fondement de ces dispositions avant votre arrêt à venir dans la présente affaire. La solution serait d'autant plus envisageable qu'afin d'assurer la sécurité juridique et la bonne administration de la justice, il est désormais assez fréquent que vous écartiez l'application immédiate d'une solution nouvelle peu prévisible ou constituant un revirement de jurisprudence. Vous l'avez fait, par exemple, lorsque vous avez étendu l'exigence de motivation aux peines d'amende contraventionnelles[97], lorsque vous avez admis la responsabilité pénale de la société absorbante[98] ou encore lorsque vous avez posé une règle nouvelle relative au droit d'appel de la partie civile[99].

Cependant cette suspension même provisoire des effets de la déclaration de non-conformité a été exclue très fermement par la Cour de justice dans son arrêt *Commissioner of An Garda Síochána*. La Cour y énonce que *« Le droit de l'Union doit être interprété en ce*

[97] Crim., 30 mai 2018, n° 16-85.777

[98] Crim., 25 novembre 2020, n° 18-86.955

[99] Crim. 15 févr. 2022, n° 20-86.486

sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de la charte des droits fondamentaux." (point 115).

La solution procède d'une jurisprudence abondante et d'une absolue constance de la Cour de justice dont les éléments sont rappelés par elle dans ses arrêts *La Quadrature du Net* (points 216 et 2117) et *Commissioner of An Garda Síochána* (points 118, 119, 125, 126)[100].

Citant la formule de son célèbre arrêt *Costa* du 15 juillet 1964, la Cour rappelle qu'en vertu du principe de primauté du droit de l'Union, "*à défaut de pouvoir procéder à une interprétation de la législation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel*".

Certes, pour des "*considérations impérieuses de sécurité juridique*", la Cour se reconnaît le pouvoir d'accorder une "*suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national*" qui lui serait contraire. Mais elle rappelle, en premier lieu, qu'elle dispose seule de cette prérogative, en deuxième lieu, que celle-ci ne peut être exercée qu'à titre exceptionnel et, enfin, que la limitation dans le temps des effets de l'interprétation du droit de l'Union donnée par elle "*ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée*". Pour la Cour, "*il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire*".

Autrement dit, en l'absence de dispositions contraires prises par la Cour dans son arrêt, "*dès lors que l'interprétation* [qu'elle] *donne d'une règle du droit de l'Union, dans l'exercice de la compétence que lui confère l'article 267 TFUE, éclaire et précise la signification et la portée de cette règle, telle qu'elle doit ou aurait dû être comprise et appliquée depuis le moment de son entrée en vigueur, la règle ainsi interprétée peut et doit être appliquée par le juge à des rapports juridiques nés et constitués avant le prononcé de l'arrêt statuant sur la demande d'interprétation*" (*Commissioner of An Garda Síochána,* point 125*).*

Rappelons, par ailleurs, que la Cour juge de manière également constante que "*la primauté du droit* [de l'Union] *impose au juge national d'appliquer* [ce droit] *et de laisser inappliquées les dispositions nationales contraires indépendamment de l'arrêt de la juridiction*

[100] v. not. pour quelques arrêts anciens : CJCE, 8 avr. 1976, *Defrenne*, C-117/76 ; CJCE 27 mars 1980, *Denkavit*, C-61/79 ; CJCE, 27 mars 1980, *Salumi*, 66,67,128/79 ; CJCE, 27 mai 1981, *Essevi et Salango*, 142, 143/80 ; CJCE, 2 févr. 1988, *Blaizo*, C 24/86 ; CJCE, 19 oct. 1995, *Richardson*, aff. C-137/94.

constitutionnelle nationale qui a décidé l'ajournement de la perte de force obligatoire des mêmes dispositions jugées inconstitutionnelles"[101]. Aucun argument ne peut donc être tiré des décisions par lesquelles le Conseil constitutionnel a différé les conséquences de la censure des articles L. 34-1 CPCE et 77-1-1 du code de procédure pénale.

Cependant, si la nécessité de prendre en compte l'objectif de sécurité juridique ne peut justifier le report des conséquences de la non-conformité au droit de l'Union, sauf à ce que vous interrogiez la Cour de justice sur ce point[102], il nous semble qu'elle peut justifier une modulation de la sanction.

3.2.4.3.- Possibilité d'une modulation de la sanction procédurale de la non conformité

a) Principe d'autonomie procédurale

Tirant les conséquences du principe d'autonomie procédurale consacré par elle de longue date - que l'on retrouve d'ailleurs dans la jurisprudence de la Cour européenne des droits de l'homme[103] - la Cour de justice rappelle qu'"*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 grave, d'informations et d'éléments de preuve qui ont été obtenus par une telle conservation de données contraire au droit de l'Union*" (*Commissioner of An Garda Síochána*, point 222). De même, en vertu du même principe, c'est, pour elle, à l'ordre juridique interne de chaque Etat membre, "*de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tiennent du droit de l'Union*" (ibid. point 223).

Toutefois, cette autonomie doit s'exercer dans le respect de deux principes. Le premier est celui "*d'équivalence*" en vertu duquel les modalités procédurales ne doivent "*pas être moins favorables que celles régissant des situations similaires soumises au droit interne*". Le second est le principe "*d'effectivité*" en vertu duquel elles ne doivent pas rendre "*impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union*" (*ibid.*)[104]. Cette double limite tend en réalité à assurer le plus haut degré de protection car une sanction équivalente sera insuffisante si elle ne garantit pas l'effectivité du droit de l'Union et une sanction effective le sera également si elle n'apparaît pas équivalente à la sanction plus rigoureuse, appliquée en droit interne, dans des cas de figure comparables.

---

[101] CJUE, 19 nov. 2009, *Filipak*, aff. C-314/08, pour le Tribunal constitutionnel polonais ; CJUE, 8 sept. 2010, *Winner Wetten*, aff. C-409/06 pour la Cour constitutionnelle allemande

[102] Ce que vous aviez fait pour l'accès aux données de connexion par les agents de l'autorité des marchés financiers (Crim. 1er avr. 2020, n° 19-80.908, n° 19-82.222, n° 19-82.223). Au cas présent, si elle a exclu expressément un report s'agissant de l'interdiction d'une conservation généralisée et indifférenciée, la Cour n'a pas pris expressément parti s'agissant de l'exigence d'une autorisation juridictionnelle. Le débat n'est donc peut-être pas tout à fait clos.

[103] v. not. CEDH, 10 mars 2009, *Bykov c. Russie*, n° 4378/02 ; CEDH 12 juil. 1988, *Schenk c. Suisse*, n°10862/84 ; CEDH 4 oct. 2000, *Khan c. Royaume-Uni*, n°35394/97 ; CEDH 17 oct. 2019, *Lopez Ribalda c. Espagne*, n° 1874/13 et 8567/13

[104] CJUE, *La Quadrature du Net*, pt 223 ; CJUE 6 oct. 2015, *Târsia*, C-69/14, points 26 et 27 ; CJUE 24 oct. 2018, *XC e.a.*, C-234/17, points 21 et 22 ; CJUE 19 déc. 2019, *Deutsche Umwelthilfe*, C-752/18, point 33

Tandis que la détermination des exigences découlant du principe d'effectivité, qui tend à assurer un seuil minimal de protection du droit de l'Union, ressortit à la Cour de justice, celle des exigences découlant du principe d'équivalence revient principalement au juge national qui est évidemment le mieux placé pour mettre celui-ci en oeuvre[105].

b) Respect du principe d'effectivité

Au cas présent, la Cour de justice a défini précisément les implications du principe d'effectivité. Nous nous bornerons à évoquer sur ce point les motifs de son arrêt *Prokuraturr* puisque son objet était plus spécialement de fixer les conditions d'accès aux données de connexion. Soulignons toutefois qu'ils expriment une solution établie de longue date, l'arrêt *La Quadrature du Net* comptant au nombre des précédents (points 225 à 227) et renvoyant lui-même à l'arrêt *Steffensen* du 10 avril 2003[106].

Pour la Cour de justice, les dispositions nationales qui tendent à 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 peuvent selon le cas en interdire l'exploitation, en pondérer la valeur ou même ne prendre le cadre de la détermination de la peine".* Lorsqu'il s'agit d'assurer l'effectivité du droit de l'Union, la nécessité d'une exclusion doit être appréciée en considérant, notamment*, "le 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".* La Cour en déduit que 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'un accès de l'autorité compétente à ces données en violation du droit de l'Union, dans le cadre d'une procédure pénale"* si les personnes mises en cause dans cette procédure *"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" (Prokuratuur,* points 43 et 44*)*

A la lumière de ces motifs, il ne fait pas de doute que notre droit satisfait à l'exigence d'effectivité ainsi requise. Certes, les procédés techniques au moyen desquels les données de connexion ont été collectées échappent à la connaissance des juges qui n'ont accès qu'aux données telles qu'elles leur sont restituées après exploitation. La personne mise en cause n'est pas davantage en mesure de "commenter efficacement" l'utilisation de ces procédés dont dépend l'authenticité, la fiabilité et la pertinence des données dont l'émission lui est attribuée. Toutefois elle dispose de la possibilité d'être éclairée par un technicien en sollicitant, au stade de l'enquête, un examen technique en application de l'article 77-1 du code de procédure pénale, ou, au stade de l'instruction et du jugement, une expertise prévue par l'article 156 de ce code. Il faut donc considérer que le moyen lui est donné *"de commenter efficacement ces informations et ces éléments de preuve, provenant d'un*

---

[105] E. Dubout, *Droit constitutionnel de l'Union européenne*, Ed. Bruylant, 2021, n° 248 s.

[106] CJUE, 10 avr. 2003, *Steffensen*, C-276/01

domaine échappant à la connaissance des juges" (v. sur le recours à l'expertise, CJUE *Steffensen préc.*).

Il reste à examiner de quelle manière le respect du principe d'équivalence peut être également satisfait.

c) Respect du principe d'équivalence

1) Solution du grief intrinsèque

Il résulte de votre jurisprudence que, dans les cas où une mesure attentatoire à la vie privée doit être précédée de l'autorisation d'un juge ou du ministère public, le défaut de cette autorisation emporte la nullité de la mesure sans qu'il soit nécessaire d'établir l'existence d'un grief distinct de celui résultant de l'atteinte à la vie privée causée par la mesure[107]. Autrement dit, une telle irrégularité fait nécessairement grief de sorte que les dispositions des articles 171 et 802 du code de procédure pénale, qui subordonnent le prononcé de la nullité à la démonstration d'un grief, sont en quelque sorte satisfaites mécaniquement. La solution se justifie à la fois par la gravité de l'irrégularité et par sa nature. A moins d'ouvrir la voie à toutes les dérives, on ne peut, pour apprécier s'il y a lieu à annulation, supputer les conséquences du défaut d'une autorisation judiciaire exigée par la loi pour, le cas échéant, couvrir une telle irrégularité. Cela reviendrait à ménager la possibilité de se dispenser de l'autorisation. En outre, lorsque l'irrégularité tient dans le défaut d'une autorisation, il est assez difficile de démontrer un grief qui ne tiendrait pas au défaut d'autorisation lui-même.

2) Prise en compte de l'exigence de sécurité juridique

Cela étant, si la rigueur de la sanction trouve sa raison d'être dans la violation d'une formalité essentielle imposée par la loi, elle apparaît inadaptée lorsque, comme en l'espèce, d'une part, une disposition nationale écartait expressément la nécessité d'une telle autorisation et que, d'autre part, la non-conformité de cette disposition à la norme supérieure était incertaine. En raison de l'absence de clarté et de prévisibilité de la norme, la sanction perd en ce cas sa dimension qu'on pourrait qualifier de "disciplinaire" justifiant sa quasi automaticité. Ce n'est en effet pas la même chose de violer la loi et de se conformer à une loi dont la non-conformité à la norme internationale est incertaine. Dans ce second cas, il nous semble indispensable de prendre en compte l'exigence de sécurité juridique, non pour différer la sanction - solution proscrite - mais pour l'adapter ou la moduler.

- *Exigence de la démonstration d'un grief*

Dans cette perspective, vous pourriez songer à écarter toute annulation lorsque la juridiction en charge du contrôle de la régularité de l'acte - au cas présent, la chambre de l'instruction saisie de la requête en nullité - est en mesure de s'assurer que, nonobstant

---

[107] Crim. 14 oct. 2003, n° 03-84.539, B. n° 187 ; Crim. 1er sept. 2005, n° 05-84.061, B. n° 211 ; Crim. 6 déc. 2015, n° 05-85.076, B. n° 319. La solution est la même pour le défaut de motivation de l'autorisation lorsqu'elle est exigée : Crim. 10 janv. 2018, n° 17-83.932 ; Crim. 8 juill. 2015, n° 15-81.731

l'absence d'autorisation d'un juge, la réquisition litigieuse n'a pas porté une atteinte disproportionnée à la vie privée du requérant. C'est d'ailleurs le constat fait en l'espèce par la chambre de l'instruction.

La solution peut apparaître cohérente dans la mesure où la raison d'être du contrôle préalable est "*d'empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire*" (CJUE, *Prokuraturr*, point 58).

Cependant, elle reviendrait peu ou prou à substituer un contrôle a posteriori à un contrôle préalable et donc, en réalité, à suspendre transitoirement l'application du droit de l'Union tel qu'il a été interprété par la Cour de justice. Rappelons que, pour la Cour de justice, un contrôle préalable revêt une importance cruciale. Pour elle, *"un contrôle ultérieur ne permettrait pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire" Commissioner of An Garda Síochána*, point 110 ; *La Quadrature du Net*, point 189 ; *Prokuratuu*r, point 58) ou encore "*un contrôle exercé a posteriori ne saurait se substituer à l'exigence* (...) *de contrôle indépendant et, sauf cas d'urgence dûment justifiée, préalable*" (*Commissioner of An Garda Síochána*, point 112).

Il paraît en revanche admissible de considérer que, dans le cas où, comme en l'espèce, la mesure, décidée par un enquêteur, a été poursuivie quelques jours plus tard par un juge, cette circonstance suffit à établir rétrospectivement que la mesure aurait été, dès l'origine, autorisée par celui-ci. La solution revient à considérer que, dans un tel cas de figure, aucun grief n'est résulté de l'irrégularité, l'intervention du juge valant régularisation. Si la solution ne correspond pas, on l'a vu, à votre jurisprudence, elle nous paraît pouvoir être retenue dans l'objectif de ménager la sécurité juridique durant une période transitoire. Elle ne heurte pas le principe d'équivalence dès lors qu'elle n'est qu'une application particulière des dispositions de la règle "pas de nullité sans grief" énoncée aux articles 171 et 802 du code de procédure pénale. Bien entendu, en ce cas, l'absence d'annulation en raison de l'incompétence de l'autorité ayant délivré l'autorisation n'exclut pas un contrôle de proportionnalité a posteriori, toujours possible.

- *Perte de valeur probante*

La solution peut se combiner avec une autre qui, en tout état de cause, nous semble devoir être appliquée lorsqu'aucune "régularisation" ne peut être constatée. Elle ne heurte pas le principe d'équivalence car précisément, vous l'avez déjà retenue dans un cas de figure semblable à celui qui vous est soumis.

Comme celles de la Cour de justice de l'Union européenne, les décisions de la Cour européenne des droits de l'homme doivent être respectées sans possibilité d'en reporter les effets dans le temps. Ainsi, par quatre arrêts du 15 avril 2011, l'Assemblée plénière de la Cour de cassation a posé en principe "*que les Etats adhérents à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales sont tenus de respecter les décisions de la Cour européenne des droits de l'homme, sans attendre d'être attaqués devant elle ni d'avoir modifié leur législation*". Faisant application de ce principe, à la suite des arrêts de la Cour de Strasbourg *Salduz c/ Turquie* et *Dayanan c/ Turquie*, des 27 novembre 2008 et 13 octobre 2009 imposant l'accès à un avocat dès le premier

interrogatoire d'un suspect par la police, l'Assemblée plénière a retenu que la méconnaissance de cette exigence devait donner lieu à annulation alors même qu'à la date de la garde à vue l'intervention d'un avocat n'était pas imposée par la loi[108].

Sans remettre en cause bien entendu, la nécessité de la sanction procédurale, vous en avez toutefois tempéré la rigueur de deux manières.

Dans le cas où la question de la régularité de la garde à vue était posée au stade du jugement sur le fond, vous avez jugé qu'il ne pouvait être fait grief à la juridiction correctionnelle d'avoir écarté ou omis d'examiner une exception de nullité tirée du défaut d'assistance d'un avocat lorsque "*la déclaration de culpabilité n'est fondée ni exclusivement ni même essentiellement sur les déclarations recueillies au cours de la garde à vue*""[109]. Vous avez donc déplacé le débat du terrain de la nullité vers celui de la preuve. Pour reprendre les termes précités de l'arrêt *Prokuratuur*, à défaut d'annulation, vous avez "*interdit l'exploitation*" ou, à tout le moins, "*pondéré la valeur*" des déclarations en garde à vue lors de l'appréciation du bien-fondé de l'accusation.

Par un arrêt du 11 décembre 2018, vous avez étendu cette solution au cas où, comme en l'espèce, la question se posait devant la chambre de l'instruction saisie d'une requête en nullité et donc indépendamment de toute appréciation du bien-fondé de l'accusation[110]. Constatant qu'à la date de l'arrêt attaqué la solution résultant des arrêts précités de la Cour européenne des droits de l'homme n'était pas bien établie, vous avez jugé qu'il n'y avait pas lieu à annulation mais que "*les déclarations incriminantes"* faites lors des auditions en garde à vue sans l'assistance d'un avocat ne pourraient, *"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*". Dans l'espèce considérée, la garde à vue était très antérieure aux arrêts de la Cour de Strasbourg mais la solution est indépendante de cette circonstance. Elle eût été la même si elle ne les avait précédées que de quelques jours.

Les éléments contenus dans l'acte irrégulier sont ainsi réduits à de simples renseignements susceptibles de guider les investigations sans pouvoir fonder l'accusation. Cette solution équilibrée est celle que vous retenez également lorsqu'il s'agit d'apprécier le sort devant être réservé à des informations dont l'origine est anonyme ou qui émanent des services de

---

[108] Crim. 14 avril 2011, n° 10-17.049, n° 10-30.242, n° 10-30.313 et 1n° 0-30.316, B. Ass. plén. n° 1, 2, 3 et 4

[109] Crim., 6 déc. 2011,n° 11-80.326, B., n° 247 ; Crim., 14 mars 2012, n° 11-81.274, B., n° 72 ; Crim., 21 mars 2012, n° 11-83.637, B. n° 78 ; Crim., 31 mai 2012, n° 11-83.494, B. no 141 ; Crim., 13 juin 2012, n° 10-82.420, 11-81.573, B. n° 147 ; Crim., 18 sept. 2012, n° 11-85.031, B., no 190 ; Crim., 12 déc. 2012, n° 12-80.788, B. n° 275 ; Crim., 24 avr. 2013, n° 12-83.602, B., no 101 ; Crim. 15 juin 2016, no 14-87.715, B. n° 184 - Et pour le cas un peu différent où la demande d'annulation a été examinée par la chambre de l'instruction dont l'arrêt fait l'objet d'un pourvoi examiné en même temps que le pourvoi formé contre l'arrêt sur le fond : Crim., 13 juin 2012, no 10-82.420, 11-81.573, B. no 147; Crim., 12 déc. 2012, no 12-80.788, B. no 275 ; Crim. 12 févr. 2014, no 12-84.500 ; Crim. 30 avr. 2014, no 08-85.410, 12-85.115, B., no 118

[110] Crim. 11 déc. 2018, n° 18-82.854, n° 18-82.854, B. n° 209

renseignement ou des attachés de sécurité intérieure[111]. Elle fait donc indiscutablement partie de la gamme des réponses que vous apportez aux défauts de la procédure et satisfait aux exigence du procès équitable ainsi que l'a jugé la Cour européenne des droits de l'homme[112].

3.3.- Appréciation du moyen

3.3.1.- Constat de non-conformité au droit de l'Union

En l'espèce, vous ne pourrez donc que constater que les réquisitions ayant pu être délivrées au cours de l'enquête de flagrance, l'ont été en méconnaissances des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la Cour de justice de l'Union européenne, sans l'autorisation d'un juge ou d'une autorité administrative indépendante et sans que soit constatée l'urgence laquelle ne peut découler mécaniquement de la flagrance.

Il ne pourrait en être autrement que si vous décidiez de poser une question préjudicielle à la Cour de justice. Compte tenu de la clarté et de la fermeté avec lesquelles, par deux arrêts rendus en grande chambre, la Cour a affirmé sa position, il nous paraît difficile que cette question porte sur le point de savoir si, pour l'application de l'article précité de la directive 2002/58, le ministère public français peut être regardé comme une autorité/entité administrative indépendante. De même, il nous paraît assez vain de demander à la Cour s'il n'y aurait pas lieu de distinguer selon l'ampleur de l'atteinte à la vie privée causée par l'accès aux données relatives au trafic et aux données de localisation dès lors qu'elle a déjà indiqué on ne peut plus clairement qu'elle tenait une telle distinction pour inopérante (supra, 3.2.3.4, a). Par ailleurs, comme nous l'avons relevé, si l'identité constitutionnelle de la France nous paraît exclure que soit soustraite au contrôle de l'autorité judiciaire une mesure attentatoire à la vie privée, nous doutons qu'elle fasse obstacle à ce qu'une telle mesure soit soumise au contrôle d'un juge du siège plutôt qu'à celui du ministère public. Enfin, même si elle peut être envisagée, une question préjudicielle sur la suspension de l'application du droit de l'Union nous paraît se heurter à la jurisprudence ferme et constante de la Cour.

3.3.2.- Rejet du moyen par substitution de motifs

Cependant, en l'espèce, le rejet du moyen s'impose en tout état de cause.

---

[111] Crim., 9 juillet 2003, n° 03-82.119, B. n° 138 ; Crim., 13 sept. 2011, n°11-83.100, B. n° 178 ; Crim., 9 nov. 2011, n° 05-87.745, 09-86.381, B. n° 230 ; Crim., 28 mai 2014, n° 13-83.197, 11-81.640, B. n° 142 ; Crim. 3 sept. 2014, n° 11-83.598 ; Crim., 1er avr. 2015, n°14-87.647, B. n° 74 ; Crim., 6 oct. 2015, n° 15-82.247, B. n° 217 ; Crim. 19 sept. 2017, n° 17-82.317 ; Crim., 19 mai 2021, n° 21-80.849

[112] CEDH, 25 nov. 2021, *Sassi et Benchellali c/ France*, req. n°s 10917/15 et 10941/15, § 101 ; CEDH, 28 avr. 2022, *Dubois c. France*, n° 52833/19, § 89-90

Sans discuter l'irrégularité, la chambre de l'instruction, se référant aux motifs de la Cour de justice relatifs au principe d'effectivité, a écarté la demande d'annulation de l'intéressé en opposant en substance que, mis en examen le 26 juin 2020, il avait été "*mis en mesure de commenter efficacement l'ensemble des éléments de la procédure apparaissant comme constituant des indices graves ou concordants rendant vraisemblable son implication comme auteur ou complice des faits pour lesquels il est mis en examen*".

Pour les raisons exposées, cette motivation peut être approuvée en précisant qu'en l'espèce le "commentaire efficace" de questions échappant à la connaissance des juges est permis par le recours à l'examen technique ou à l'expertise.

La chambre de l'instruction retient par ailleurs que, compte tenu de la gravité des infractions reprochées, l'atteinte à la vie privée était proportionnée. Mais, comme nous l'avons vu, ce contrôle a posteriori assuré par elle plus d'un an et demi après la réalisation des actes contestés ne peut être regardé comme satisfaisant aux exigences du droit de l'Union et notamment, au principe d'équivalence.

Néanmoins, vous pourrez écarter le moyen après avoir substitué vos motifs à ceux de l'arrêt attaqué. A cet égard, nous vous proposons de juger qu'en raison de l'incertitude qui entourait la règle applicable avant sa clarification par votre arrêt - ou, au plus tôt, par l'arrêt *Prokuratuur* du 2 mars 2021 - la nullité ne peut être prononcée sans qu'il soit démontré que l'irrégularité tenant au défaut d'autorisation préalable a causé un grief à l'intéressé. Au cas présent, vous êtes en mesure de vous assurer par un examen des pièces de la procédure dont vous avez le contrôle que, le juge d'instruction a été saisi le 6 septembre 2019, soit une dizaine de jours après la délivrance des réquisitions relatives à la ligne dont l'intéressé avait l'usage, et que le magistrat a poursuivi les investigations de téléphonie à l'égard de celui-ci. Il résulte de ces circonstances qu'est intervenu, dans un délai rapproché, le contrôle d'une juridiction qui a nécessairement validé, en les reprenant à son compte, les réquisitions critiquées.

En tout état de cause, si vous ne suiviez pas ce raisonnement, il conviendrait de juger qu'en raison de l'incertitude évoquée, l'irrégularité ne peut avoir d'autre conséquence que de retirer leur valeur probante aux réquisitions litigieuses lors de l'appréciation du bien-fondé de l'accusation, que ce soit au stade du règlement ou au stade du jugement.

3.3.3.- Observation finale

En conséquence de la non-conformité des articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale au droit de l'Union, l'autorisation d'un juge doit être sollicitée, sous réserve de l'urgence, pour la délivrance de réquisitions tendant à l'obtention de données relatives au trafic et de données de localisation. La solution ne soulève pas seulement, pour le passé, une question de prévisibilité de la règle et de sécurité juridique. Elle pose, pour l'avenir, une question de moyens. Pour les réquisitions qui seront délivrées postérieurement à votre arrêt - ou, selon ce que vous jugerez, pour celles délivrées depuis l'arrêt *Prokuratuur* - ce n'est pas la prévisibilité de la règle qui est en cause mais la capacité à la mettre en oeuvre en raison de l'impossibilité de prendre *ex abrupto* les dispositions nécessaires à cet effet - notamment la création de centaines d'emplois de juges. Il pourra alors être envisagé d'interroger la Cour de justice sur la possibilité d'écarter à titre transitoire le principe d'équivalence afin de permettre le maintien de la modulation de la sanction pour une durée raisonnable - nécessairement limitée -

de manière à prendre en compte cette contrainte exceptionnelle sinon insurmontable. Mais la question ne se pose pas en ces termes dans la présente affaire.

4. En conséquence, nous concluons au rejet de l’ensemble des moyens et, partant, du pourvoi.

A titre subsidiaire, si vous ne reteniez pas la solution proposée pour écarter le deuxième moyen, nous concluons à ce que la Cour de justice de l’Union européenne soit saisie à titre préjudiciel dans les conditions indiquées (supra, 2.6.3). En ce cas, vous apprécierez s’il y a lieu de l’interroger en outre sur la possibilité de maintenir provisoirement les effets d'une législation permettant aux enquêteurs, dans les procédures pénales, d'obtenir sans contrôle préalable d'une juridiction ou d'une autorité administrative indépendante, la communication de données de connexion (supra, 3.2.4.2).

Avis de rejet